MATHEMATICAL SCIENCES AND APPLICATIONS E-NOTES
8 (1) 25-28 (2020) ©MSAEN
HTTPS://DOI.ORG/10.36753/MATHENOT.608443

Some Involutions which Generate the Finite Symmetric Group

Leyla Bugay*

Abstract
Let S_n be the symmetric group on $X_n = \{1, \ldots, n\}$ for $n \geq 2$. In this paper we state some properties of subsemigroups generated by two involutions (a permutation with degree 2) α, β such that $\alpha\beta$ is an n-cycle, and then we state some generating sets of S_n which consists of involutions.

Keywords: *Symmetric group; involution; generating set.*

AMS Subject Classification (2020): *Primary: 20B30.*

**Corresponding author*

1. Introduction

Let $X_n = \{1, \ldots, n\}$ for $n \geq 2$, and let S_n be the symmetric group (the group of all permutations) on X_n. Recall from Cayley's theorem for finite groups that every group G is isomorphic to a subgroup of the symmetric group acting on G. Hence the finite symmetric group S_n and its subgroups have an important role in finite group theory and also in finite semigroup theory.

We consider the concept of quasi-idempotent, a bijection α such that $\alpha \neq \alpha^2 = \alpha^4$, as introduced by Garba and Imam in [6], and also studied by Bugay in [2]. Then clearly $\alpha \in S_n$ is a quasi-idempotent if and only if the order of α is 2, and so $\varepsilon \neq \alpha = \alpha^{-1}$ where ε is the identity permutation on X_n. As usual a quasi-idempotent in S_n is also called an *involution*. We denote the set of all involutions in any subset $U \subseteq S_n$ by $I(U)$. As it is well known that the involutions are used for classification of finite simple groups. As emphasized in [9], although there appears to be almost nothing that can be said about the structure of a subgroup generated by two elements of given orders $m \geq 1$ and $n \geq 1$ in any case other than $m = n = 2$, two involutions in any group generate a dihedral subgroup. Moreover, involutions also have an important role for group presentation, since there is no need to use the inverse of any generators in relations since the inverse of any involution is itself.

Let S be a semigroup, and let W be a nonempty subset of S. Then the subsemigroup generated by W, that is the smallest subsemigroup of S containing W, is denoted by $\langle W \rangle$. There are a lot of studies which examine some properties of special kinds of generating sets (see, for example, [1, 4, 5, 7]). In this paper we restrict attention to another special kind of elements, say involutions, which generate S_n.

The *fix* and *shift* of $\alpha \in S_n$ are defined by

$$\begin{aligned} \operatorname{fix}(\alpha) &= \{x \in X_n : x\alpha = x\} \text{ and} \\ \operatorname{shift}(\alpha) &= \{x \in X_n : x\alpha \neq x\} = X_n \setminus \operatorname{fix}(\alpha), \end{aligned}$$

respectively. A permutation $\alpha \in S_n$ with $\operatorname{shift}(\alpha) = \{a_1, \ldots, a_k\}$ $(2 \leq k \leq n)$ is called a *cycle* of size k ($k-$cycle) and denoted by $\alpha = (a_1 \ldots a_k)$ if

$$a_i\alpha = a_{i+1} \quad (1 \leq i \leq k-1) \quad \text{and} \quad a_k\alpha = a_1.$$

Received : *21–08–2019,* ***Accepted :*** *21–02–2020*

In particular, a $2-$cycle (a_1a_2) is called a *transposition*. The identity permutation ε on X_n is expressible as (a), for any $1 \leq a \leq n$, and called a 1-cycle. Two cycles $(a_1 \dots a_k)$ and $(b_1 \dots b_t)$, for $1 \leq k, t \leq n$, are said to be *disjoint* if the sets $\{a_1, \dots, a_k\}$ and $\{b_1, \dots, b_t\}$ are disjoint.

Recall that every permutation can be written as a product of disjoint cycles, more particularly, as a product of transpositions. Also recall that $S_2 = \langle (12) \rangle$, $S_3 = \langle (13), (23) \rangle$, and that $S_n = \langle (12), (12 \dots n) \rangle$ for $n \geq 3$. For unexplained terms see [3, 8] for semigroup theory, and see [9] for group theory. In this paper first we state some properties of subsemigroups generated by two involutions α, β such that $\alpha\beta$ is an n-cycle, and then state some generating sets of S_n consists of involutions.

2. Some involutions which generate S_n

Lemma 2.1. *For two distinct involutions $\alpha, \beta \in I(S_n)$, $\alpha\beta \in I(S_n)$ if and only if $\alpha\beta = \beta\alpha$.*

Proof. ($\Rightarrow$) Let $\alpha\beta \in I(S_n)$ for two distinct involutions $\alpha, \beta \in I(S_n)$. Then we have

$$\alpha\beta = (\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1} = \beta\alpha, \tag{2.1}$$

as required.

($\Leftarrow$) Suppose that $\alpha\beta = \beta\alpha$ for two distinct involutions $\alpha, \beta \in I(S_n)$. Then we have

$$(\alpha\beta)^2 = \alpha(\beta\alpha)\beta = \alpha(\alpha\beta)\beta = \alpha^2\beta^2 = \varepsilon, \tag{2.2}$$

and so the order of $\alpha\beta$ is 2 since $\alpha\beta \neq \varepsilon$. Thus, $\alpha\beta \in I(S_n)$, as required. □

For any $\alpha, \beta \in S_n$, it is well known that $\operatorname{fix}(\alpha) \cap \operatorname{fix}(\beta) \subseteq \operatorname{fix}(\alpha\beta)$, in other words, $\operatorname{shift}(\alpha\beta) \subseteq \operatorname{shift}(\alpha) \cup \operatorname{shift}(\beta)$. Hence, it is easy to see that for any $\alpha \in S_n$

(i) if $\operatorname{fix}(\alpha) \neq \emptyset$ then α^k is not an n-cycle for each $k \in \mathbb{Z}^+$;

(ii) if α is not an n-cycle then α^k is not an n-cycle for each $k \in \mathbb{Z}^+$;

(iii) if α is an n-cycle then $\operatorname{shift}(\alpha^k) = \operatorname{shift}(\alpha) = X_n$ for each $k \in \mathbb{Z} \setminus n\mathbb{Z}$, and $\operatorname{shift}(\alpha^k) = \emptyset$ for each $k \in n\mathbb{Z}$.

Now, for convenience we define a new notation. Let $(b_1, b_2, \dots, b_m)$ be an ordered m-tuple for any $2 \leq m \leq n$. Then let

$$[[b_1, b_2, \dots, b_m]] = \begin{cases} (b_1 b_m)(b_2 b_{m-1}) \cdots (b_{\frac{m}{2}} b_{\frac{m}{2}+1}), & \text{if } m \text{ is an even number} \\ (b_1 b_m)(b_2 b_{m-1}) \cdots (b_{\frac{m-1}{2}} b_{\frac{m+3}{2}}), & \text{if } m \text{ is an odd number} \end{cases} \tag{2.3}$$

where $(b_i\, b_j)$ denotes a 2-cycle for $1 \leq i, j \leq m$.

Lemma 2.2. *For any n-cycle $\pi \in S_n$ let*

$$M(\pi) = \{k \in \mathbb{N} : \pi = \alpha_1 \cdots \alpha_k \,;\, \alpha_i \in I(S_n),\, 1 \leq i \leq k\}. \tag{2.4}$$

Then $\min(M(\pi)) = 1$ for $n = 2$ and $\min(M(\pi)) = 2$ for $n \geq 3$.

Proof. Let $\pi = (a_1 \dots a_n) \in S_n$ be any n-cycle. For $n = 2$ clearly $(a_1a_2) = (12) \in I(S_2)$, as required. For $n \geq 3$ it is also clear that $\pi = (a_1 \dots a_n) \notin I(S_n)$ and so $\min(M(\pi)) \geq 2$. Now consider the maps $\alpha = [[a_1, \dots, a_n]]$ and $\beta = [[a_2, \dots, a_n]]$. Then $\alpha, \beta \in I(S_n)$ and it is easy to check that $\pi = \alpha\beta$, and so $\min(M(\pi)) = 2$, as required. □

Lemma 2.3. *For any $\alpha, \beta \in I(S_n)$ there exists $1 \leq m < n!$ such that*

$$\langle \alpha, \beta \rangle = \{(\alpha\beta)^k, (\beta\alpha)^k, (\alpha\beta)^k\alpha, (\beta\alpha)^k\beta : 1 \leq k \leq m\}. \tag{2.5}$$

Proof. Let $\alpha, \beta \in I(S_n)$ and let U be the set which is on the right side of the above equality. Obviously, $U \subseteq \langle \alpha, \beta \rangle$. Conversely, let $\gamma \in \langle \alpha, \beta \rangle$. Then there exist $p \in \mathbb{Z}^+$ and some integers $0 \leq k_1, \dots, k_p, t_1, \dots, t_p \leq 1$ such that

$$\gamma = \alpha^{k_1}\beta^{t_1}\alpha^{k_2}\beta^{t_2} \cdots \alpha^{k_p}\beta^{t_p}. \tag{2.6}$$

Moreover, if m is the order of $\alpha\beta$, and so of $\beta\alpha$, then $1 \leq m < n!$. Thus we have $\gamma \in U$ since

$$\alpha(\beta\alpha)^k = (\alpha\beta)^k\alpha \text{ and } \beta(\alpha\beta)^k = (\beta\alpha)^k\beta, \tag{2.7}$$

for any $k \in \mathbb{Z}^+$, $\alpha^2 = \beta^2 = \varepsilon$, and since $(\alpha\beta)^m = (\beta\alpha)^m = \varepsilon$, as required. □

Notice that for any $\alpha, \beta \in I(S_n)$, $((\alpha\beta)^k)^{-1} = (\beta\alpha)^k$ for each $k \in \mathbb{Z}^+$. Moreover, for any n-cycle $\pi \in S_n$, π^{-1} is also an n-cycle. Hence we conclude that $(\alpha\beta)^k$ is an n-cycle if and only if $(\beta\alpha)^k$ is an n-cycle for any $\alpha, \beta \in I(S_n)$.

Theorem 2.1. *For any $\alpha, \beta \in I(S_n)$, $\langle \alpha, \beta \rangle$ contains an n-cycle if and only if $\alpha\beta$ (and so $\beta\alpha$) is an n-cycle.*

Proof. First suppose that, for any $\alpha, \beta \in I(S_n)$, $\langle \alpha, \beta \rangle$ contains an n-cycle $\pi \in S_n$. Then notice that, for any $k \in \mathbb{Z}^+$, neither $(\alpha\beta)^k\alpha$ nor $(\beta\alpha)^k\beta$ can be an n-cycle since $((\alpha\beta)^k\alpha)^2 = \varepsilon = ((\beta\alpha)^k\beta)^2$. Thus, $\langle \alpha, \beta \rangle$ contains an n-cycle π if and only if there exists $1 \leq k < n!$ such that $(\alpha\beta)^k = \pi$ or $(\beta\alpha)^k = \pi$ from Lemma 2.3. Then $\alpha\beta$ (and so $\beta\alpha$) is an n-cycle.

The other side of the proof is clear. □

Lemma 2.4. *For any $\alpha, \beta \in I(S_n)$ if $\alpha\beta$ is an n-cycle then*

$$\langle \alpha, \beta \rangle = \{(\alpha\beta)^k, (\alpha\beta)^k\alpha : 1 \leq k \leq n\}. \tag{2.8}$$

Proof. Suppose that, for any $\alpha, \beta \in I(S_n)$, $\alpha\beta$ is an n-cycle. Then, since $(\alpha\beta)^{-1} = \beta\alpha$ and $(\alpha\beta)^{-1} = (\alpha\beta)^{n-1}$, we have

$$\begin{array}{lcll} \beta\alpha & = & (\alpha\beta)^{-1} & = & (\alpha\beta)^{n-1}, \\ (\beta\alpha)^k & = & ((\alpha\beta)^{n-1})^k & = & (\alpha\beta)^{k(n-1)}, \\ (\beta\alpha)^k\beta & = & (\alpha\beta)^{k(n-1)}\beta & = & (\alpha\beta)^{k(n-1)-1}\alpha, \end{array}$$

for each $1 \leq k \leq n$, and since the order of $\alpha\beta$ is n, the result is clear from Lemma 2.3. □

Lemma 2.5. *Let $n \geq 4$ and let $\alpha\beta$ be an n-cycle for any $\alpha, \beta \in I(S_n)$, say $\alpha\beta = (a_1 \dots a_n)$. Then the 2-cycle $(a_i a_{i+1}) \notin \langle \alpha, \beta \rangle$ for each $1 \leq i \leq n$ where $a_{n+1} = a_1$.*

Proof. It is enough to show that $(a_1 a_2) \notin \langle \alpha, \beta \rangle$ since

$$(a_1 \dots a_n) = (a_2\, a_3 \dots a_n\, a_1) = \cdots = (a_n\, a_1 \dots a_{n-1}). \tag{2.9}$$

First notice that neither α nor β can be $(a_1 a_2)$. Otherwise, it must be $\beta = (a_1 a_3 \dots a_n)$ when $\alpha = (a_1 a_2)$ and it must be $\alpha = (a_2 a_3 \dots a_n)$ when $\beta = (a_1 a_2)$, which contradicts with the assumptions $n \geq 4$ and $\alpha, \beta \in I(S_n)$ in both cases. Moreover, since $\operatorname{shift}(\alpha\beta)^k = X_n$ for each $1 \leq k \leq n-1$ and $(\alpha\beta)^n = \varepsilon$ we have $(\alpha\beta)^k \neq (a_1 a_2)$. Now suppose that there exists $1 \leq k \leq n-1$ such that $(\alpha\beta)^k\alpha = (a_1 a_2)$. Then, since

$$(\alpha\beta)^k = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ a_{1+k} & a_{2+k} & a_{3+k} & \cdots & a_{n-1+k} & a_{n+k} = a_k \end{pmatrix},$$

we have

$$\alpha = \begin{pmatrix} a_{1+k} & a_{2+k} & a_{3+k} & \cdots & a_{n-k+k} = a_n & \cdots & a_{n-1+k} & a_{n+k} = a_k \\ a_2 & a_1 & a_3 & \cdots & a_{n-k} & \cdots & a_{n-1} & a_n \end{pmatrix}$$

where $a_{n+1} = a_1, a_{n+2} = a_2, \dots, a_{2n-1} = a_{n-1}, a_{2n} = a_n$. Then we have $a_k\alpha^2 = a_{n-k} = a_k$, and since $\alpha \in I(S_n)$, we have $n = 2k$. However, when $n = 2k$, we have $a_1\alpha^2 = a_2$ which contradicts with the assumption $\alpha \in I(S_n)$. Hence the result follows from Lemma 2.4, as required. □

Lemma 2.6. *Let $n \geq 4$ and let $\alpha\beta$ be an n-cycle for any $\alpha, \beta \in I(S_n)$, say $\alpha\beta = (a_1 \dots a_n)$. Then $\operatorname{shift}(\alpha) \cap \{a_i, a_{i+1}\} \neq \emptyset$ and $\operatorname{shift}(\beta) \cap \{a_i, a_{i+1}\} \neq \emptyset$ for each $1 \leq i \leq n$ where $a_{n+1} = a_1$.*

Proof. Suppose that $n \geq 4$ and $\alpha\beta = (a_1 \dots a_n)$ for any $\alpha, \beta \in I(S_n)$. It is enough to see for $i = 1$ due to similar reasons mentioned in the proof of Lemma 2.5. First assume that $\{a_1, a_2\} \subseteq \operatorname{fix}(\alpha)$. Then, since $a_1\alpha\beta = a_2$ and $a_2\alpha\beta = a_3$, we have $a_1\beta^2 = a_3$ which contradicts with the assumption $\beta \in I(S_n)$. Now assume that $\{a_1, a_2\} \subseteq \operatorname{fix}(\beta)$. Then, since $a_n\alpha\beta = a_1$ and $a_1\alpha\beta = a_2$, we have $a_n\alpha^2 = a_2$ which similarly contradicts with the assumption $\alpha \in I(S_n)$. Therefore $\{a_1, a_2\} \not\subseteq \operatorname{fix}(\alpha)$ and $\{a_1, a_2\} \not\subseteq \operatorname{fix}(\beta)$, as required. □

Corollary 2.1. *Let $n \geq 4$ and let $(a_1 \dots a_n)$ be an arbitrary n-cycle in S_n. Then $\alpha\beta = (a_1 \dots a_n)$ for $\alpha, \beta \in I(S_n)$ if and only if α and β have one of the following n many forms:*

- $\alpha = [[a_1, \dots, a_{k+1}]]\,[[a_{k+2}, \dots, a_n]]$,
  $\beta = [[a_1, \dots, a_{k+2}]]\,[[a_{k+3}, \dots, a_n]]$ $(1 \leq k \leq n-4$ *and* $n \geq 5)$;
- $\alpha = [[a_1, \dots, a_{n-2}]](a_{n-1}a_n)$,
  $\beta = [[a_1, \dots, a_{n-1}]]$;
- $\alpha = [[a_1, \dots, a_{n-1}]]$,
  $\beta = [[a_1, \dots, a_n]]$;
- $\alpha = [[a_1, \dots, a_n]]$,
  $\beta = [[a_2, \dots, a_n]]$;
- $\alpha = [[a_2, \dots, a_n]]$,
  $\beta = (a_1a_2)\,[[a_3, \dots, a_n]]$.

Corollary 2.2. *For $n \geq 4$, $S_n = \langle (a_1a_2), \alpha, \beta \rangle$ for each $\alpha, \beta \in I(S_n)$ with one of the n-many forms given above.*

Proof. The result is clear since $\alpha\beta = (a_1a_2 \dots a_n)$ for each case. □

References

[1] Ayık, G., Ayık, H., Bugay, L., Kelekci, O.: *Generating sets of finite singular transformation semigroups*. Semigroup Forum. 86, 59–66 (2013).

[2] Bugay, L.: *Quasi-idempotent ranks of some permutation groups and transformation semigroups*. Turk. J. Math. 43, 2390-2395 (2019).

[3] Ganyushkin, O., Mazorchuk, V.: Classical finite transformation semigroups. Springer-Verlag. London (2009).

[4] Garba, G. U.: *Idempotents in partial transformation semigroups*. Proc. Royal Soc. Edinburgh. 116A, 359–366 (1990).

[5] Garba, G. U.: *On the idempotent ranks of certain semigroups of order-preserving transformations*. Portugal. Math. 51, 185–204 (1994).

[6] Garba, G. U., Imam, A. T.: *Products of quasi-idempotents in finite symmetric inverse semigroups*. Semigroup Forum. 92, 645–658 (2016).

[7] Howie, J. M.: *Idempotent generators in finite full transformation semigroups*. Proc. Royal Soc. Edinburgh. 81A, 317–323 (1978).

[8] Howie, J. M.: Fundamentals of semigroup theory. Oxford University Press. New York (1995).

[9] Isaacs, I. M.: Finite group theory. American Mathematical Society, Graduate Studies in Mathematics, Volume 92. United States of America (2008).

Affiliations

LEYLA BUGAY
ADDRESS: Department of Mathematics, Çukurova University,
Sarıçam, 01330, Adana, Turkey.
E-MAIL: ltanguler@cu.edu.tr
ORCID ID: 0000-0002-8316-2763