Séminaire Lotharingien de Combinatoire **65** (2011), Article B65b

GENERATOR SETS FOR THE ALTERNATING GROUP

AVIV ROTBART[†]

Abstract. Although the alternating group is an index 2 subgroup of the symmetric group, there is no generating set that gives a Coxeter structure on it. Various generating sets were suggested and studied by Bourbaki, Mitsuhashi, Regev and Roichman, Vershik and Vserminov, and others. In a recent work of Brenti, Reiner and Roichman, it is explained that palindromes in Mitsuhashi's generating set play a role similar to that of reflections in a Coxeter system.

We study in detail the length function with respect to the set of palindromes. Results include an explicit combinatorial description, a generating function, and an interesting connection to Broder's restricted Stirling numbers.

1. Introduction

The study of parameters (statistics) of the symmetric group and other related groups is a very active branch of combinatorics in recent years. A major step was made about one hundred years ago, when MacMahon [6] showed that the parameters *major index* and *inversion number* are equi-distributed on the symmetric group, S_n. This important result is the foundation of the field, and stimulated many subsequent generalizations and refinements.

It is well known that several statistics on S_n may be defined via its Coxeter generators (simple reflections) $\{s_i = (i, i{+}1) \mid 1 \le i \le n{-}1\}$, or via the transpositions (reflections) $\{t_{ij} = (i, j) \mid 1 \le i < j \le n\}$. Unfortunately, the alternating group $A_n \subseteq S_n$ is not a Coxeter group. Our goal is to study generating sets for the alternating group that play a role similar to that of reflections in the symmetric group, and to explore the combinatorial properties of A_n based on these sets.

A good candidate is the set $\{s_1 s_{i+1} = (1, 2)(i{+}1, i{+}2) \mid 1 < i < n{-}1\}$. Mitsuhashi [7] pointed out that these generators for the alternating group play a role similar to that of the above Coxeter generators of S_n. Regev and Roichman [8] describe a canonical presentation of the elements in A_n based on this set. They also calculate the generating functions of length and other statistics, with respect to this set of generators.

Our work deals with A_n-statistics calculated with respect to a new set of generators, $\{s_1 t_{ij} = (1, 2)(i, j) \mid 1 \le i < j \le n\}$. This set consists of palindromes in Mitsuhashi's generators discussed above. As Brenti, Reiner and Roichman [3] explain, these palindromes play a role similar to that of reflections in the symmetric group. The following diagram describes the relations between the four generating sets mentioned above.

[†] Department of Mathematics, Bar-Ilan University, Ramat Gan 52900, Israel.
Email: `aviv.rotbart@gmail.com`.

This paper is part of the author's MSc thesis, which was written at Bar-Ilan University under the supervision of Prof. R. M. Adin and Prof. Y. Roichman.

$$\begin{tikzcd}
\begin{array}{c} S_n\text{-Coxeter} \\ C = \{s_i \mid 1 \leq i \leq n-1\} \end{array} \arrow[r, "\text{conjugate by } S_n"] \arrow[d, "\text{multiply by } s_1"] & \begin{array}{c} S_n\text{-Transpositions} \\ T = \{t_{ij} \mid 1 \leq i < j \leq n\} \end{array} \arrow[d, "\text{multiply by } s_1"] \\
\begin{array}{c} A_n\text{-Coxeter (Mitsuhashi)} \\ C(A_n) = \{s_1 s_{i+1} \mid 1 < i \leq n-1\} \end{array} \arrow[r, "\text{take palindromes}"] & \begin{array}{c} A_n\text{-Transpositions} \\ T(A_n) = \{s_1 t_{ij} \mid 1 \leq i < j \leq n\} \end{array}
\end{tikzcd}$$

Various aspects of the generating set $T(A_n)$ are studied in this work, including: canonical forms of elements in A_n with respect to $T(A_n)$; length of elements and the relation between length and number of cycles; a generating function for length expectation and variance for length; and finally a connection with Broder's restricted Stirling numbers [2].

The methods used in this work include: manipulations on generating functions of Stirling numbers; theorems on the number of cycles of a permutation and on the number of permutations of a given length in S_n; bijections between certain subsets of permutations in A_n, S_n and permutations with Broder's property (see Definition 2.13).

The paper is organized as follows. Detailed background and notations for the symmetric and alternating groups, as well as for Stirling numbers, is given in Section 2. In Section 3 we present the main results achieved in this work. The A canonical presentation is analyzed in Section 4. In Section 5 we discuss refined counts of permutations in A_n, while the relation between length and the number-of-cycles statistic is analyzed in Section 6. In Section 7 we calculate the generating function of length with respect to the generating set $T(A_n)$. The expectation and variance of the length function are studied in Section 8. The relation between our results and restricted Stirling numbers is analyzed in Section 9.

2. Background

2.1. **The Symmetric Group.**

In this subsection, we present the main notations, definitions and theorems on the symmetric group, denoted by S_n.

Notation 2.1. Let n be a nonnegative integer, then $[n] := \{1, 2, 3, \dots, n\}$ (where $[0] := \emptyset$).

Definition 2.2. Denote by $\mathbb{N}$ the set of natural numbers. The *symmetric group* on $n \in \mathbb{N}$ letters (denoted by S_n) is the group consisting of all permutations on n letters, with composition as the group operation.

Definition 2.3. Given a permutation $v \in S_n$, we say that a pair $(i, j) \in [n] \times [n]$ is an *inversion* of v if $i < j$ and $v(i) > v(j)$. If $(i, i+1)$ is a transposition of v, then it is called an *adjacent transposition.*

Definition 2.4. The *Coxeter generators* of S_n are

$$\{s_i = (i, i+1) \mid 1 \leq i \leq n-1\},$$

i.e., all the adjacent transpositions.

It is a well-known fact that the *symmetric group* is a *Coxeter group* with respect to the above generating set. The following natural statistic describes the length of permutations in the symmetric group, with respect to the Coxeter generating set:

Definition 2.5. The *length* of a permutation $v \in S_n$ with respect to the Coxeter generators is defined to be

$$\ell_C(v) := \min\{\ r \geq 0 \mid v = s_{i_1} \dots s_{i_r} \text{ for some } i_1, \dots, i_r \in [n-1]\ \}.$$

Definition 2.6. The *inversion number* of $v \in S_n$ is

$$inv(v) := |\{(i,j) \mid 1 \leq i < j \leq n,\ v(i) > v(j)\}|.$$

Fact 2.7. *For each $v \in S_n$, we have*

$$inv(v) = \ell_C(v).$$

Another important set of generators for S_n is the set of all transpositions.

Notation 2.8. Denote by T the set of all transpositions in S_n, i.e.,

$$T = \{(i,j) \mid 1 \leq i < j \leq n\}.$$

The definition of length with respect to T is similar.

Definition 2.9. Let $v \in S_n$, then

$$\ell_T(v) := \min\{\ r \geq 0 \mid v = t_1 \dots t_r, \quad t_i \in T\ \}.$$

A well known result describes the connection between the number of cycles and this length statistics in S_n.

Theorem 2.10. *If $cyc(v)$ is the number of cycles in $v \in S_n$, then*

$$\ell_T(v) + cyc(v) = n$$

This result will be useful in some of the proofs in this work.

2.2. **The Alternating Group.** In this section we define the alternating group, which is a subgroup of the symmetric group. We also describe a known generating set for this group and the corresponding generating function of length.

Definition 2.11. The *Alternating Group* on n letters, denoted by A_n, is the group consisting of all even permutations in the symmetric group S_n; i.e., $A_n := \{v \in S_n \mid sign(v) = 1\}$.

Following Mitsuhashi [7] we let

$$a_i := s_1 s_i = (1,2)(i,i+1) \qquad (2 \leq i \leq n-1).$$

The set $C(A_n) := \{a_i \mid 2 \leq i \leq n-1\}$ generates the alternating group on n letters, A_n.

Regev and Roichman [8] used Mitsuhashi's generators to describe a covering map $f : A_{n+1} \to S_n$, which allows us to translate S_n-identities into corresponding A_{n+1}-identities. They gave a formula for the generating function of length with respect to these generators.

Proposition 2.12 ([8, Thm. 6.1]). *Denoting by $\ell_{C(A_n)}(\cdot)$ is the length with respect to Mitsuhashi's generators, we have*

$$\sum_{w \in A_{n+1}} q^{\ell_{C(A_n)}(w)} = (1+2q)(1+q+2q^2)\cdots(1+q+\ldots+q^{n-2}+2q^{n-1}).$$

2.3. **Stirling Numbers.** For basic properties of Stirling numbers the reader is referred to [9]. In this subsection we describe one important generalization of them, Broder's [2] restricted Stirling numbers.

Definition 2.13. The unsigned r-restricted Stirling number of the first kind, denoted by $\left[{n \atop k}\right]_r$, is the number of permutations of the set $\{1, 2, \ldots, n\}$ with k disjoint cycles, with the restriction that the numbers $1, 2, \ldots, r$ belong to distinct cycles. The case $r = 1$ gives the usual unsigned Stirling numbers of the first kind.

Definition 2.14. The Kronecker delta function is defined as follows:

$$\delta_{i,j} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}$$

Claim 2.15. *r-Stirling numbers of the first kind satisfy the same recurrence relation as unsigned Stirling numbers of the first kind, except for the initial conditions:*

$$\begin{bmatrix} n \\ k \end{bmatrix}_r = (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix}_r + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_r, \qquad (r < k < n),$$

with the following initial conditions:

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_r &= 0, & & (k < r \text{ or } n < k); \\ \begin{bmatrix} n \\ r \end{bmatrix}_r &= \frac{(n-1)!}{(r-1)!}, & & (r \le n); \\ \begin{bmatrix} n \\ n \end{bmatrix}_r &= 1, & & (r \le n). \end{aligned}$$

Theorem 2.16 ([2, §6.9]). *The generating function of unsigned r-restricted Stirling numbers of the first kind is*

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_r \cdot x^k = \begin{cases} x^r(x+r)(x+r+1)\cdots(x+n-1) & \text{if } 1 \le r \le n; \\ 0 & \text{otherwise.} \end{cases}$$

Definition 2.17. The r-restricted Stirling number of the second kind, denoted by $\left\{{n \atop k}\right\}_r$, is the number of ways to partition the set $\{1, 2, \ldots, n\}$ into k nonempty disjoint subsets with the restriction that the numbers $1, 2, \ldots, r$ belong to distinct subsets. The case $r = 1$ gives the usual Stirling numbers of the second kind.

Claim 2.18. *r-restricted Stirling numbers of the second kind satisfy the same recurrence relation as Stirling numbers of the second kind, except for the initial conditions.*

$$\begin{Bmatrix} n \\ k \end{Bmatrix}_r = k \cdot \begin{Bmatrix} n-1 \\ k \end{Bmatrix}_r + \begin{Bmatrix} n-1 \\ k-1 \end{Bmatrix}_r, \qquad (r < k < n),$$

with the following initial conditions:

$$\left\{ {n \atop k} \right\}_r = 0, \qquad (k < r \text{ or } n < k);$$

$$\left\{ {n \atop k} \right\}_r = r^{n-r}, \qquad (r \leq n);$$

$$\left\{ {n \atop n} \right\}_r = 1, \qquad (r \leq n).$$

Theorem 2.19 ([2, §6.10])**.** *The generating function of r-restricted Stirling numbers of the second kind is*

$$\sum_{n=0}^{\infty} \left\{ {n \atop k} \right\}_r \cdot x^n = \begin{cases} \frac{x^k}{(1-rx)(1-(r+1)x)\cdots(1-kx)}, & \text{if } 1 \leq r \leq k; \\ 0, & \text{otherwise.} \end{cases}$$

Restricted Stirling numbers of the first and second kind satisfy the same orthogonality relation as the usual (unsigned) Stirling numbers, as described in the following theorem.

Theorem 2.20 ([2, §4.5])**.** *We have*

$$\sum_{k=0}^{n} \left[{n \atop k} \right]_r \cdot \left\{ {k \atop m} \right\}_r \cdot (-1)^k = \begin{cases} (-1)^n \cdot \delta_{m,n}, & \text{if } r \leq m \leq n; \\ 0, & \text{otherwise.} \end{cases}$$

2.4. **Harmonic Numbers.**

Definition 2.21. The *n-th harmonic number*, denoted by H_n, is the sum of the reciprocals of the first n positive integers:

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Definition 2.22. The *generalized n-th harmonic number of order m*, denoted by $H_{n,m}$, is

$$H_{n,m} = 1 + \frac{1}{2^m} + \frac{1}{3^m} + \cdots + \frac{1}{n^m}.$$

3. Main Results

In this section we present the main results of this paper. Details and proofs will be given in Sections 4–8.

Let

$$a_{ij} := s_1 t_{ij} = (12)(ij), \qquad (1 \leq i < j \leq n).$$

The set of *A-transpositions*

$$T(A_n) := \{a_{ij} \mid 1 \leq i < j \leq n\}$$

generates the alternating group on n letters. The length of an element $v \in A_n$ can be naturally defined with respect to the above generators:

$$\ell_{T(A_n)}(v) = \min\{k \geq 0 \mid v = v_1 \cdots v_k, \quad v_i \in T(A_n)\}.$$

Notation 3.1. Denote by $a(n,m)$ the number of elements of length m in A_n.

Our first result is a Stirling-type recursion for $a(n,m)$.

Proposition 3.2 (*Corollary 5.4*).

$$a(n,m) = (n-1)\cdot a(n-1,m-1) + a(n-1,m), \qquad (0 < m < n),$$

with initial conditions $a(n,0) = 1$ *for* $n \geq 0$*, and* $a(n,n) = 0$ *for* $n > 0$*.*

The following result relates the length function to the cycle number.

Proposition 3.3 (*Corollary 6.4*). *Let* $v \in A_n$*,* $n \geq 2$*, Then*

$$\ell_{T(A_n)}(v) = \begin{cases} n - cyc(v) & \text{if 1,2 are in different cycles of } v; \\ n - cyc(v) - 1 & \text{if 1,2 in the same cycle of } v. \end{cases}$$

(For $n \leq 2$, A_n contains only the identity permutation.)
Note that the length function $\ell_{T(A_n)}(v)$ is odd if and only if $1, 2$ are in the same cycle in v (see Corollary 6.2).

Proposition 3.4 (*Theorem 7.2*). *For* $n \geq 2$*, we have*

$$\begin{aligned} \sum_{v\in A_n} x^{\ell_{T(A_n)}(v)} &= \sum_{k=0}^{n} a(n,k)\cdot x^k \\ &= (1+2x)(1+3x)\cdots(1+(n-1)x) \\ &= \prod_{t=2}^{n-1}(1+tx). \end{aligned}$$

Theorem 3.5 (*Theorem 8.4*). *The expected value of* $\ell_{T(A_n)}$ *is*

$$E[\ell_{T(A_n)}] = n - H_n - \frac{1}{2},$$

and its variance is

$$Var[\ell_{T(A_n)}] = H_n - H_{n,2} - \frac{1}{4}.$$

Finally, we discuss a certain generalization of Stirling numbers and relate it to our statistic $a(n,k)$. The generalization discussed is Broder's restricted Stirling numbers [2], see Definitions 2.13 and 2.17. The connection was initially established using the On-Line Encyclopedia of Integer Sequences [11].

Proposition 3.6 (*Theorem 9.2*). *For* $0 \leq k \leq n-2$*, we have*

$$a(n,k) = \begin{bmatrix} n \\ n-k \end{bmatrix}_2$$

4. The A Canonical Presentation

In this section we consider a canonical presentation of elements in A_n by the corresponding $s_1 t_{ij}$ generators.

4.1. **A Generating Set for A_n.** We let

$$a_{ij} := s_1 t_{ij} = (12)(ij), \qquad (1 \le i < j \le n).$$

Denote by $T(A_n) := \{a_{ij} \mid 1 \le i < j \le n\}$ the set of A-transpositions.

Definition 4.1. For $n \ge 3$ define the following subset of permutations in A_n:

$$R_n = \{(12)(in) \mid 1 \le i < n\} \cup \{e\}.$$

Note 4.2. R_n is a subset of $T(A_n)$, $R_n = (T(A_n) \setminus T(A_{n-1})) \cup \{e\}$.

Theorem 4.3. *Let $v \in A_n$, $n \ge 3$. Then there exist unique elements $v_i \in R_i$, $3 \le i \le n$, such that $v = v_3 \cdots v_n$. Call it the canonical presentation of v.*

Lemma 4.4. *Let $k \in \mathbb{N}$, $m_1, \cdots, m_{2k} \in \{1, \cdots, n\}$ be distinct and let*

$$v = (m_1 m_2) \cdots (m_{2k-1} m_{2k}) \in S_n, \quad m_1 \ne m_2, \cdots, m_{2k-1} \ne m_{2k}$$

be a product of transpositions. Then, for every $1 \le i \le 2k$, there exists a presentation of v as a product of transpositions in which m_i appears in the rightmost factor only.

Proof of Lemma 4.4. We provide a proof for $i = 1$. First we prove the assertion for the case $k = 2$, i.e., for the case where v is a product of two cycles. If $\{m_1, m_2\} \cap \{m_3, m_4\} = \varnothing$, then $v = (m_1 m_2)(m_3 m_4) = (m_3 m_4)(m_1 m_2)$, as required. Else, if $m_2 = m_3$, then $v = (m_1 m_2)(m_2 m_4) = (m_1 m_2 m_4) = (m_2 m_4 m_1) = (m_2 m_4)(m_4 m_1)$, as required. The case $m_2 = m_4$ is similar. Else, if $m_1 = m_3$, then $v = (m_1 m_2)(m_1 m_4) = (m_2 m_1 m_4) = (m_4 m_2 m_1) = (m_4 m_2)(m_2 m_1)$, as required. The case $m_1 = m_4$ is similar. If $m_1 = m_3$ and $m_2 = m_4$, then v is the identity, thus its cycles are disjoint and commute with each other. All possible cases were checked and thus we are finished.

Now we turn to the general case, where v is a product of k cycles. By induction the lemma applies also for this case as we can perform the same steps described in the simple case repeatedly until the desired form of v is achieved. □

Proof of Theorem 4.3. We proceed by induction on n. For $n = 3$, we have

$$A_3 = \{(12)(13), (12)(23), e\} = R_3,$$

and thus the claim holds. Now assume that each $w \in A_{n-1}$, $n \ge 4$, has a unique canonical presentation $w = w_3 \cdots w_{n-1}$, $w_i \in R_i$. We will show that, if $v \in A_n$, then v has a unique canonical presentation as well. This follows actually from Lemma 4.4. We assume that $v \in A_n \setminus A_{n-1}$, otherwise the proof follows immediately from the induction hypothesis. First we apply Lemma 4.4 to v to get n in the rightmost factor only. We have $v = g_1 \cdots g_k = g_1 \cdots g_{k-1}(12)(12)g_k$ with n in g_k only. Now, since $g_1 \cdots g_{k-1}(12) \in A_{n-1}$, according to the induction hypothesis it has a unique canonical presentation, say $w_1 \cdots w_t$. Thus we have $v = w_1 \cdots w_t (12) g_k$ and this is unique canonical presentation for v, because $(12)g_k$ is unique. □

By Theorem 4.3, we obtain the following corollary.

Corollary 4.5. *The set of A-transpositions, $T(A_n) := \{a_{ij} \mid 1 \le i < j \le n\}$, generates the alternating group on n letters.*

Definition 4.6. For $v \in A_n$ with the canonical presentation $v = v_3 \cdots v_n$, let

$$\hat{\ell}(v) = \#\{i \mid v_i \ne e\}.$$

Theorem 4.7. *For all $v \in A_n$,*

$$\hat{\ell}(v) = \ell_{T(A_n)}(v).$$

In other words the length of the canonical presentation coincides with the natural length with respect to the generating set $T(A_n)$.

Proof of Theorem 4.7. It suffices to show that, if $\hat{\ell}(v) = r$, then v can not be presented as a product of less than r generators. For $n = 3$ it was shown that $A_3 = R_3$, thus all the elements in A_3 are of length 1, except for the identity e whose length is 0. For $n > 3$ denote the length of the canonical presentation of v by $\hat{\ell}(v) = r$. Denote the shortest presentation of v by $v_2 = b_1 \cdots b_k$, $b_i \in T(A_n)$. Then $\ell_{T(A_n)}(v) = k$. Now we can apply the corollary of Lemma 4.4 described in the proof of Theorem 4.3 to turn v_2 into a canonical presentation of v, say v_2', with $\ell_{T(A_n)}(v_2') = k$. Since v_1 and v_2' are two canonical presentations of the same permutation, according to Theorem 4.2 they are actually the same presentation, i.e., $r = k$. □

In the rest of this paper, we explore the natural length function with respect to $T(A_n)$. For this purpose, we use the equivalence to the length of the canonical expression proved above, as needed.

5. Counting Permutations in A_n

In this section we study the number of permutations in A_n of a given length with respect to $T(A_n)$. A Stirling-type recurrence relation for this statistic is described.

Definition 5.1. Let

$$A(n, m) = \{v \in A_n \mid \ell_{T(A_n)}(v) = m\}$$

and

$$a(n, m) = |A(n, m)|.$$

Proposition 5.2. *For $n \geq 3$,*

$$a(n, 1) = a(n - 1, 1) + n - 1.$$

Proof of Proposition 5.2. By Definition 4.1, $R_n \setminus \{e\}$ is the subset of generators of A_n that do not belong to A_{n-1}; namely $R_n \setminus \{e\} = (T(A_n) \setminus T(A_{n-1})) = \{(12)(nj) \mid 1 \leq j < n\}$. These are the generators that involve the new letter n. Thus $|R_n| = n$.

For every n, $A(n, 1) = T(A_n)$, and since $T(A_n) = T(A_{n-1}) \cup (R_n \setminus \{e\})$ (this is a disjoint union), we conclude $a(n, 1) = a(n - 1, 1) + n - 1$. □

Theorem 5.3. *We have*

$$A(n, m) = A(n - 1, m - 1) \cdot R_n \ \cup \ A(n - 1, m),$$

where the union on the right-hand side is a disjoint union.

Proof of Proposition 5.3. We prove the claim by two-sided set inclusion. First we prove that $A(n, m) \supseteq A(n - 1, m - 1) \cdot R_n \cup A(n - 1, m)$. Note that the right-hand side of the equation is a disjoint union, according to the properties of the A_n canonical presentation.

On the other hand, we also have $A(n - 1, m) \subseteq A(n, m)$ because a permutation v of length m in A_{n-1} is also of length m in A_n. The new generators in A_n can not shorten the length of v because they involve the new letter n which is a fixed point in v.

Let $v \in A(n-1, m-1)$, and consider its canonical presentation. Multiply v by $w \in R_n$ from the right side to have the canonical presentation of a permutation $v \cdot w \in A_n$ of length $m - 1 + 1 = m$, i.e., $v \cdot w \in A(n, m)$.

We showed that each part of the union on the right-hand side of the equation is contained in the left-hand side, therefore the union itself is also contained in the left-hand side. This proves the first inclusion. Now we show that $A(n, m) \subseteq A(n-1, m-1) \cdot R_n \cup A(n-1, m)$. Let $v \in A(n, m)$.

(1) If n is a fixed point in v, then $v \in A(n-1, m)$ with the same canonical presentation.
(2) Otherwise, n is not a fixed point, and therefore the canonical presentation of v reads as follows:

$$v = \underbrace{r_1 \cdots r_{k-1}}_{\in A(n-1,m-1)} \cdot \underbrace{r_n}_{\in (R_n \setminus \{e\})}, \quad r_i \in R_i, \quad 1 \leq i \leq n.$$

We have $r_n \in R_n \setminus \{e\}$ because n is not a fixed point and must appear in the presentation. The above canonical presentation of v establishes the required inclusion.

□

From Proposition 5.2 and Theorem 5.3 we can conclude the following relation.

Corollary 5.4. *For $1 \leq m \leq n-2$, we have*

$$a(n, m) = a(n-1, m-1) \cdot (n-1) + a(n-1, m).$$

6. Relation between Length and Cycle Number

In this section we show that the length $\ell_{T(A_n)}(\cdot)$ and the number of cycles $cyc(\cdot)$ are strongly related statistics on A_n.

Observation 6.1. *For $n \geq 3$, and $v \in A(n, 1)$, $cyc(v) = n - 2$.*

In other words, the number of cycles in a generator of A_n is $n - 2$.

Proof of Observation 6.1. Every generator $v \in A_n$ is of the form $(12)(in)$, where $1 \leq i < n$. If $i = 1$, or $i = 2$, then v has one cycle of length 3 and $n - 3$ cycles of length 1 (fixed points). This sums to $n - 2$ cycles. Otherwise $i > 2$, and then v has two cycles of length 2 and $n - 4$ more cycles of length 1. This also sums to $n - 2$ cycles in v. □

Corollary 6.2. *For every $n \geq 2$ and $v \in A_n$, the letters $1, 2$ are in the same cycle in v if and only if $\ell_{T(A_n)}(v)$ is odd.*

Proof of Corollary 6.2. If $v \in A_n$ is of length one, $1, 2$ share the same cycle since the structure of a generator is $(12)(ij)$. In length two, $1, 2$ appear in different cycles because of the multiplication process described in the proof of Theorem 5.3. For length three, $1, 2$ are in the same cycle according to the same process, and so on and so forth. For odd length, the letters $1, 2$ are in the same cycle, and for even length they are in different cycles. This proves both implications of the equivalence. □

Theorem 6.3. *For $n \geq 3$ and $v \in A_n$, we have*

$$cyc(v) = \begin{cases} n - \ell_{T(A_n)}(v) & \text{if } \ell_{T(A_n)}(v) \text{ is even,} \\ n - \ell_{T(A_n)}(v) - 1 & \text{if } \ell_{T(A_n)}(v) \text{ is odd.} \end{cases}$$

Proof of Theorem 6.3. We proceed by induction on n. For $n = 3$, we have

$$A_3 = \{(12)(13) = (213), (12)(23) = (123), e = (1)(2)(3)\},$$

and the claim follows. Assume that, for each $v \in A_n$, we have

$$cyc(v) = \begin{cases} n - \ell_{T(A_n)}(v) & \text{if } \ell_{T(A_n)}(v) \text{ is even,} \\ n - \ell_{T(A_n)}(v) - 1 & \text{if } \ell_{T(A_n)}(v) \text{ is odd.} \end{cases}$$

Now, $w \in A_{n+1}$ can be obtained in two ways by Theorem 5.3. First, by multiplying $v \in A_n$ by $r \in R_{n+1}$, and secondly by adding the letter $n + 1$ as fixed point to some $v \in A_n$. Both cases will be analyzed.

(1) In this case $w = vr$ for $v \in A_n$, $r \in R_{n+1}$. If $\ell_{T(A_n)}(v)$ is even, then, by Corollary 6.2, the letters $1, 2$ are in different cycles in v, and therefore they will be in the same cycle in w, thus $cyc(w) = cyc(v) - 1$ (see Theorem 5.3 for details). The length of w is $\ell_{T(A_{n+1})}(w) = \ell_{T(A_n)}(v) + 1$. By the induction hypothesis,

$$cyc(w) = cyc(v) - 1 = n - \ell_{T(A_n)}(v) - 1 = n - \ell_{T(A_{n+1})}(w) = (n + 1) - \ell_{T(A_{n+1})}(w) - 1,$$

as required. If $\ell_{T(A_n)}(v)$ is odd, then, by Corollary 6.2 and Theorem 5.3, $cyc(w) = cyc(v) + 1$ and $\ell_{T(A_{n+1})}(w) = \ell_{T(A_n)}(v) + 1$. By the induction hypothesis,

$$cyc(w) = cyc(v) + 1 = n - \ell_{T(A_n)}(v) - 1 + 1 = n - \ell_{T(A_{n+1})}(w) + 1 = (n+1) - \ell_{T(A_{n+1})}(w),$$

as required.

(2) In this case $w = v$ for some $v \in A_n$, where the letter $n + 1$ is a fixed point in w. Here, $cyc(w) = cyc(v) + 1$ and $\ell_{T(A_{n+1})}(w) = \ell_{T(A_n)}(v)$. If $\ell_{T(A_n)}(v)$ is even,

$$cyc(w) = cyc(v) + 1 = n - \ell_{T(A_n)}(v) + 1 = n - \ell_{T(A_{n+1})}(w) + 1 = (n + 1) - \ell_{T(A_{n+1})}(w),$$

as required, and, if $\ell_{T(A_n)}(v)$ is odd,

$$cyc(w) = cyc(v) + 1 = n - \ell_{T(A_n)}(v) - 1 + 1 = n - \ell_{T(A_{n+1})}(w) = (n+1) - \ell_{T(A_{n+1})}(w) - 1,$$

as required.

In both cases the relation between cycle number and length holds, therefore the theorem is proved. □

Corollary 6.2 and Theorem 6.3 imply the following relation.

Corollary 6.4. *Let $v \in A_n$.*

$$\ell_{T(A_n)}(v) = \begin{cases} n - cyc(v) & \text{if } 1, 2 \text{ are in different cycles of } v, \\ n - cyc(v) - 1 & \text{if } 1, 2 \text{ are in the same cycle of } v. \end{cases} \tag{6.1}$$

Equation (6.1) provides a simple way to find the length of a permutation v given as a product of disjoint cycles.

Theorem 6.3 implies that all the permutations of the same length in A_n have the same number of cycles.

Definition 6.5.

$$m(n,k) = \textit{number of cycles in a permutation } v \in A_n \textit{ of length } \ell_{T(A_n)}(v) = k.$$

7. Generating Function of Length in A_n

An explicit formula for the generating function of the length in A_n, with respect to the generating set $T(A_n)$, is given in this section.

According to Theorem 6.3, the number $m(n,k)$, of cycles in a permutation $v \in A_n$ of length k, can be calculated by the following formula:

$$m(n,k) = \begin{cases} n-k, & \text{if } k \text{ is even,} \\ n-k-1, & \text{if } k \text{ is odd.} \end{cases} \tag{7.1}$$

A well known result in S_n is

$$m(n,k) = n-k \tag{7.2}$$

where the length k is taken with respect to the generating set $T = \{(ij) \mid 1 \le i < j \le n\}$, that is, all the transpositions in S_n. Since the number of cycles in a permutation is independent of the generating set, from Equations (7.1) and (7.2) we can conclude that, for $v \in A_n$, we have

$$\ell_T(v) = \begin{cases} \ell_{T(A_n)}(v), & \text{if } \ell_{T(A_n)}(v) \text{ is even,} \\ \ell_{T(A_n)}(v)+1, & \text{if } \ell_{T(A_n)}(v) \text{ is odd,} \end{cases} \tag{7.3}$$

where $\ell_T(v)$ is the length with respect to T. Note that, in each of the cases, $\ell_T(v)$ is even, which complies with the fact that we deal with even permutations in S_n. From Equation (7.3) we can conclude that the number of permutations of even length k in S_n equals the sum of the number of permutations of lengths k and $k-1$ in A_n. Since the number of permutations of length k in S_n with respect to T is the unsigned Stirling number of the first kind $c(n, n-k)$, we can deduce the following equation for even k:

$$c(n, n-k) = a(n,k) + a(n,k-1). \tag{7.4}$$

A further consequence is the following.

Claim 7.1. *Equation* (7.4) *holds also for odd* $k \in \mathbb{N}$.

Proof of Claim 7.1. Let $k+1$ be even. Using the recursive relation of Stirling numbers, we can expand the left-hand of Equation (7.4) to obtain

$$\begin{aligned} c(n, n-(k+1)) &= c(n-1, n-(k+1)-1) + c(n-1, n-(k+1)) \cdot (n-1) \\ &= c(n-1, n-1-(k+1)) + c(n-1, n-1-((k+1)-1)) \cdot (n-1) \\ &= c(n-1, n-k-2) + c(n-1, n-1-k) \cdot (n-1). \end{aligned}$$

Rearrangement of terms gives the following result:

$$(n-1) \cdot c(n-1, n-1-k) = c(n, n-k-1) - c(n-1, n-k-2).$$

The expressions at the right-hand side represent even length, so we can use Equation (7.4) and Conclusion 5.4 to obtain the desired result:

$$\begin{aligned}(n-1)\cdot c(n-1,n-1-(k-1)) &= a(n,k)+a(n,k-1)-a(n-1,k)-a(n-1,k-1)\\ &= a(n-1,k-1)\cdot(n-1)+a(n-1,k)+a(n-1,k-2)\cdot(n-1)\\ &\qquad +a(n-1,k-1)-a(n-1,k)-a(n-1,k-1)\\ &= a(n-1,k-1)\cdot(n-1)+a(n-1,k-2)\cdot(n-1).\end{aligned}$$

Dividing both sides by $(n-1)$, we deduce, for odd k, the equation

$$c(n-1,n-1-k)=a(n-1,k)+a(n-1,k-1).$$

□

The following generating function for unsigned Stirling numbers of the first kind is well known [4, pp. 213]:

$$\sum_{k=1}^{n} c(n,k)\cdot x^{n-k}=(1+x)(1+2x)\cdots(1+(n-1)x). \tag{7.5}$$

By Equation (7.4), we have

$$\sum_{k=0}^{n} c(n,n-k)\cdot x^{k}=\sum_{k=0}^{n} a(n,k)\cdot x^{k}+\sum_{k=0}^{n} a(n,k-1)\cdot x^{k}.$$

Using Equation (7.5) for the left-hand side, we obtain

$$\begin{aligned}&(1+x)(1+2x)\cdots(1+(n-1)x)\\ &\qquad=\sum_{k=0}^{n} a(n,k)\cdot x^{k}+x\cdot\sum_{k=0}^{n} a(n,k-1)\cdot x^{k-1}=(1+x)\cdot\sum_{k=0}^{n} a(n,k)\cdot x^{k}.\end{aligned}$$

Dividing both sides by $(x+1)$, we get the generating function of length in A_n with respect to the generating set $T(A_n)$.

Theorem 7.2. *We have*

$$\begin{aligned}\sum_{k=0}^{n} a(n,k)\cdot x^{k} &= (1+2x)(1+3x)\cdots(1+(n-1)x)\\ &= \prod_{t=2}^{n-1}(1+tx).\end{aligned} \tag{7.6}$$

8. Expectation and Variance

In this section, the expectation and variance of the length function in A_n are studied.

Definition 8.1. Let A be a finite set, and $s : A \to \mathbb{R}$ a real function. The expectation of s is defined by

$$E[s] := \frac{1}{|A|}\sum_{a\in A} s(a),$$

and the variance of s is defined by

$$Var[s] := E[s^2]-E^2[s].$$

Given a generating function of s, we can use it to calculate these statistics. The following formulas are well-known.

Proposition 8.2. *Let*

$$F_s(x) := \sum_{a\in A} x^{s(a)}$$

be the generating function of s. Then

$$E[s] = \frac{1}{|A|} F_s'(x)\Big|_{x=1},$$

and

$$Var[s] = \frac{1}{|A|}\Big[F_s''(x) + F_s'(x) - \frac{1}{|A|}(F_s'(x))^2\Big]\Big|_{x=1}.$$

Definition 8.3. We recall the definitions of harmonic numbers (see Definitions 2.21 and 2.22),

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

and generalized harmonic numbers,

$$H_{n,m} = 1 + \frac{1}{2^m} + \frac{1}{3^m} + \cdots + \frac{1}{n^m}$$

Theorem 8.4. *The expected value of $\ell_{T(A_n)}$ is*

$$E[\ell_{T(A_n)}] = n - H_n - \frac{1}{2},$$

and its variance is

$$Var[\ell_{T(A_n)}] = H_n - H_{n,2} - \frac{1}{4}.$$

Proof of Theorem 8.4. Compute the derivative of the generating function with respect to length (see Theorem 7.2) as a product of functions:

$$\left(\prod_{t=2}^{n-1}(1+tx)\right)' = \left(\prod_{t=2}^{n-1}(1+tx)\right)\sum_{t=2}^{n-1}\frac{t}{1+tx}.$$

Thus, by Proposition 8.2,

$$E[\ell_{T(A_n)}] = \frac{1}{|A_n|}\left(\prod_{t=2}^{n-1}(1+tx)\right)\sum_{t=2}^{n-1}\frac{t}{1+tx}\Bigg|_{x=1} = \frac{2}{n!}\cdot\frac{n!}{2}\left(n-2-\sum_{t=2}^{n-1}\frac{1}{1+t}\right) = n-H_n-\frac{1}{2}.$$

For the variance, we have

$$\begin{aligned}\left(\prod_{t=2}^{n-1}(1+tx)\right)'' &= \left[\left(\prod_{t=2}^{n-1}(1+tx)\right)\sum_{t=2}^{n-1}\frac{t}{1+tx}\right]' \\ &= \left(\prod_{t=2}^{n-1}(1+tx)\right)\sum_{t=2}^{n-1}\frac{t}{1+tx}\sum_{t=2}^{n-1}\frac{t}{1+tx} + \left(\prod_{t=2}^{n-1}(1+tx)\right)\sum_{t=2}^{n-1}\frac{-t^2}{(1+tx)^2},\end{aligned}$$

and thus

$$
\begin{aligned}
Var[\ell_{T(A_n)}] &= \frac{1}{|A_n|}\Bigg[\Big(\prod_{t=2}^{n-1}(1+tx)\Big)'' + \Big(\prod_{t=2}^{n-1}(1+tx)\Big)' - \frac{1}{|A_n|}\Big(\Big(\prod_{t=2}^{n-1}(1+tx)\Big)'\Big)^2\Bigg]_{x=1} \\
&= \frac{2}{n!}\Bigg[\Big(\prod_{t=2}^{n-1}(1+tx)\Big)\sum_{t=2}^{n-1}\frac{t}{1+tx}\sum_{t=2}^{n-1}\frac{t}{1+tx} + \Big(\prod_{t=2}^{n-1}(1+tx)\Big)\sum_{t=2}^{n-1}\frac{-t^2}{(1+tx)^2} \\
&\quad + \Big(\prod_{t=2}^{n-1}(1+tx)\Big)\sum_{t=2}^{n-1}\frac{t}{1+tx} - \frac{2}{n!}\Big(\Big(\prod_{t=2}^{n-1}(1+tx)\Big)\sum_{t=2}^{n-1}\frac{t}{1+tx}\Big)^2\Bigg]_{x=1} \\
&= \frac{2}{n!}\Bigg[\frac{n!}{2}\Big(n - H_n - \frac{1}{2}\Big)^2 + \frac{n!}{2}\Big(2H_n + \frac{1}{4} - n - H_{n,2}\Big) + \frac{n!}{2}\Big(n - H_n - \frac{1}{2}\Big) \\
&\quad - \frac{2}{n!}\Big(\frac{n!}{2}(n - H_n - \frac{1}{2}\Big)^2\Bigg] \\
&= H_n - H_{n,2} - \frac{1}{4}.
\end{aligned}
$$

□

9. Connection with Restricted Stirling Numbers

This section discusses the relation between our statistic $a(n,m)$ and 2-restricted Stirling numbers of the first kind (see Broder [2, §1]). This relation was initially observed using the On-Line Encyclopedia of Integer Sequences [11].

Recall Definition 2.13 of the r-restricted Stirling numbers of the first kind, $\left[{n \atop k}\right]_r$. We shall use it with $r = 2$. The number $\left[{n \atop k}\right]_1 = c(n,k)$ is the usual (unrestricted) Stirling number of the first kind.

Claim 9.1 (See Broder [2, § 3, Thm. 3] for a generalized version)**.** *We have*

$$c(n,k) = \left[{n \atop k}\right]_2 + \left[{n \atop k+1}\right]_2.$$

Theorem 9.2. *The number of permutations in A_n of length $\ell_{T(A_n)}(\cdot) = k$ is equal to a corresponding 2-restricted Stirling number. Namely,*

$$a(n,k) = \left[{n \atop n-k}\right]_2, \quad (0 \le k \le n-2).$$

We give two proofs to Theorem 9.2. The first proof is algebraic, and the second consists of a direct bijection between two sets.

Proof of Theorem 9.2. From Claims 9.1 and 7.1 we can deduce the following equation:

$$a(n,k) + a(n,k-1) = \left[{n \atop n-k}\right]_2 + \left[{n \atop n-k+1}\right]_2, \quad (0 \le k \le n-1).$$

Now the theorem can be proved by induction on k. By assumption, $n \ge 2$. For $k = 0$, we have $a(n,0) = 1$ and $\left[{n \atop n}\right]_2 = 1$. The claim $a(n,k) = \left[{n \atop n-k}\right]_2$ now follows by induction on k. □

Definition 9.3. Let

$$P(n,k) = \{v \in S_n \mid cyc(v) = k \text{ and } 1,2 \text{ are in different cycles in } v\}.$$

We now present an explicit bijection between the sets $A(n,k)$ and $P(n,n-k)$.

A Bijective Proof of Theorem 9.2. Define a map $f : A(n,k) \to P(n,n-k)$ by

$$f(v) = \begin{cases} v & \text{if } \ell_{T(A_n)}(v) \text{ is even,} \\ (1,2)v & \text{if } \ell_{T(A_n)}(v) \text{ is odd.} \end{cases}$$

We will show that f is one-to-one and onto $P(n,n-k)$.

(1) Consider $v_1, v_2 \in A(n,k)$ with $f(v_1) = f(v_2)$. If v_1, v_2 are both of even length, or both of odd length, then, by the definition of f, $v_1 = v_2$. If v_1 is of even length and v_2 is of odd length or vice versa, then, by the definition of f and the fact that $f(v_1) = f(v_2)$, $v_1 = (1,2)v_2$. This contradicts the assumption that $v_1, v_2 \in A(n,k)$, and is therefore impossible. Since only the first case is feasible, $v_1 = v_2$ and f is one-to-one.

(2) Consider $w \in P(n,n-k)$. The length of w in S_n, $\ell_T(w)$, is k. If k is even, then $w \in A_n$. By Corollaries 6.2 and 6.4, we have $\ell_{T(A_n)}(w) = k$, therefore $w \in A(n,k)$ and $f(w) = w$. If k is odd, then $(1,2)w \in A_n$. By Corollaries 6.2 and 6.4, we have $\ell_{T(A_n)}((1,2)w) = k$, therefore $(1,2)w \in A(n,k)$ and $f((1,2)w) = w$. This proves that f is onto $P(n,n-k)$.

□

Acknowledgements

I wish to thank my supervisors Prof. Ron M. Adin and Prof. Yuval Roichman for their professional guidance, patience and for introducing me to the fascinating world of combinatorial research.

I want to thank my parents for their love and support.

I would like to thank all those who helped me and supported me during this work.

References

[1] R. M. Adin, F. Brenti and Y. Roichman, *Descent numbers and major indices for the hyperoctahedral group.* Special issue in honor of Dominique Foata's 65th birthday (Philadelphia, PA 2000). Adv. in Appl. Math. 27 (2001), 210–224.
[2] A. Z. Broder, *The r-Stirling numbers.* Discrete Math. 49 (1984), 241–259
[3] F. Brenti, V. Reiner and Y. Roichman, *Alternating subgroups of Coxeter groups.* J. Comb. Theory, Series A 115 (2008), 845–877.
[4] L. Comtet, *Advanced Combinatorics.* D. Reidel Publishing Company, Dordrecht, Holland (1974).
[5] J. E. Humphreys, *Reflection Groups and Coxeter Groups.* Cambridge Studies in Advanced Mathematics. 29. Cambridge Univ. Press, Cambridge, 1990.
[6] P. A. MacMahon, *Combinatory Analysis I-II.* Cambridge Univ. Press, London/New-York, 1916. (Reprinted by Chelsea, New-York, 1960.)
[7] H. Mitsuhashi, *The q-analogue of the alternating group and its representations.* J. Algebra 240 (2001), 535–558.
[8] A. Regev and Y. Roichman, *Permutation statistics on the alternating group.* Adv. in Appl. Math. 33 (2004), 676–709.
[9] R. P. Stanley, *Enumerative Combinatorics, vol. 1.* Cambridge Univ. Press, 1998.

[10] A. Vershik and M. Vsemirnov, *The local stationary presentation of the alternating groups and the normal form.* J. Algebra 319 (2008), 4222–4229.

[11] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, electronically available at `http://www.research.att.com/~njas/sequences/Seis.html`;
Sequences A001705, A143491, A143494.