Note

Representation of permutations as products of two cycles

Marcel Herzog\textsuperscript{a}, Gil Kaplan\textsuperscript{b}, Arieh Lea\textsuperscript{b}

\textsuperscript{a}School of Mathematical Sciences, Sackler Faculty of Exact Sciences, Tel Aviv University, Ramat Aviv, Tel-Aviv 69978, Israel
\textsuperscript{b}Department of Computer Sciences, The Academic College of Tel-Aviv-Jaffo, 4 Antokolsky st., Tel-Aviv 64044, Israel

Received 7 November 2002; received in revised form 29 December 2003; accepted 20 January 2004

Abstract

Given a permutation $\sigma$ on $n$ letters, we determine for which values of the integers $l_1$ and $l_2$ it is possible to represent $\sigma$ as a product of two cycles of sizes $l_1$ and $l_2$, respectively. Our results are of a constructive nature. We also deal with the special cases $l_1 = l_2$ for even permutations and $l_1 = l_2 + 1$ for odd permutations, which were solved differently by Bertram in (J. Combin. Theory 12 (1972) 368).

\textcopyright{} 2004 Elsevier B.V. All rights reserved.

Keywords: Permutations; Cycles; Products of cycles

1. Introduction

Let $S_n$ and $A_n$ denote the symmetric and the alternating groups of permutations on $\Omega = \{1, 2, \ldots, n\}$, respectively. Suppose that $\sigma \in S_n$ and $\sigma = C_1C_2$, where $C_1, C_2$ are cycles in $S_n$ of lengths $l_1$ and $l_2$, respectively. The question we are concerned with is: what are the possible values of $l_1$ and $l_2$? The answer to this question is given in Theorem 7, which is the main result of this paper. An important feature of our proof is that it is constructive. By that we mean that given $n \in \mathbb{N}$ and $\sigma \in S_n$, there exists a procedure, based on the proof of Theorem 7 and on the lemmas preceding it, for the construction of representations of $\sigma$ as a product of two cycles for all the allowed values of $l_1$ and $l_2$. A description of this procedure, followed by a numerical example, can be found in the final part of this paper.

In the paper [3] published in 1978, Boccara also dealt with representations of permutations as products of two cycles. Our methods of proof are more direct than his and our results are more explicit and of a constructive nature. We also mention another paper of Boccara [4], in which he presents a formula for the number of representations of a given permutation as a product of two cycles of fixed lengths.

As special cases of Theorem 7, we determine in Theorems 8 and 9 all the possible values of the integer $r$, such that a given $\sigma \in A_n$ can be represented as a product of two cycles of length $r$ and a given $\sigma \in S_n - A_n$ can be represented as a product of two cycles of lengths $r + 1$ and $r$, respectively. These special results were first obtained by Bertram in [1]. Our proofs are simpler and, as mentioned above, constructive.

By checking the extreme cases it is possible to determine, using Theorems 8 and 9, for which values of $r \in \mathbb{N}$ each $\sigma \in A_n$ can be represented as a product of two cycles in $S_n$ of length $r$, and for which values of $r$ each $\sigma \in S_n - A_n$ can be represented as a product of two cycles in $S_n$ of lengths $r + 1$ and $r$, respectively. These results, which appear also in [1], were summarized without a proof in Corollary 10. Additional results, dealing with representation of each permutation in $A_n$ as a product of three or four cycles in $S_n$ of equal lengths, can be found in [2].

Most of our notation is standard. The positive integers are denoted by $\mathbb{N}$. If $M \subseteq \Omega = \{1, 2, \ldots, n\}$, then $\text{Sym}(M)$ denotes the symmetric group on $M$. Product of permutations will be executed from left to right. Suppose, first, that $\sigma \in S_n - \{1\}$. Then $\text{supp}(\sigma)$, the support of $\sigma$, is the set $\{i \in \Omega : \sigma(i) \neq i\}$ and $\text{dcd}*(\sigma)$, a restricted disjoint cycle decomposition of $\sigma$, denotes a representation of $\sigma$ as a product of disjoint cycles of length $>1$. It is well known that $\text{dcd}*(\sigma)$ is unique.

E-mail address: herzogm@post.tau.ac.il (M. Herzog).

0012-365X/$ - see front matter \textcopyright{} 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2004.01.019
except for a cyclic shift within the cycles and the order in which the cycles are written. We denote \( m_\sigma = |\text{supp}(\sigma)| \) and the number of cycles in \( \text{dcd} * (\sigma) \) is denoted by \( n_\sigma \). For \( \sigma = 1 \), we define \( \text{dcd} * (1) = (1) \) and \( m_1 = n_1 = 1 \). If \( G \) is a subgroup of \( S_n \) we denote by \( \text{supp}(G) \) the subset of letters in \( \Omega \) which are moved by an element of \( G \). If \( q \) is a rational number, then \( \lfloor q \rfloor = k \), where \( k \) is the unique integer satisfying \( k \leq q < k + 1 \).

We conclude this introduction with four results of a general nature. Theorem 4 is an important result of Ree [6], whose elementary proof can be found in [5].

**Lemma 1.** Let \( a = (a_1 a_2 \ldots a_r) \) and \( b = (b_1 b_2 \ldots b_s) \) be cycles in \( S_n \). Then the following statements hold.

\[
(1) \quad (a_1 \ldots a_{r-1} a_r) = (a_1 \ldots a_r) (a_1 a_r) = (a_{r-1} a_r) (a_1 \ldots a_{r-1}).
\]

(2) Suppose that

\[
(i) \quad \text{supp}(a) \cap \text{supp}(b) \neq \emptyset
\]

and

\[
(ii) \quad \text{supp}(a) \not\subseteq \text{supp}(b).
\]

Then, for a proper cyclic reordering of \( a \) and \( b \), we have

\[
ab = (a_1 \ldots a_{r-1}) (b_1 \ldots b_s a_1)
\]

where \( a_1 \in \text{supp}(a) - \text{supp}(b) \).

**Proof.** Claim (1) can be easily checked. Suppose, now, that (i) and (ii) hold. By (i) there exists \( i \) such that \( a_i \in \text{supp}(b) \). If \( a_i \in \text{supp}(b) \) always implies that \( a_{i+1} \in \text{supp}(b) \) (with \( r+1 \) replaced by 1), then \( \text{supp}(a) \subseteq \text{supp}(b) \), contradicting (ii). So there exists \( i \) such that \( a_i \in \text{supp}(b) \) and \( a_{i+1} \notin \text{supp}(b) \) and we may assume, without loss of generality, that \( a_r \in \text{supp}(b) \), \( a_i \notin \text{supp}(b) \) and \( b_s = a_r \). Then, by (1),

\[
ab = (a_1 \ldots a_{r-1}) (a_i a_1) (b_1 \ldots b_s a_1) = (a_1 \ldots a_{r-1}) (b_1 \ldots b_{s-1} b_s a_1)
\]

as claimed. \( \square \)

**Lemma 2.** Let \( \sigma \in S_n \) and let

\[
\text{dcd} * (\sigma) = (a_1 \ldots a_{m_\sigma}) (a_{m_\sigma+1} \ldots a_{m_\sigma+1}) \cdots (a_{m_\sigma+n_\sigma-1} \ldots a_{m_\sigma+n_\sigma}).
\]

Then \( \sigma \) can be represented as a product of the following two cycles of lengths \( m_\sigma \) and \( n_\sigma \), respectively:

\[
\sigma = (a_1 a_2 \ldots a_{m_\sigma}) (a_{m_\sigma+1} \ldots a_{m_\sigma+n_\sigma-1} a_{m_\sigma+n_\sigma}).
\]

Hence \( m_\sigma + n_\sigma \) is even if \( \sigma \in A_n \) and it is odd if \( \sigma \in S_n - A_n \).

**Proof.** If \( \sigma = 1 \), then \( m_\sigma = n_\sigma = 1 \), \( \text{dcd} * (\sigma) = (1) \) and \( \sigma = (1)(1) \), as claimed. In other cases, the truth of Lemma 2 can be easily checked by inspection. \( \square \)

**Lemma 3.** Let \( r, s \in \mathbb{N} \) satisfy \( 1 \leq s \leq r \leq n - 1 \) and let \( R \) and \( S \) be an \( r \)-cycle and an \( s \)-cycle in \( S_n \), respectively. Then there exist an \( r + 1 \)-cycle \( R' \) and an \( s + 1 \)-cycle \( S' \) in \( S_n \), such that \( RS = R'S' \).

**Proof.** The proof of Lemma 14 in [2] holds verbatim, even though the assumption there was that \( 2 \leq s \leq r \leq n - 1 \). \( \square \)

**Theorem 4.** Let \( D_i \in S_n \) for \( 1 \leq i \leq k \) and let \( G = \langle D_1, D_2, \ldots, D_k \rangle \) be the subgroup of \( S_n \) generated by the \( D_i \). Suppose that \( D_1 D_2 \cdots D_k = 1 \) and let \( T \) be the number of orbits of \( G \) on its support. Then

\[
\sum_{i=1}^{k} (m_{D_i} - n_{D_i}) \geq 2(F - T),
\]

where \( F = |\text{supp}(G)| \).

A group-theoretical proof of this result can be found in [5].
2. On products of two cycles in \( S_n \)

**Proposition 5.** Let \( \sigma \in S_n \) and let \( M = \text{supp}(\sigma) \). Then, whenever \( l_1, l_2 \in \mathbb{N} \) satisfy

(1) \( l_1 + l_2 = m_\sigma + n_\sigma \), and

(2) \( \min(l_1, l_2) > n_\sigma \),

there exist two cycles \( C_1, C_2 \in \text{Sym}(M) \) of sizes \( l_1, l_2 \), respectively, such that \( \sigma = C_1C_2 \).

**Proof.** By Lemma 2 the lemma is true for \( l_1 = m_\sigma \) and \( l_2 = n_\sigma \), with \( \text{supp}(C_2) \subseteq \text{supp}(C_1) \). By part (2) of Lemma 1, we may transfer, one by one and in the proper order, each element of \( D = \text{supp}(C_1) - \text{supp}(C_2) \) from \( C_1 \) to \( C_2 \), and at each step of the transfer we obtain new couples of cycles in \( \text{Sym}(M) \), whose product equals \( \sigma \) and whose lengths \( l_1 \) and \( l_2 \) satisfy (1) and (2) of this proposition. Indeed, property (i) of Lemma 1 is satisfied at each stage, as both cycles contain \( \text{supp}(C_2) \), and property (ii) is satisfied as long as not all elements of \( D \) have been transferred from \( C_1 \) to \( C_2 \). Since the length of \( C_1 \) decreases in steps of one from \( m_\sigma \) to \( n_\sigma \), the existence of couples of cycles in \( \text{Sym}(M) \) of lengths \( l_1 \) and \( l_2 \) satisfying (1) and (2) of this proposition and whose product equals \( \sigma \) has been established for all allowed values of \( l_1 \) and \( l_2 \).

**Lemma 6.** Let \( \sigma \in S_n \) and suppose that \( \sigma = C_1C_2 \), where \( C_1, C_2 \) are cycles in \( S_n \) of lengths \( l_1, l_2 \), respectively, with \( l_1, l_2 \geq 2 \). Let \( M = \text{supp}(\sigma) \), \( U = \text{supp}(C_1) \cup \text{supp}(C_2) \) and let \( d = |U - M| \). Then either \( C_1C_2 = \text{dcd} * (\sigma) \) or

(1) \( l_1 + l_2 = m_\sigma + n_\sigma + 2r \)

for some integer \( r \geq d \).

**Proof.** Let \( G = \langle C_1, C_2 \rangle \) and let \( T \) be the number of orbits of \( G \) on \( U \). We may assume that \( C_1C_2 \neq \text{dcd} * (\sigma) \), in which case \( T = 1 \) and since \( \sigma^{-1}C_1C_2 = 1 \), Theorem 4 implies

\[
(m_\sigma - n_\sigma) + (l_1 - 1) + (l_2 - 1) \geq 2(F - 1),
\]

where \( F = |U| \). As \( F = m_\sigma + d \), it follows that \( m_\sigma - n_\sigma + l_1 + l_2 \geq 2m_\sigma + 2d \), which implies \( l_1 + l_2 \geq m_\sigma + n_\sigma + 2d \). Since by Lemma 2 \( l_1 + l_2 \) and \( m_\sigma + n_\sigma \) are of the same parity, the result follows.

**Theorem 7.** Let \( \sigma \in S_n \) and let \( l_1, l_2 \in \mathbb{N}, n \geq l_1 \geq l_2 \geq 2 \). Then

\[
\sigma = C_1C_2,
\]

where \( C_1, C_2 \) are cycles in \( S_n \) of lengths \( l_1, l_2 \), respectively, if and only if either \( n_\sigma = 2 \), \( l_1, l_2 \) are the lengths of the cycles in \( \text{dcd} * (\sigma) \) and \( l_1 + l_2 = m_\sigma \), or the following conditions hold:

(1) \( l_1 + l_2 = m_\sigma + n_\sigma + 2s \) for some \( s \in \mathbb{N} \cup \{0\} \), and

(2) \( l_1 - l_2 \leq m_\sigma - n_\sigma \).

**Proof.** If \( n_\sigma = 2 \) and \( l_1, l_2 \) are the lengths of the cycles in \( \text{dcd} * (\sigma) \), then clearly \( l_1 + l_2 = m_\sigma \) and \( \sigma \) can be represented as required. So assume that this is not the case and that \( l_1, l_2 \in \mathbb{N}, n \geq l_1 \geq l_2 \geq 2 \), satisfy conditions (1) and (2). Then

\[
l_1 - m_\sigma + n_\sigma \leq l_2 = m_\sigma + n_\sigma + 2s - l_1
\]

which implies that \( l_1 \leq m_\sigma + s \). Thus, by (1), \( l_2 \geq n_\sigma + s \) and we may conclude that \( (l_1 - s) + (l_2 - s) = m_\sigma + n_\sigma \) and \( \min((l_1 - s), (l_2 - s)) \geq n_\sigma \). It follows by Proposition 5 that \( \sigma = D_1D_2 \), where \( D_1, D_2 \) are cycles in \( S_n \) of lengths \( l_1 - s, l_2 - s \), respectively. Lemma 3 then implies that there exist cycles \( C_1, C_2 \) in \( S_n \) of lengths \( l_1, l_2 \), respectively, such that \( \sigma = C_1C_2 \), as required.

Conversely, suppose that \( \sigma = C_1C_2 \), where \( C_1, C_2 \) are cycles in \( S_n \) of lengths \( l_1, l_2 \), respectively, and \( l_1 \geq l_2 \geq 2 \). Then \( n \geq l_1 \geq l_2 \geq 2 \) and we may assume that \( C_1C_2 \neq \text{dcd} * (\sigma) \). Then, by Lemma 6, \( l_1 + l_2 = m_\sigma + n_\sigma + 2r \), with \( r \in \mathbb{N} \cup \{0\} \), yielding (1). Let \( G = \langle C_1, C_2 \rangle \) and let \( T \) be the number of orbits of \( G \) on \( U = \text{supp}(C_1) \cup \text{supp}(C_2) \). As \( C_1C_2 \neq \text{dcd} * (\sigma) \), we have \( T = 1 \) and since \( \sigma^{-1}C_1^{-1}C_2^{-1} = 1 \), Theorem 4 implies that

\[
(m_\sigma - n_\sigma) + (l_1 - 1) + (l_2 - 1) \geq 2(F - 1),
\]

where \( F = |U| \). As \( F \geq l_1 \), it follows that \( m_\sigma - n_\sigma \geq l_1 - l_2 \), yielding (2). The proof of Theorem 7 is complete.
**Remark 7'**. (a) Since $C_1C_2 = C_2C_1$, one can equivalently express $\sigma$ as the product of two cycles $C_1C_2$ of lengths $l_1$ and $l_2$, respectively, where $l_1 \leq l_2$.

(b) As shown above, conditions (1) and (2) of Theorem 7 imply

\[(2') \ l_1 \leq m_\sigma + s.\]

It is easy to see that conditions (1) and (2) are equivalent to conditions (1) and (2').

Theorem 7 easily yields the following two results, which were first proved by Bertram in [1].

**Theorem 8.** Let $\sigma \in A_n$, and let $r \in \mathbb{N}$, $n \geq r \geq 2$. Then $l = (m_\sigma + n_\sigma)/2$ is an integer. Moreover,

$$\sigma = C_1C_2,$$

where $C_1, C_2$ are cycles in $S_n$ of length $r$, if and only if either $n_\sigma = 2, r$ is the length of both cycles in $\text{cyc} \ast (\sigma)$ and $r = l - 1$, or the following condition holds:

\[(1) \ l \leq r.\]

**Proof.** By Lemma 2 $l$ is an integer. As condition (2) of Theorem 7 is trivially satisfied in our case and condition (1) of Theorem 7 reads: $r = l + s$ for some $s \in \mathbb{N} \cup \{0\}$, which is equivalent to (1), Theorem 8 follows from Theorem 7. \[\square\]

**Theorem 9.** Let $\sigma \in S_{n - 2} - A_n$, and let $r \in \mathbb{N}$, $n - 1 \geq r \geq 2$. Then $l = (m_\sigma + n_\sigma - 1)/2$ is an integer. Moreover,

$$\sigma = C_1C_2,$$

where $C_1, C_2$ are cycles in $S_n$ of lengths $r + 1, r$, respectively, if and only if either $n_\sigma = 2, r + 1, r$ are the lengths of the cycles in $\text{cyc} \ast (\sigma)$ and $r = l - 1$, or the following condition holds:

\[(1) \ l \leq r.\]

**Proof.** By Lemma 2 $l$ is an integer and if $\sigma$ is a product of two cycles of lengths $r + 1$ and $r$, then $\sigma \in S_n - A_n$, which implies that $m_\sigma - n_\sigma \geq 1 = (r + 1) - r$. Thus condition (2) of Theorem 7 is satisfied by all $\sigma$ under consideration and in our case condition (1) of Theorem 7 reads: $r = l + s$ for some $s \in \mathbb{N} \cup \{0\}$, which is equivalent to (1). Thus Theorem 9 follows from Theorem 7. \[\square\]

By checking the extreme cases, the following result can be proved using Theorems 8 and 9. Details of the proof can be found in [1], Corollaries 2.1 and 3.1.

**Corollary 10.** (1) Each permutation of $A_n$, $n \geq 2$, is a product of two cycles of length $r$ if and only if either $[3n/4] \leq r \leq n$ or $n = 4$ and $r = 2$.

(2) Each permutation of $S_{n - 2} - A_n$, $n \neq 5$, is a product of two cycles of lengths $r + 1$ and $r$, respectively, if and only if

$$\left\lfloor \frac{3n}{4} \right\rfloor \leq r \leq n - 1 \quad \text{when } n \equiv 1 \text{ or } 2 \pmod{4} \quad \text{and} \quad \left\lfloor \frac{3n}{4} \right\rfloor - 1 \leq r \leq n - 1 \quad \text{when } n \equiv 0 \text{ or } 3 \pmod{4}.$$

Conditions concerning the representation of each permutation in $A_n$ as a product of three or four cycles in $S_n$ of equal length can be found in [2].

As mentioned in the Introduction, Theorem 7, together with Lemmas 1–3, allows us to construct, for given $\sigma$ and $n$, representations of $\sigma$ as a product of two cycles in $S_n$, for all allowed lengths $l_1$ and $l_2$. Indeed, if $n_\sigma = 2$, then cyc $\ast (\sigma)$, when properly arranged, is a representation of type: $l_1 + l_2 = m_\sigma$. Otherwise, $l_1 + l_2$ is determined by the inequalities

$$m_\sigma + n_\sigma \leq l_1 + l_2 = m_\sigma + n_\sigma + 2s \leq 2n,$$

where $s$ is an arbitrary integer in $\mathbb{N} \cup \{0\}$, and the possible values of $(l_1 + l_2, s)$ can be set accordingly. Fix one of the allowed values for $(l_1 + l_2, s)$. Then, as shown in Remark 7(b), $l_1$ is determined by the inequalities $l_2 \leq l_1 \leq \min(m_\sigma + s, n)$ and since $l_1 + l_2$ was fixed, we obtain all the possible values of $l_1$ and $l_2$. Fix now $l_1$ and $l_2$; then $(l_1 - s) + (l_2 - s) = m_\sigma + n_\sigma$ and $l_1 - s \leq m_\sigma$ implies that $l_2 - s \geq n_\sigma$. Then, as described in the proof of Proposition 5, by an application of
Lemmas 2 and 1 we can construct a representation \( \sigma = D_1D_2 \), where \( D_1, D_2 \) are cycles in \( S_n \) of lengths \( l_1-s, \ l_2-s \), respectively. Finally, by successive application of Lemma 3, we can blow up the representation \( \sigma = D_1D_2 \) into a representation of \( \sigma \) as a product of cycles of lengths \( l_1 \) and \( l_2 \), respectively, thus completing the required construction.

We conclude this paper with a simple numerical example of the above mentioned procedure. Let \( \sigma = (12)(345) \in S_7 \); then \( m_\sigma = 5 \), \( n_\sigma = 2 \) and \( \mu = 7 \). Clearly \( \sigma = (345)(12) \) is a representation of \( \sigma \) as a product of two cycles of lengths \( l_1 = 3 \) and \( l_2 = 2 \), with \( l_1 + l_2 = m_\sigma \). Otherwise \( l_1 + l_2 \) is determined by the inequalities

\[
7 = 5 + 2 = m_\sigma + n_\sigma = l_1 + l_2 = m_\sigma + n_\sigma + 2s = 7 + 2s \leq 2n = 14,
\]

where \( s \in \mathbb{N} \cup \{0\} \). Thus \( (l_1 + l_2, s) \in \{ (7,0), (9,1), (11,2), (13,3) \} \) and we fix, as an example, \( (l_1 + l_2, s) = (11,2) \). Then

\[
l_2 \leq l_1 \leq \min(m_\sigma + s, n) = \min(5 + 2, 7) = 7 \quad \text{and as} \quad l_1 + l_2 = 11, \ \text{we get} \quad (l_1, l_2) \in \{ (7,4), (6,5) \}.
\]

If \( (l_1, l_2) = (7,4) \), then

\[
l_1 - m_\sigma = l_2 - n_\sigma = 2, \quad \text{and it follows by Lemmas 2 and 3 that}
\]

\[
\sigma = (12345)(31) = [(12345)(167)](761)(31) = (1234567)(1763)
\]

which is a \( (7,4) \)-representation of \( \sigma \). Finally, if \( (l_1, l_2) = (6,5) \), then \( l_1 - l_2 = 1 = (5 - 1) - (2 + 1) = (m_\sigma - 1) - (n_\sigma + 1) \). So we first use Lemmas 2 and 1 to get a \( (4,3) \)-representation of \( \sigma \)

\[
\sigma = (12345)(31) = (23451)(31) = (2345)(312)
\]

and then we apply Lemma 3 to get \( \sigma = [(2345)(267)](762)(312) = (234567)(12763) \), which is a \( (6,5) \)-representation of \( \sigma \), as required.

References