Journal of Algebra and Its Applications
Vol. 11, No. 6 (2012) 1250110 (8 pages)

DOI: 10.1142/S0219498812501101

ECONOMICAL GENERATING SETS FOR THE SYMMETRIC AND ALTERNATING GROUPS CONSISTING OF CYCLES OF A FIXED LENGTH

SCOTT ANNIN* and JOSH MAGLIONE†

Mathematics Department
California State University
Fullerton, CA 92834, USA
**sannin@fullerton.edu*
†joshmaglione@gmail.com

Received 2 June 2011
Accepted 4 January 2012
Published 9 November 2012

Communicated by S. Sehgal

The symmetric group S_n and the alternating group A_n are groups of permutations on the set $\{0, 1, 2, \ldots, n-1\}$ whose elements can be represented as products of disjoint cycles (the representation is unique up to the order of the cycles). In this paper, we show that whenever $n \geq k \geq 2$, the collection of all k-cycles generates S_n if k is even, and generates A_n if k is odd. Furthermore, we algorithmically construct generating sets for these groups of smallest possible size consisting exclusively of k-cycles, thereby strengthening results in [O. Ben-Shimol, The minimal number of cyclic generators of the symmetric and alternating groups, *Commun. Algebra* **35**(10) (2007) 3034–3037]. In so doing, our results find importance in the context of theoretical computer science, where efficient generating sets play an important role.

Keywords: Generating sets; step cycles; conjugation.

1. Introduction

The concept of a generating set for a mathematical structure is extraordinarily important across a broad spectrum of mathematics, particularly in algebra, and it has been the subject of many research investigations (e.g. [1–3, 5, 7, 8]). In the context of a group G, for example, the goal is to find a subset $S \subseteq G$ such that S generates G, often written as $G = \langle S \rangle$. The present article, largely motivated by the question posed in [8], extends the list of known generating sets for the symmetric group S_n and the alternating group A_n (and strengthens the main result in [3]) by considering the collection $C_{n,k}$ of all cycles in S_n of a fixed length k (i.e. all k-cycles), where, of course, $k \leq n$. As we shall see, if k is odd, then we can construct a subset S of $C_{n,k}$ such that $A_n = \langle S \rangle$, and if k is even, then we can do the same for S_n.

In both cases, we do this in such a way that the subset S constructed has the smallest possible size. The results we prove utilize the following well-known result that highlights what is perhaps the best known generating set for A_n.

Theorem 1.1. *The alternating group A_n is generated by $C_{n,3}$ for all $n \geq 3$.*

This theorem is useful in proving that A_n is simple whenever $n \geq 5$ (see, for example, [4, 6]).

2. Preliminary Results

We begin with some basic notations and terminology. For a given set X, let S_X (respectively, A_X) denote the group of all permutations (respectively, even permutations) of X. In case $X = \{0, 1, 2, \ldots, n-1\}$, we denote this group by S_n (respectively, A_n). For each positive integer n, let $\mathbb{Z}_n$ denote the group of integers modulo n. If k is a positive integer with $k \leq n$, a k-cycle $\sigma \in S_n$ that can be written in the form $\sigma = (a_0, a_1, a_2, \ldots, a_{k-1})$ such that $a_i \in \mathbb{Z}_n$ for all $i = 0, 1, 2, \ldots, k-1$ and $a_i = a_0 + i$ in $\mathbb{Z}_n$ for all $i = 0, 1, 2, \ldots, k-1$ will be called a *step k-cycle*, or simply *step cycle*, and we write $\sigma = h_k(a_0)$. We will refer to $a_0, a_1, a_2, \ldots, a_{k-1}$ as the *elements* of $h_k(a_0)$. Note that in the case $k < n$, the choice of a_0 is unique for each step k-cycle. We will sometimes refer to a pair of step cycles $h_k(a)$ and $h_k(a+1)$ as *consecutive* step cycles. Finally, let $H_{n,k} \subseteq C_{n,k}$ denote the set of all step cycles of length k in S_n. Observe that $|H_{n,n}| = 1$ for all n, and for $n > k$, we have $|H_{n,k}| = n$.

Our first main goal is to show, for positive integers k and n with $n > k \geq 2$, that $H_{n,k}$ generates A_n if k is odd, and $H_{n,k}$ generates S_n if k is even. The first step towards this end is Lemma 2.2 below, but before we proceed, we remind the reader of an important fact regarding the computation of conjugate elements in S_n that will be used freely throughout this paper (see, e.g. [4, 6]).

Proposition 2.1. *Let $\sigma, \tau \in S_n$. For each cycle $(a_0, a_1, a_2, \ldots, a_r)$ in the disjoint cycle representation of σ, the element $\tau\sigma\tau^{-1}$ contains the cycle $(\tau(a_0), \tau(a_1), \tau(a_2), \ldots, \tau(a_r))$ in its disjoint cycle representation, where $\tau(a_i)$ denotes the image of a_i under the permutation τ. In particular, the elements σ and $\tau\sigma\tau^{-1}$ have the same structure when expressed (uniquely up to order) as a product of disjoint cycles.*

Lemma 2.2. *Let n be an integer with $n \geq 3$. Then $C_{n,3} \subseteq \langle H_{n,3} \rangle$.*

Proof. We proceed by induction on n, with the case $n = 3$ being obvious. Now assume that $C_{n,3} \subseteq \langle H_{n,3} \rangle$. We claim that $C_{n+1,3} \subseteq \langle H_{n+1,3} \rangle$. The first step is to show that

$$\langle H_{n,3} \rangle \subseteq \langle H_{n+1,3} \rangle. \tag{1}$$

Note that the only elements of $H_{n,3}$ not belonging to $H_{n+1,3}$ are $(n-2, n-1, 0)$ and $(n-1, 0, 1)$, and these can be generated by elements of $H_{n+1,3}$ as follows:

$$(n-2, n-1, 0) = (n, 0, 1)(n-2, n-1, n)(n, 0, 1)^{-1} \quad \text{and}$$
$$(n-1, 0, 1) = (n, 0, 1)(n-1, n, 0)(n, 0, 1)^{-1}.$$

This establishes (1). Now consider $(a, b, c) \in C_{n+1,3}$. If $0 \leq a, b, c \leq n-1$, then already we have

$$(a, b, c) \in C_{n,3} \subseteq \langle H_{n,3} \rangle \subseteq \langle H_{n+1,3} \rangle,$$

as needed. Therefore, we may assume without loss of generality that $c = n$. Observe that since $\langle H_{n+1,3} \rangle$ is closed under inverses, we may assume that $a < b$. Then

$$(a, b, n) = \begin{cases} (n-2, n-1, n) & \text{if } a = n-2 \text{ and } b = n-1, \\ (a, 0, n-1)(n-1, n, 0)^2(a, n-2, 0) & \text{if } b = n-2, \\ (a, n-2, n-1)(n-2, n-1, n)^2(a, b, n-2) & \text{otherwise,} \end{cases}$$

and all cycles on the right-hand side belong to $C_{n,3} \cup H_{n+1,3} \subseteq \langle H_{n+1,3} \rangle$. Thus, $(a, b, n) \in \langle H_{n+1,3} \rangle$. Therefore, all cycles $(a, b, c) \in C_{n+1,3}$ belong to $\langle H_{n+1,3} \rangle$, as needed. □

Proposition 2.3. *Let n and k be positive integers with $n > k \geq 2$. Then, $H_{n,3} \subseteq \langle H_{n,k} \rangle$.*

Proof. For all $a \in \mathbb{Z}_n$,

$$h_k(a+2)^2 h_k(a) h_k(a+1)^{-1} h_k(a+2)^{-2} = \begin{cases} h_3(a) & \text{if } n > k+1, \\ h_3(a+1) & \text{if } n = k+1, \end{cases}$$

from which the result immediately follows. □

Corollary 2.4. *Let n and k be positive integers with $n > k \geq 2$. If k is odd, then $\langle H_{n,k} \rangle = A_n$, and if k is even, then $\langle H_{n,k} \rangle = S_n$.*

Proof. Observe from Lemma 2.2 and Proposition 2.3 that $C_{n,3} \subseteq \langle H_{n,k} \rangle$. Hence, by Theorem 1.1, $A_n \subseteq \langle H_{n,k} \rangle$. If k is odd, then $\langle H_{n,k} \rangle \subseteq A_n$ and we conclude that $A_n = \langle H_{n,k} \rangle$. On the other hand, if k is even, then $A_n \subsetneq \langle H_{n,k} \rangle$ (since $H_{n,k}$ contains an odd permutation), so $\langle H_{n,k} \rangle = S_n$. □

The aim of the remainder of this article is to shrink the size of the generating set $H_{n,k}$ for A_n (or S_n, if k is even) in Corollary 2.4.

3. Main Result

The main result of this paper is as follows.

Theorem 3.1. *Let n and k be positive integers with $n \geq k \geq 2$ such that $(n,k) \neq (2,2)$ and $(n,k) \neq (3,3)$. If k is odd (respectively, even), then the minimum number of k-cycles needed to generate A_n (respectively, S_n) is*

$$\max\left\{2, \left\lceil \frac{n-1}{k-1} \right\rceil\right\}.$$

According to this result, A_n (respectively, S_n) can be generated by exactly 2 elements if and only if $2 \leq k \leq n \leq 2k-1$ and $(n,k) \neq (2,2)$ and $(n,k) \neq (3,3)$. Therefore, before establishing the full content of Theorem 3.1, let us consider these restrictions on n and k.

Lemma 3.2. *Let n and k be positive integers with $2 \leq k \leq n \leq 2k-1$ and $(n,k) \neq (2,2)$ and $(n,k) \neq (3,3)$. Then if k is odd (respectively, even), then A_n (respectively, S_n) can be generated by two k-cycles.*

Proof. We will use several slightly different cases to prove Lemma 3.2.

Case 1: Suppose $n = k \geq 4$. Let $T := \{h_n(0), (0,1,2,\ldots,n-3,n-1,n-2)\}$. Observe that for all $a = 0,1,2,\ldots,n-1$,

$$h_3(a) = h_n(0)^{a+2}[(0,1,2,\ldots,n-3,n-1,n-2)h_n(0)^{-1}]h_n(0)^{-(a+2)} \in \langle T \rangle.$$

Hence, $H_{n,3} \subseteq \langle T \rangle$. Therefore, by applying Corollary 2.4 (with $k = 3$), we have $A_n = \langle H_{n,3} \rangle \subseteq \langle T \rangle$. If k is odd, then we have $A_n = \langle T \rangle$, and if k is even, we have $S_n = \langle T \rangle$. Since A_n and S_n are not cyclic for $n > 3$, no generating set smaller than T can be found.

Case 2: Suppose $n = k+1$. In what follows, we adopt the notation that

$$\alpha := h_k(0) \quad \text{and} \quad \beta := h_k(k).$$

From the fact that $h_3(k-1) = \beta\alpha^{-1} \in \langle \alpha, \beta \rangle$, we can apply Proposition 2.1 to deduce that

$$\begin{aligned} h_3(k) &= \alpha h_3(k-1)^{-1}\alpha^{-1} \in \langle \alpha, \beta \rangle, \\ h_3(r) &= \beta^{r+1} h_3(k) \beta^{-(r+1)} \in \langle \alpha, \beta \rangle \quad \text{for } 0 \leq r \leq k-4, \\ h_3(k-3) &= \alpha h_3(k-4)\alpha^{-1} \in \langle \alpha, \beta \rangle, \\ h_3(k-2) &= \beta h_3(k-3)^{-1}\beta^{-1} \in \langle \alpha, \beta \rangle, \end{aligned}$$

so we have shown that $H_{n,3} \subseteq \langle \alpha, \beta \rangle$. Proceeding similarly to Case 1 completes Case 2.

Case 3: Suppose $k+2 \leq n \leq 2k-2$. Observe that this requires $k \geq 4$. In the case $k=4$, we only need to consider $n=6$, and note that $\langle (0123), (4051) \rangle = S_6$ by direct verification. Thus, we may assume $k \geq 5$. In this case, we begin by noting that

$$[\alpha, \beta] := \alpha\beta\alpha^{-1}\beta^{-1} = (0,1)(2k-n, k) \in \langle \alpha, \beta \rangle.$$

Therefore, by Proposition 2.1, we obtain

$$\gamma := \alpha^{-2}[\alpha, \beta]\alpha^2 = (k-2, k-1)(2k-n-2, k) \in \langle \alpha, \beta \rangle.$$

Define

$$\mu := \beta^2\gamma\beta^2\gamma\beta^{-4} = (k, k+2, k+4).$$

Direct calculation verifies that we have

$$h_3(0) = \begin{cases} \alpha^2\beta^2\alpha^{-1}\beta^2\alpha^{-1}\beta^{n-k-4}\mu^{-1}\beta^{-(n-k-4)}\alpha\beta^{-2}\alpha\beta^{-2}\alpha^{-2} & \text{if } n \geq k+4, \\ \beta[\mu^{-1}, \alpha^{-1}]\beta^{-1} & \text{if } n = k+3, \\ \alpha^3\beta^{-2}\alpha\beta\alpha^{n-6}\mu\alpha^{6-n}\beta^{-1}\alpha^{-1}\beta^2\alpha^{-3} & \text{if } n = k+2. \end{cases}$$

Conjugating $h_3(0)$ by α^a for $a = 0, 1, 2, \ldots, k-3$ shows that $h_3(a) \in \langle \alpha, \beta \rangle$ for $a = 0, 1, 2, \ldots, k-3$. On the other hand, observe that

$$h_3(n-1) = \begin{cases} \beta^{-1}h_3(0)\beta & \text{if } n < 2k-2, \\ \beta\alpha^{-2}\beta^{-2}h_3(0)\beta^2\alpha^2\beta^{-1} & \text{if } n = 2k-2. \end{cases}$$

Then, conjugating $h_3(n-1)$ by β^{-b} for each $b = 0, 1, 2, \ldots, n-k-1$ shows that $h_3(a) \in \langle \alpha, \beta \rangle$ for each $a = k, k+1, \ldots, n-1$. Furthermore,

$$h_3(k-2) = \beta^{-(n-k)}\alpha h_3(k-3)\alpha^{-1}\beta^{n-k} \quad \text{and}$$
$$h_3(k-1) = \alpha^{n-k}\beta^{-1}h_3(k)\beta\alpha^{-(n-k)}.$$

Thus, $h_3(a) \in \langle \alpha, \beta \rangle$ for all $a = 0, 1, 2, \ldots, n-1$, so that $H_{n,3} \subseteq \langle \alpha, \beta \rangle$, and thus we can complete the proof as in Cases 1 and 2.

Case 4: Suppose $n = 2k-1$. We can easily deduce that $H_{n,k} \subseteq \langle \alpha, \beta \rangle$ as follows:

$$h_k(a) = (\beta\alpha)^a\alpha(\beta\alpha)^{-a} \in \langle \alpha, \beta \rangle$$

for all $a = 0, 1, 2, \ldots, n-1$. Thus, by Corollary 2.4, $\langle \alpha, \beta \rangle = S_n$ if k is even, and $\langle \alpha, \beta \rangle = A_n$ if k is odd.

The above cases complete the verification of Lemma 3.2. □

Before we complete the general proof of Theorem 3.1, let us establish a lower bound on the size of any generating set of A_n (respectively, S_n) that consists exclusively of k-cycles.

Lemma 3.3. *Let n and k be integers with $n \geq k \geq 2$, and let $T \subseteq C_{n,k}$ with $A_n \subseteq \langle T \rangle$. Then,*

$$|T| \geq \left\lceil \frac{n-1}{k-1} \right\rceil .$$

Proof. Consider the graph G whose vertices are $V := \{0, 1, 2, \ldots, n-1\}$ and whose edge set E is defined by the condition that $\{a, b\} \in E$ if and only if there exists $\sigma \in \langle T \rangle$ such that $\sigma(a) = b$. Of course, if $\sigma \in T$, then the k elements of σ belong to the same connected component of G. From this, it is easy to see that the number of connected components of G is at least $n - |T|(k-1)$. Since $A_n \subseteq \langle T \rangle$, the graph G must be connected; hence, G has one connected component. Therefore, $n - |T|(k-1) \leq 1$, from which the conclusion follows. □

Now we are ready to prove Theorem 3.1.

Proof of Theorem 3.1. Lemma 3.2 establishes the result in the case $2 \leq k \leq n \leq 2k-1$ with $(n,k) \neq (2,2)$ and $(n,k) \neq (3,3)$. Therefore, we may assume $2k \leq n$. Note that $\lceil \frac{n-1}{k-1} \rceil \geq 3$. Use the Division Algorithm to find integers d and r such that

$$n - 1 = (k-1)d + r,$$

where $2 \leq d$ and $0 \leq r < k-1$. Define

$$\sigma_t := (0, t(k-1)+1, t(k-1)+2, \ldots, (t+1)(k-1)) \tag{2}$$

for each $t = 0, 1, 2, \ldots, d-1$ and define

$$\sigma_d := (0, d(k-1)+1, d(k-1)+2, \ldots, n-2, n-1, 1, 2, 3, \ldots, k-r-1). \tag{3}$$

Let $T = \{\sigma_0, \sigma_1, \sigma_2, \ldots, \sigma_d\}$. If $r = 0$, then $\sigma_d = \sigma_0$; thus σ_d may be omitted. Note that $|T| = \lceil \frac{n-1}{k-1} \rceil$. We have two cases:

Case 1: $r = 0$.

Define

$$\sigma := \prod_{i=1}^{d} \sigma_{d-i} = (0, 1, 2, \ldots, n-1) \in \langle T \rangle.$$

We can easily see that $H_{n,k} \subseteq \langle T \rangle$ as follows:

$$h_k(a) = \sigma^a \sigma_0 \sigma^{-a},$$

for all $a = 0, 1, 2, \ldots, n-1$. Therefore, by Corollary 2.4, $\langle T \rangle = S_n$ if k is even, or $\langle T \rangle = A_n$ if k is odd.

Case 2: $1 \le r \le k-2$.

Define

$$\sigma := \prod_{i=1}^{d} \sigma_{d-i} = (0, 1, 2, \ldots, d(k-1)) \in \langle T \rangle, \tag{4}$$

and $X := \{0, 1, 2, \ldots, d(k-1)\}$. Since $d \ge 2$, Eq. (4) implies that $\sigma \ne \sigma_0$. Therefore, we can generate all step k-cycles of A_X (respectively, S_X) via:

$$h_k(a) = \sigma^a \sigma_0 \sigma^{-a},$$

for all $a \in X$. Hence, by Corollary 2.4 it follows that $A_X \subseteq \langle T \rangle$ (respectively, $S_X \subseteq \langle T \rangle$). In particular,

$$h_3(s) \in \langle T \rangle \quad \text{for all } s = 0, 1, 2, \ldots, d(k-1) - 2. \tag{5}$$

We also have

$$\tau := (d(k-1) - 1, d(k-1), 0) \in A_X \subseteq \langle T \rangle.$$

The reader may verify that

$$h_3(d(k-1) - 1) = \sigma_d \tau \sigma_d^{-1} \in \langle T \rangle. \tag{6}$$

If $r = 1$, then (5) and (6) together with

$$h_3(n-2) = h_3(n-3)\sigma_d^{-1} h_3(n-3)\sigma_d h_3(n-3)^{-1} \in \langle T \rangle \tag{7}$$

and

$$h_3(n-1) = h_3(n-2)\sigma_d h_3(n-2)^{-1}\sigma_d^{-1} h_3(n-2)^{-1} \in \langle T \rangle \tag{8}$$

imply that $H_{n,3} \subseteq \langle T \rangle$, so that Corollary 2.4 finishes the proof. If $r = 2$, we can use (5)–(8) in conjunction with (9) below to draw the same conclusion:

$$h_3(d(k-1)) = [h_3(d(k-1) - 1)\sigma_d^2]\tau[h_3(d(k-1) - 1)\sigma_d^2]^{-1} \in \langle T \rangle. \tag{9}$$

Next, if $r = 3$, then we use the preceding formulas and

$$h_3(d(k-1) + 1) = [h_3(d(k-1) - 1)\sigma_d] h_3(d(k-1)) [h_3(d(k-1) - 1)\sigma_d]^{-1} \in \langle T \rangle,$$

in the same way. Finally if $4 \le r \le k-2$, then

$$h_3(d(k-1) + i) = \sigma_d^{i-1} h_3(d(k-1) + 1)\sigma_d^{-(i-1)} \in \langle T \rangle$$

for all $2 \le i \le r-2$, so that we once more can apply Corollary 2.4 as in the preceding cases. □

Example 3.4. Let us find an economical generating set consisting only of 5-cycles for A_{274}.

From Theorem 3.1, the fewest number of 5-cycles needed to generate A_{274} is $\lceil \frac{274-1}{5-1} \rceil = 69$. We follow the proof of Theorem 3.1. Note that $2k - 1 \le n$, and observe that with $d = 68$ and $r = 1$,

$$273 = 4d + r.$$

We will define our generators as we did in Eqs. (2) and (3). That is,

$$\sigma_t := (0, 4t + 1, 4t + 2, 4t + 3, 4t + 4),$$

for $t = 0, 1, 2, \ldots, 67$, and

$$\sigma_{68} := (0, 273, 1, 2, 3).$$

Let $T = \{\sigma_t : t = 0, 1, 2, \ldots, 68\}$. Hence, by Theorem 3.1, $\langle T \rangle = A_{274}$.

Example 3.5. Let us find an economical generating set consisting only of 12-cycles for S_{20}.

From Theorem 3.1, we need only two 12-cycles. Note that we are in the case where $k + 2 \le n \le 2k - 2$ in the proof of Lemma 3.2 from which it follows that $S_{20} = \langle \alpha, \beta \rangle$, where

$$\alpha := (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) \quad \text{and}$$

$$\beta := (12, 13, 14, 15, 16, 17, 18, 19, 0, 1, 2, 3).$$

Acknowledgment

The authors gratefully acknowledge the valuable input from the referee which has served to enhance this manuscript.

References

[1] S. Annin, Hierarchy of efficient generators of the symmetric inverse monoid, *Semigroup Forum* **54**(3) (1997) 327–355.

[2] L. Babai *et al.*, On the diameter of finite groups, in *31st Annual Symposium on Foundations of Computer Science*, Vols. I, II (IEEE Computer Society Press, Los Alamitos, CA, 1990), pp. 857–865.

[3] O. Ben-Shimol, The minimal number of cyclic generators of the symmetric and alternating groups, *Commun. Algebra* **35**(10) (2007) 3034–3037.

[4] D. Dummit and R. Foote, *Abstract Algebra*, 3rd edn. (John Wiley & Sons, Hoboken, NJ, 2004), 932 pp.

[5] D. Heath, I. M. Isaacs, J. Kiltinen and J. Sklar, Symmetric and alternating groups generated by a full cycle and another element, *Amer. Math Monthly* **116** (2009) 447–451.

[6] T. Hungerford, *Abstract Algebra: An Introduction*, 2nd edn. (Brooks Cole, Florence, KY, 1996), 608 pp.

[7] R. Nekkoei and A. Jabari, Generating alternating groups, *Algebras Groups Geom.* **20** (2003) 435–442.

[8] R. Stong and B. Suceava, The fewest 3-cycles to generate an even permutation, *Amer. Math. Monthly* **110**(2) (2003) 162.