ON GENERATING SETS OF INFINITE SYMMETRIC GROUP

A. V. Semenov* and A. D. Denisova†

UDC 512.5

It is shown that in the group of all bijections of an infinite set, certain families of subsets related to the cardinality of some proper subsets are generating. A criterion for generating an infinite symmetric group by sets of this kind is obtained. As a special case of these results, the number of generating sets of the symmetric group $S(\Omega)$ is described for $\Omega = \mathbb{Z}$. Bibliography: 8 titles.

1. INTRODUCTION

For an arbitrary infinite set $\Omega$, the symmetric group $S(\Omega)$ is a “large” group in the sense that it is difficult to study even particular cases. Thus almost nothing is known about generating sets of this group. George Bergman studied generating sets in some special cases (see [1, Lemmas 1-4]) and proved several statements about this group and its generating sets (see also [1, Theorem 5]). Manfred Droste studied classes of words and chains of subgroups in $S(\Omega)$ in [6–8]. Unfortunately, most of these results are too abstract to be applied to particular problems.

The situation is different for the classification of simpler objects: for example, all normal subgroups of $S(\Omega)$ had been classified (see [2]). There are also known results about the “classical” objects of group theory (see [3,4]).

In the present paper, we consider the problem of generating certain infinite symmetric groups $S(\Omega)$ for arbitrary infinite set $\Omega$. It is shown that in an infinite group of bijections, some families of subsets connected with the number of proper subsets and their structure are generating. We derive a criterion for generating by subsets of this kind, therefore solving a practical problem of generating $S(\Omega)$ for families of subsets of this structure.

2. DEFINITIONS AND KNOWN FACTS

In the present paper, we fix an infinite set $\Omega$, the group $S(\Omega)$ of all bijection of it, and the cardinality $|\Omega|$. For obvious reasons, $\Omega$ stands both for the set and for its cardinality. Also, $I_n$ denotes the set of all elements of order $n$ in $S(\Omega)$.

**Definition 1.** A subset $U \subset \Omega$ is said to be $f$-proper if $f(x) \in U$ for all $x \in U$.

**Definition 2.** Let $M_f$ denote the set of all moved elements of $f \in S(\Omega)$ that is

$$M_f = \{x \in \Omega \mid f(x) \neq x\}.$$

**Definition 3.** Let $W_{\alpha,\beta}(\Omega)$ denote the set of all $f \in S(\Omega)$ such that $M_f$ is a disjoint union of at most $\alpha$ $f$-proper subsets of cardinality less than (or equal to) $\beta$.

**Definition 4.** Let $K_{\alpha,\beta}(\Omega)$ denote the set of all $f \in S(\Omega)$ such that $M_f$ is a disjoint union of $\alpha$ $f$-proper subsets of cardinality less than (or equal to) $\beta$.

**Definition 5.** Let $R_{\alpha,\beta}(\Omega)$ denote the set of all $f \in S(\Omega)$ such that $M_f$ is a disjoint union of at most $\alpha$ $f$-proper subsets of cardinality $\beta$.

*Chebyshev Laboratory, St.Petersburg State University, St.Petersburg, Russia, e-mail: asemenov.spb.56@gmail.com.
†Laboratory for Continuous Mathematical Education, St.Petersburg, Russia, e-mail: leo.denisova@gmail.com.

Translated from Zapiski Nauchnykh Seminarov POMI, Vol. 500, 2021, pp. 177–187. Original article submitted April 8, 2021.
Definition 6. Let $S_{\alpha,\beta}(\Omega)$ denote the set of all $f \in S(\Omega)$ such that $M_f$ is a disjoint union of $\alpha$ $f$-proper subsets of cardinality $\beta$.

Theorem 1 ([1, Theorem 5]). Let $\Omega$ be an infinite set, and let $\{G_i\}_{i \in I}$ be a chain of subgroups of $S(\Omega)$. If $|I| \leq |\Omega|$ and $\bigcup_{i \in I} G_i = S(\Omega)$, then there exists an index $i$ such that $G_i = S(\Omega)$ for all $j \geq i$.

Theorem 2 (Schreier–Ulam, [2, Sec. 8]). For any normal subgroup $H \leq S(\Omega)$, there exists a cardinal $\alpha$ such that $H = S_{\alpha}(\Omega) = \{f \in S(\Omega) \mid |M_f| \leq \alpha \leq \Omega\}$.

3. Study of $W_{\alpha,\beta}(\Omega)$

The question on minimal generating sets does not arise because of the following almost trivial result.

Theorem 3. $S(\Omega)$ has no minimal generating subset.

Proof. Assume on the contrary that there exists a set $S$ which is at least countable. Then it has a countable subset $A = \{a_1, a_2, a_3, \ldots\}$. Put $S_0 = S \setminus A$, $S_1 = S_0 \cup \{a_1\}$, and $S_n := S_{n-1} \cup \{a_n\}$.

Note that $\langle S_0 \rangle \subseteq \langle S_1 \rangle \subseteq \langle S_2 \rangle \subseteq \cdots \subseteq S(\Omega)$, and any set in this chain is not the entire group. However, $\bigcup_{i=0}^{\infty} S_i = S(\Omega)$ which contradicts the previous theorem. Hence, $S(\Omega)$ has no minimal generating subset.

Despite this result, one can study almost arbitrary sets connected with orbits of the action of $S(\Omega)$ on $\Omega$. Let us describe the “largest” set $W_{\alpha,\beta}(\Omega)$.

Theorem 4. For any cardinals $\alpha, \beta$ such that $\alpha \cdot \beta < \Omega$, the set $W_{\alpha,\beta}(\Omega)$ is not generating for $S(\Omega)$.

Proof. Fix arbitrary cardinals $\alpha, \beta$ smaller than $\Omega$. Without loss of generality, we may assume that $\alpha > \beta$. Fix a permutation $f \in W_{\alpha,\beta}(\Omega)$. Then $M_f$ can be obtained as a union of less than $\alpha$ $f$-proper subsets of cardinality smaller than that of $\beta$. Also, the cardinality of $M_f$ is less than $\alpha \cdot \beta = \alpha$. Hence, $f \in S_{\alpha}(\Omega)$. Thus, $W_{\alpha,\beta}(\Omega) \subseteq S_{\alpha}(\Omega)$, which is not a generating set, because $\alpha < \Omega$.

Lemma 1. $W_{\Omega,\alpha}(\Omega)$ is a subset of $W_{\Omega,\beta}(\Omega)$ for any cardinals $\alpha < \beta < \Omega$.

Proof. Fix $\alpha < \beta$ and $f \in W_{\Omega,\alpha}(\Omega)$. The cardinality of any $f$-proper subset is not greater than $\alpha$, and hence is not greater than $\beta$. Thus, $f \in W_{\Omega,\beta}(\Omega)$.

Lemma 2. $W_{\beta,\Omega}(\Omega) \subseteq W_{\alpha,\Omega}(\Omega)$ for any cardinals $\alpha < \beta$.

Proof. Fix $\alpha < \beta$ and $f \in W_{\beta,\Omega}(\Omega)$. Obviously, $M_f = \bigcup_{1 \leq \beta} V_f$, where the $V_f$ are $f$-proper subsets of cardinality not greater than that of $\Omega$. Since $V = \bigcup_{1 \leq \beta} V_f$ is an $f$-proper subset itself, we have $f \in W_{\alpha,\Omega}(\Omega)$, because $1 \leq \alpha$ and $|V| < \Omega$.

Theorem 5 (Criterion for $W_{\alpha,\beta}(\Omega)$). The set $W_{\alpha,\beta}(\Omega)$ is generating for $S(\Omega)$ if and only if at least one of the cardinals $\alpha, \beta$ is equal to $\Omega$.

Proof. In order to prove the first statement, let $W_{\alpha,\beta}(\Omega)$ generate $S(\Omega)$. Assume that $\alpha < \Omega$ and $\beta < \Omega$. By Theorem 4, $|S(\Omega)| = |W_{\alpha,\beta}(\Omega)| < |S(\Omega)|$, which contradicts the assumption.

On the other hand, let $\alpha = \Omega$ or $\beta = \Omega$. From Lemmas 1 and 2, it follows that $I_2 = W_{\Omega,2} \subseteq W_{\alpha,\beta}$, and $I_2$ is a generating set by Theorem 8. Then

$$S(\Omega) = \langle I_2 \rangle \subseteq \langle W_{\alpha,\beta}(\Omega) \rangle \subseteq S(\Omega),$$

and the set $W_{\alpha,\beta}(\Omega)$ is generating.

465
4. Study of $S_{\alpha,\beta}(\Omega)$

Let us consider the smallest of the sets described in Sec. 1.

**Lemma 3.** $S_{\beta,\Omega}(\Omega) \subseteq S_{\alpha,\Omega}(\Omega)$ for any cardinals $\alpha < \beta$.

**Proof.** Let $\alpha < \beta$ be cardinals and fix $f \in S_{\beta,\Omega}(\Omega)$. It is easy to see that $M_f = \bigcup_{\Omega} V_f$, where the $V_f$ are $f$-proper subsets of cardinality equal to that of $\Omega$. Since $\alpha < \beta$, there exists $\gamma < \Omega$ such that $\beta = \alpha + \sum_{\gamma} \alpha$. Then $M_f$ can be obtained as $(\bigcup V_f) \cup (\bigcup V_f)$, i.e., as a union of $\alpha$ $f$-proper subsets. Since $|\bigcup V_f| = \sum_{\gamma} \alpha = \Omega$, it follows that $f \in S_{\alpha,\Omega}(\Omega)$. $\square$

**Lemma 4.** $S_{\Omega,\alpha}(\Omega) \subseteq S_{\Omega,\beta}(\Omega)$ for any infinite cardinals $\alpha < \beta$.

**Proof.** Fix $\alpha < \beta$ and $f \in S_{\Omega,\alpha}(\Omega)$. Obviously, $M_f = \bigcup_{\Omega} V_f$, where the $V_f$ are $f$-proper subsets each of cardinality $\alpha$. Observe that $\Omega$ can be obtained as $\alpha \cdot \beta \cdot \Omega$. Hence, $M_f = \bigcup_{\Omega} \bigcup_{\beta} V_f$, where the cardinality of any $V_f$ is equal to $\alpha$ and $\bigcup V_f$ is an $f$-proper subset of cardinality equal to that of $\beta$. Then $f \in S_{\Omega,\beta}(\Omega)$ by definition. $\square$

**Theorem 6.** $\langle I_n \rangle \subseteq \langle S_{\Omega,n}(\Omega) \rangle$ for any $n \geq 2$.

**Proof.** It is sufficient to prove that any permutation of order $n$ can be obtained as a finite composition of permutations of $S_{\Omega,n}(\Omega)$.

Fix $n \in \mathbb{N}$ and $f \in I_n$. Consider two cases depending on whether $|M_f| = \Omega$ or $|M_f| < \Omega$.

The first case is obvious by definition (because $M_f$ can be obtained as $\Omega$ $f$-proper subsets each of cardinality $n$).

In the second case, we can take $g_1 \in S_{\Omega,n}$ such that $g_1|_{M_f} = f$. Observe that $|M_{g_1 \setminus M_f}| = \Omega$, because $|M_f| < \Omega$. Hence, $M_{g_1 \setminus M_f}$ can be obtained as a disjoint union of $f$-proper subsets of cardinality $n$. One can construct a function $g_2$ such that $g_2|_{M_{g_1 \setminus M_f}} = g_1^{-1}$ and $g_2|_{M_f} = \text{id}_\Omega$. Obviously $g_2$ also lies in $S_{\Omega,n}(\Omega)$. Hence the composition of $g_1$ and $g_2$ equals $f$, and $f \in \langle S_{\Omega,n}(\Omega) \rangle$. $\square$

**Lemma 5.** $S_{\Omega,2}(\Omega) \subseteq S_{\Omega,\alpha}(\Omega)$ for any infinite cardinal $\alpha$.

**Proof.** Let $f \in S_{\Omega,2}(\Omega)$. Then $M_f = \bigcup_{\Omega} V_f$, where the $V_f$ are $f$-proper subsets of cardinality 2. Since $2 < \alpha < \Omega$, $\Omega$ can be obtained as $\Omega \cdot (\alpha \cdot 2)$. Then $M_f = \bigcup_{\Omega} \bigcup_{\alpha} V_f$, where the cardinality of any $V_f$ is equal to 2 and $\bigcup V_f$ is an $f$-proper subset of cardinality $\alpha$. Hence, $f \in S_{\Omega,\alpha}(\Omega)$. $\square$

**Theorem 7** (Criterion for $S_{\alpha,\beta}(\Omega)$). The set $S_{\alpha,\beta}(\Omega)$ is generating for $S(\Omega)$ if and only if at least one of the cardinals $\alpha, \beta$ is equal to $\Omega$.

**Proof.** The first statement follows from Theorem 4, because if $\alpha \cdot \beta < \Omega$, then $S_{\alpha,\beta}(\Omega)$ cannot be a generating set.

From Lemma 5 and Theorem 6, it follows that $\langle I_2 \rangle \subseteq \langle S_{\Omega,2}(\Omega) \rangle \subseteq \langle S_{\Omega,\beta}(\Omega) \rangle$ for any infinite cardinal $\beta$, and $I_2$ is a generating set by Theorem 8. Then $S_{\Omega,\beta}(\Omega)$ is a generating set for any infinite $\beta$. Since $S_{\Omega,\Omega}(\Omega) \subseteq S_{\Omega,\alpha}(\Omega)$, Lemma 4 implies that the set $S_{\alpha,\Omega}(\Omega)$ is generating for any cardinal $\alpha$.

Finally, if $\beta$ is a natural number, then $\langle I_\beta \rangle \subseteq \langle S_{\Omega,\beta}(\Omega) \rangle$ by Theorem 6, and $I_\beta$ is a generating set by Theorem 8 proved in Sec. 5. $\square$
5. The main result

**Theorem 8.** \( I_n = S(\Omega) \) for any \( n \in \mathbb{N} \).

**Proof.** It is easily seen that the normal closure of \( I_n \) coincides with the subgroup generated by \( I_n \),

\[
I_n = \langle I_n^S(\Omega) \rangle = \langle \{gs_s^{-1} \mid s \in I_n \} \rangle = \langle I_n \rangle.
\]

Assume that \( \langle I_n \rangle < S(\Omega) \). By the Schrier-Ulam Theorem, there exists a cardinal \( \alpha < \Omega \) such that \( \langle I_n \rangle = S_{\alpha}(\Omega) \). However this contradicts the fact that there exists a permutation \( f \in I_n \) such that \( M_f = \Omega \), which is impossible by definition. \( \square \)

**Theorem 9.** The following statements hold:

1. \( W_{\alpha,\beta}(\Omega), R_{\alpha,\beta}(\Omega), K_{\alpha,\beta}(\Omega), S_{\alpha,\beta}(\Omega) \) are not generating sets for any \( \alpha \cdot \beta < \Omega \),
2. \( W_{\alpha,\Omega}(\Omega), R_{\alpha,\Omega}(\Omega), K_{\alpha,\Omega}(\Omega), S_{\alpha,\Omega}(\Omega) \) are generating sets for any \( \alpha \leq \Omega \),
3. \( W_{\Omega,\beta}(\Omega), R_{\Omega,\beta}(\Omega), K_{\Omega,\beta}(\Omega), S_{\Omega,\beta}(\Omega) \) are generating sets for any \( \beta \leq \Omega \).

**Proof.** Fix \( \alpha, \beta \). By definition, we have

\[
S_{\alpha,\beta}(\Omega) \subseteq K_{\alpha,\beta}(\Omega) \subseteq W_{\alpha,\beta}(\Omega) \quad \text{and} \quad S_{\alpha,\beta}(\Omega) \subseteq R_{\alpha,\beta}(\Omega) \subseteq W_{\alpha,\beta}(\Omega).
\]

Then the first case follows from Theorem 4 and the second and third cases follow from Theorem 7. \( \square \)

6. Special case \( \Omega = \mathbb{Z} \)

The case of a countable set is especially interesting, because here we can deal with permutations acting on \( \Omega \) as cycles. This is strengthening of our definitions as will be shown below and requires a separate study. We consider the orbits (cycles) \( O_f(x) = \{f^k(x) \mid k \in \mathbb{Z}\} \) and define the following three sets.

1. A set of all local finite permutations
   \[ LF = \{f \in S(\Omega) \mid \text{the cycle } O_f(x) \text{ is finite for all } x \in \Omega\}. \]
   An example is the permutation \( \ldots (12)(34)(56) \ldots \)

2. A set of all ringed permutations
   \[ R = \{f \in S(\Omega) \mid \text{the set of all the orbits of } f \text{ is finite}\}. \]
   An example is the permutation \( f(n) = n + 1 \).

3. A set of all wild permutations
   \[ W = \{f \in S(\Omega) \mid \text{there are infinitely many countable cycles } O_f(x)\}. \]
   A typical example is obtained by a partition of \( \mathbb{Z} \) into an infinite union of countable sets.

**Lemma 6.** \( R \subseteq \langle LF \rangle \).

**Proof.** It suffices to prove that an infinite cycle can be obtained by the composition of locally finite functions. Without loss of generality, we may assume that \( f \in R \) consists of exactly one infinite cycle. Then

\[
f = (\ldots f^{-2}(x_0), f^{-1}(x_0), x_0, f(x_0), f^2(x_0), \ldots).
\]

Let \( f_1, f_2 : \Omega \rightarrow \Omega \) be locally finite functions, such that

\[
f_1(f^n(x_0)) = f^{-n-1}(x_0) \text{ and } f_2(f^n(x_0)) = f^{-n}(x_0) \text{ for an integer } n,
\]

and they are identical on the complement of this cycle.
In order to prove the statement, we need to show that $f^n(x_0)$ goes to $f^{n+1}(x_0)$ under the composition $f_1f_2$ for all $n \in \mathbb{Z}$. But it is easily seen that

$$f_2(f_1(f^n(x_0))) = f_2(f^{-n-1}(x_0)) = f^{n+1}(x_0).$$

Hence, $f = f_1f_2 \in \langle LF \rangle$.

\textbf{Lemma 7.} $I_2 \subseteq \langle R \rangle$.

\textit{Proof.} Fix $f \in I_2$ and consider two cases depending on whether $f$ is equal to a union of infinitely many or finitely many transpositions.

In the first case,

$$f = (x_1^1, x_2^1)(x_2^2, x_3^1)(x_3^2, x_4^1)(x_4^2, x_5^1) \ldots$$

We may assume that $f$ does not contain a cycle of order 1: otherwise one can add to $g_1$ (this function will be described later) a set of all the fixed elements of $f$ as a cycle, and add the cycle inverted to $g_2$. Let us define two ringed functions $g_1, g_2$ as follows:

$$g_1 = (\ldots x_3^2, x_4^1, x_2^1, x_3^1, x_1^2),$$

$$g_2 = (\ldots x_3^2, x_4^1, x_2^1, x_3^1, x_1^2, x_3^1, x_4^1, \ldots).$$

It is straightforward to check that $g_1g_2 = f$.

In order to obtain $f$ in the second case, we only need to construct a function $g_1$ which consists of infinitely many transpositions and such that the set of orbits of $f$ lies in the set of orbits of $g_1$, and also to construct a function $g_2$ such that $M_{g_1} \setminus M_{g_2} = M_f$ and $M_{g_2} \cup M_f = M_{g_1}$. Obviously, the composition $g_1g_2$ is equal to $f$. Hence, $f$ can be obtained as a finite composition of ringed functions.

\textbf{Lemma 8.} $LF \subseteq \langle W \rangle$.

\textit{Proof.} Fix $f \in LF$, and let $f$ be not finite. We need to prove that $f \in \langle W \rangle$.

Consider two cases depending on whether $\Omega \setminus M_f$ is finite or infinite. In the first case $f$, can be obtained as a composition of four wild permutations. In order to prove this, we only need to understand how a finite cycle $(x_1, x_2, \ldots, x_n)$ can be obtained. Let us take two infinite cycles

$$(\ldots a_{-1}, a_0, x_1, x_2, \ldots, x_n, a_1, a_2, \ldots)$$

and

$$(\ldots, a_2, a_1, x_n, a_0, a_{-1}, \ldots),$$

where the $a_i$ are some elements outside the cycle. Obviously the number of such elements is infinite. Let us enumerate the cycles of $f$, whose length is greater than 2 by integers (we can do this in any case, because all of the orbits are finite and hence the number of cycles is infinite, and the number of cycles of cardinality greater than 2 is also infinite, because $f$ is not finite).

We define functions $g_1, g_2$ as follows. The set of all elements of even cycles (it is, obviously, an infinite set) is a disjoint infinite union of infinite subsets. For any odd cycle $(x_1, x_2, \ldots, x_n)$, we fix only one of these (infinite) sets and take the $a_i$ from this set. The functions $g_1$ and $g_2$ consist of cycles $(\ldots a_{-1}, a_0, x_1, x_2, \ldots, x_n, a_1, a_2, \ldots)$ and $(\ldots, a_2, a_1, x_n, a_0, a_{-1}, \ldots)$, respectively. In this way, we “eliminate” all odd cycles.

Then one needs to construct functions $h_1, h_2$, by the same rule: we need to “eliminate” all even cycles by using elements from odd cycles as the $a_i$. These functions are wild, because they consist of infinitely many cycles (one cycle for one orbit, and the number of the orbits is infinite), and all these cycles are countable by construction. Thus, $h_i \in W, g_i \in W$, and

$$f = h_1h_2g_1g_2.$$
In the second case, one can obtain \( f \) by the composition of two wild functions: indeed, since \( \Omega \setminus M_f \) is infinite, one can take the \( a_i \) from this set.

Finally, in the exceptional case of finite \( f \), this algorithm gives us only ringed functions (there are only finitely many cycles of length greater than 2). To construct wild functions from them, one needs to add infinitely many cycles of the elements of \( \Omega \setminus M_f \) to \( g_1 \) and all the cycles inverse to them to \( g_2 \).

\[ \square \]

**Theorem 10.** Let \( \Omega \) be a countable set. Then each of the sets \( LF, R \) and \( W \) generates \( S(\Omega) \).

**Proof.** Be the previous lemmas, \( \langle I_2 \rangle \subseteq \langle R \rangle \subseteq \langle LF \rangle \subseteq \langle W \rangle \subseteq S(\Omega) \), and \( \langle I_2 \rangle = S(\Omega) \) by Theorem 8, whence the result follows. \[ \square \]

The first author was partially supported by the Young Russian Mathematics Prize and by a social investment program “Native Towns”, PJSC “Gazprom Neft”.

Translated by the authors.

**REFERENCES**

1. G. M. Bergman, “Generating infinite symmetric groups,” *Bull. London Math. Soc.*, 38, 429–440 (2006).
2. J. D. Dixon and B. M. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, Springer (1988).
3. F. Galvin, “Generating countable sets of permutations,” *J. London Math. Soc.* (2), 51, 230–242 (1995).
4. D. Macpherson and P. M. Neumann, “Subgroups of infinite symmetric groups,” *J. London Math. Soc.* (2), 64–84 (1990).
5. G. Moran, “Conjugacy classes whose square is an infinite symmetric group,” *Trans. Amer. Math. Soc.*, 316, 493–522 (1989).
6. M. Droste and W. Ch. Holland, “Generating automorphism groups of chains,” *Forum Math.*, 17, No. 4, 699–710 (2005).
7. M. Droste, “Classes of universal words for the infinite symmetric groups,” *Algebra Universalis*, 20, 205–216 (1985).
8. M. Droste and R. Gobel, “Uncountable cofinalities of permutation groups,” *J. London Math. Soc.* (2) 71, 335–344 (2005).