

Note: The Outer Automorphism of S_6

Koji Nuida

April 13, 2015

Abstract

In this note, we describe an explicit construction of the outer automorphism of the symmetric group S_6 on six letters. We also explain the fact that S_n for $n \neq 6$ has no outer automorphisms.

1 The Map

We briefly say (by postponing the detailed explanation) that, the group automorphism $F: S_6 \rightarrow S_6$ uniquely determined by the following conditions

$$F((12)) = (12)(34)(56)$$

$$F((23)) = (16)(24)(35)$$

$$F((34)) = (14)(23)(56)$$

$$F((45)) = (16)(25)(34)$$

$$F((56)) = (13)(24)(56)$$

is the outer automorphism of S_6 which is the subject of this note. See Section 4 for some more properties of the map.

2 Preliminaries

In this note, n denotes a positive integer. The *symmetric group of degree n* , denoted by S_n , is the set of permutations of integers from 1 to n . This set is endowed with a binary operator defined by the composition of two permutations as maps. Then S_n forms a group with respect to this operator. We use notations like $f \cdot g$ and fg for the binary operator, rather than the notation $f \circ g$ for composite maps.

Each element of S_n can be visualized by using an “Amida diagram” (“Amida-kuji” in Japanese) with n vertical axes (see Figure 1 for example).

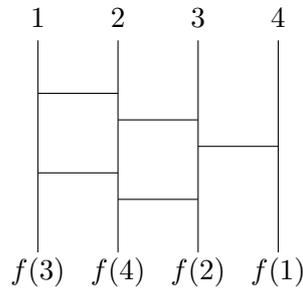


Figure 1: Amida diagram representing the permutation $f \in S_4$ defined by $f(1) = 4$, $f(2) = 3$, $f(3) = 1$ and $f(4) = 2$

Here, the vertical axes correspond to integers $1, \dots, n$ from left to right. To determine the image $f(i)$ of a number i by a given Amida diagram, we start from the top of i -th vertical axis and follow the line downward, where if we meet an endpoint of a horizontal edge joining the current vertical axis with one of the adjacent vertical axes, we move to the opposite vertical axis (by crossing the horizontal edge) and then continue to go downward.¹ Then we determine $f(i) = j$, if we finally reach to the bottom of j -th vertical axis. By the definition, distinct numbers are mapped to different numbers, therefore f is a permutation; $f \in S_n$.² When $f, g \in S_n$ are determined by Amida diagrams as above, we can construct another Amida diagram by concatenating the two Amida diagrams, with the one for f combined at the bottom of the one for g ; the resulting Amida diagram defines the product $f \cdot g \in S_n$. On the other hand, we can construct another Amida diagram by turning the Amida diagram for f upside down, which corresponds to the inverse f^{-1} of f .

Conversely, given an element f of S_n , we can construct an Amida diagram which determines the f as follows. First, for the number (say, i) which is mapped by f to n , we join i -th and $(i+1)$ -th vertical axes by a horizontal edge, join $(i+1)$ -th and $(i+2)$ -th vertical axes by a horizontal edge, and so on, and join $(n-1)$ -th and n -th vertical axes by a horizontal edge. These edges let the number i go to n -th vertical axis correctly. Secondly, we let the number mapped by f to $n-1$ go to $(n-1)$ -th vertical axis correctly,

¹We should not draw two horizontal edges from the same point in an Amida diagram, because the choice of an edge to follow becomes ambiguous. We also suppose the total number of horizontal edges to be finite.

²A rigorous proof can be given by a recursive argument with respect to the total number of horizontal edges.

by joining vertical axes *except for n -th vertical axis* by horizontal edges in a similar way. Now these two numbers have correctly moved to $(n - 1)$ -th and n -th vertical axes, respectively. Iterating this process recursively, we finally obtain the desired Amida diagram corresponding to f .

Instead of drawing such Amida diagrams, we usually use the following notations for specifying elements of S_n . For distinct numbers a_1, \dots, a_k in $\{1, \dots, n\}$, let $(a_1 a_2 \dots a_k)$ denote the element of S_n which maps a_1 to a_2 , a_2 to a_3, \dots, a_{k-1} to a_k , and a_k to a_1 , and fixes any other number. Such an element of S_n is called a *cyclic permutation* (or simply a *cycle*), and k is called the *length* of the cycle. We note that, for an index i with $1 \leq i \leq k$, the cyclic permutation $(a_i a_{i+1} \dots a_k a_1 a_2 \dots a_{i-1})$ is equal to $(a_1 a_2 \dots a_k)$. By observing the orbits generated by applying an element f of S_n to each number repeatedly, the following well-known fact is derived:

Proposition 1. *Any element of S_n can be expressed as a product of cyclic permutations $(a_1 a_2 \dots a_k)$ for which the sets $\{a_1, a_2, \dots, a_k\}$ are disjoint to each other.*

For an element f of S_n , if an expression of f as a product of disjoint cycles as in Proposition 1 involves m_i cycles of length i for each i , we say that f has *cycle type* $(1^{m_1} 2^{m_2} \dots)$. Here, by supplying cycles (j) of length one (i.e., identity permutation) for numbers j fixed by f if necessary, we may assume without loss of generality that an expression of f as a product of disjoint cycles always involves every number from 1 to n , each of which appears exactly once. Namely, we assume that $\sum_{j \geq 1} m_j \cdot j = n$ holds for the type of an element of S_n . This requirement makes the type of $f \in S_n$ uniquely determined, independent of such an expression of f as a product of disjoint cycles.³ Moreover, the following property is well-known:

Proposition 2. *For elements f, g of S_n , f and g are conjugate (i.e., $g = hfh^{-1}$ for some $h \in S_n$) if and only if f and g have the same cycle type.*

A cyclic permutation $(a_1 a_2)$ of length two is called a *transposition*, and such a transposition with $a_2 = a_1 + 1$ is called an *adjacent transposition*. For example, the permutation $f \in S_4$ given in Figure 1 is a cyclic permutation $f = (1423)$, and it can be written as $f = (23)(12)(34)(23)(12)$ by a product of adjacent transpositions. By the correspondence between permutations and Amida diagrams mentioned above, adjacent transpositions correspond to Amida diagrams with only one horizontal edge. By combining this fact with the above-mentioned construction of an Amida diagram for a given permutation, we have the following well-known result:

³In fact, such an expression of f is essentially unique.

Proposition 3. *Any element of S_n can be expressed as a product of adjacent transpositions.*

We note, however, that the way of expressing an element of S_n as a product of adjacent transpositions is not necessarily unique (even if we do not use obviously redundant adjacent transpositions like (12)(12)). For example, the transposition (13) can be expressed as (12)(23)(12) and also as (23)(12)(23). More generally, adjacent transpositions satisfy the following relations. Here, id denotes the identity permutation (i.e., the element of S_n that fixes every number), and the adjacent transposition $(i \ i+1)$ is denoted by s_i .

$$\text{For } 1 \leq i \leq n-1 : s_i s_i = \text{id} . \quad (1)$$

$$\text{For } 2 \leq i \leq n-1 : s_{i-1} s_i s_{i-1} s_i s_{i-1} s_i = \text{id} . \quad (2)$$

$$\text{For } 1 \leq i \leq n-1, 1 \leq j \leq n-1 \text{ with } |i-j| \geq 2 : s_i s_j s_i s_j = \text{id} . \quad (3)$$

Moreover, it is remarkable and well-known that, if an element of S_n can be expressed as a product of adjacent transpositions in two different ways, then the difference of the expressions is deduced from the three kinds of relations above (a rigorous explanation of this fact is omitted here).⁴

If a bijection $F: S_n \rightarrow S_n$ from the group S_n to itself satisfies that $F(f \cdot g) = F(f) \cdot F(g)$ for any $f, g \in S_n$, we call the F an *automorphism* of S_n . The set $\text{Aut}(S_n)$ of all automorphisms of S_n also forms a group with respect to composition of maps, which is called the *automorphism group* of S_n . For example, for each element f of S_n , the map that maps an element $g \in S_n$ to $fgf^{-1} \in S_n$ is an automorphism of S_n . Such an automorphism is called an *inner automorphism*; and the other automorphisms are called *outer automorphisms*. The following property of inner automorphisms is derived from Proposition 2:

Proposition 4. *For any inner automorphism F of S_n , any element of S_n and its image by F have the same cycle type.*

3 No Outer Automorphisms Exist Except for S_6

In this section, we show that, for $n \neq 6$, every automorphism of S_n is an inner automorphism. We note that, the results in this section are also valid for $n = 6$ unless we explicitly specify that $n \neq 6$.

⁴Namely, by choosing the set of all adjacent transpositions as a generating set of S_n , the above-mentioned three kinds of relations form the fundamental relations for S_n .

Lemma 1. *If an automorphism F of S_n maps every transposition to a transposition, then F is an inner automorphism.*

Proof. It is sufficient to show that, for some distinct numbers $a_1, a_2, \dots, a_n \in \{1, 2, \dots, n\}$, we have $F((i \ i+1)) = (a_i \ a_{i+1})$ for every index i with $1 \leq i \leq n-1$. Indeed, in this case, by choosing the element $f \in S_n$ satisfying $f(j) = a_j$ for each $j \in \{1, 2, \dots, n\}$, we have $F(s_i) = fs_if^{-1}$ for each adjacent transposition $s_i = (i \ i+1)$, while Proposition 3 implies that every $g \in S_n$ can be written as a product of the elements s_i , therefore we have $F(g) = fgf^{-1}$.

From now, we verify the above-mentioned property. We consider the case $n \geq 2$, since the case $n = 1$ is trivial. First, by the assumption of this lemma, $F((12))$ is a transposition, which can be written as $F((12)) = (a_1a_2)$. This proves the claim when $n = 2$; we consider the case $n \geq 3$ from now on. Secondly, by the assumption of this lemma, we have $F((23)) = (b_1b_2)$ for some b_1 and b_2 . Then $F((12)(23)) = F((12))F((23)) = (a_1a_2)(b_1b_2)$. Now if two sets $\{a_1, a_2\}$ and $\{b_1, b_2\}$ are disjoint, then we have $((a_1a_2)(b_1b_2))^3 \neq \text{id}$, while $((12)(23))^3 = \text{id}$; this is a contradiction. Therefore, $\{a_1, a_2\}$ and $\{b_1, b_2\}$ have a common element, say (by symmetry) $a_2 = b_1$. We rewrite b_2 as a_3 . This proves the claim when $n = 3$; we consider the case $n \geq 4$ from now on. By the assumption of this lemma, we have $F((34)) = (c_1c_2)$ for some c_1 and c_2 . Now, owing to the fact $((23)(34))^3 = \text{id}$, a similar argument implies that $\{a_2, a_3\}$ and $\{c_1, c_2\}$ have a common element, while the fact $((12)(34))^2 = \text{id}$ implies that $\{a_1, a_2\}$ and $\{c_1, c_2\}$ should be disjoint. Therefore, we have $a_3 \in \{c_1, c_2\}$, and (c_1c_2) can be written as $(c_1c_2) = (a_3a_4)$ for some a_4 . By iterating this argument, we finally have the above-mentioned property. Hence, this lemma holds. \square

By combining Proposition 4 with Lemma 1, we have the following property:

Corollary 1. *For an automorphism F of S_n , F is an inner automorphism if and only if a transposition in S_n is always mapped by F to a transposition.*

Lemma 2. *For an automorphism F of S_n and any possible cycle type of elements of S_n , the cycle type of $F(f)$ for any element $f \in S_n$ of the fixed cycle type is uniquely determined, regardless of the choice of such an element f .*

Proof. Let $g \in S_n$ be any element with the same cycle type as f . By Proposition 2, f and g are conjugate, namely $g = hfh^{-1}$ for some $h \in S_n$. Now we have $F(g) = F(hfh^{-1}) = F(h)F(f)F(h)^{-1}$, therefore $F(f)$ and

$F(g)$ are conjugate to each other as well. By Proposition 2, this implies that $F(f)$ and $F(g)$ have the same cycle type. Hence, this lemma holds. \square

Lemma 3. *For any integer a with $0 \leq a \leq n/2$, the number of elements of S_n having cycle type $(1^{n-2a}2^a)$ is $n(n-1) \cdots (n-2a+1)/(a! \cdot 2^a)$.*

Proof. Let Z be the set of elements of S_n with cycle type $(1^{n-2a}2^a)$, let X be the set of sequences $[b_1, \dots, b_{2a}]$ of $2a$ distinct numbers in $\{1, \dots, n\}$, and let Y be the set of sequences $[B_1, \dots, B_a]$ of a disjoint subsets $B_1, \dots, B_a \subset \{1, \dots, n\}$ of size two. We define maps $F: X \rightarrow Y$ and $G: Y \rightarrow Z$ by

$$F([b_1, \dots, b_{2a}]) = [\{b_1, b_2\}, \{b_3, b_4\}, \dots, \{b_{2a-1}, b_{2a}\}] ,$$

$$G([\{b_1, b_2\}, \{b_3, b_4\}, \dots, \{b_{2a-1}, b_{2a}\}]) = (b_1 b_2)(b_3 b_4) \cdots (b_{2a-1} b_{2a}) .$$

(For the definition of G , note that $(xy) = (yx)$ as transpositions.) Then, the elements of X mapped by F to a given $[B_1, B_2, \dots, B_a] \in Y$ are nothing but the sequences obtained by first arranging the two elements of B_1 , secondly arranging the two elements of B_2 , and so on, and finally arranging the two elements of B_a . Since there are two ways of ordering the elements of each B_i , the total number of such sequences is 2^a . Therefore $|Y| = |X|/2^a$ holds. On the other hand, the elements of Y mapped by G to a given $(b_1 b_2)(b_3 b_4) \cdots (b_{2a-1} b_{2a}) \in Z$ are nothing but the sequences obtained by rearranging the a subsets in the sequence $[\{b_1, b_2\}, \{b_3, b_4\}, \dots, \{b_{2a-1}, b_{2a}\}]$. The total number of such sequences is $a!$, therefore $|Z| = |Y|/a!$ holds. Moreover, we have $|X| = n(n-1) \cdots (n-2a+1)$. This implies that

$$|Z| = |X|/(a! \cdot 2^a) = n(n-1) \cdots (n-2a+1)/(a! \cdot 2^a) .$$

Hence, this lemma holds. \square

For an automorphism F of S_n , the square of the image of any transposition by F is the identity permutation (since the transposition has the same property), therefore its cycle type can be written as $(1^{n-2a}2^a)$ (where a is an integer with $1 \leq a \leq n/2$). Owing to Lemma 2, the cycle type does not depend on the choice of the original transposition. By applying Lemma 2 to F^{-1} as well, it follows that every element of S_n with cycle type $(1^{n-2a}2^a)$ is the image by F of some transposition. This implies that the transpositions in S_n are in one-to-one correspondence via F to the elements of S_n with cycle type $(1^{n-2a}2^a)$. Therefore, the number of transpositions in S_n is equal to the number of elements of S_n with cycle type $(1^{n-2a}2^a)$. By this and Lemma 3, we have the following equality:

$$\frac{n(n-1)}{2} = \frac{n(n-1) \cdots (n-2a+1)}{a! \cdot 2^a} . \quad (4)$$

Lemma 4. *For integers n, a with $2 \leq a \leq n/2$, the condition (4) holds if and only if $(n, a) = (6, 3)$.*

Proof. Let $f_a(n) = (n-2)(n-3)\cdots(n-2a+1)$. Then the condition (4) is equivalent to the condition $f_a(n) = a! \cdot 2^{a-1}$. Now for each fixed a , the function $f_a(n)$ is monotonically increasing in n . When $a = 2$, we have $a! \cdot 2^{a-1} = 4$, $f_2(4) = 2$ and $f_2(5) = 6$, therefore the above-mentioned monotonicity of $f_a(n)$ implies that the condition (4) does not hold. From now on, we consider the case $a \geq 3$. Now we have

$$\begin{aligned} f_a(2a) &= (2a-2)(2a-3)\cdots 2 \cdot 1 \\ &= 2^{a-1}(a-1)! \cdot (2a-3)(2a-5)\cdots 3 \cdot 1 \\ &\geq 2^{a-1}(a-1)! \cdot a = 2^{a-1} \cdot a! , \end{aligned}$$

where the equality holds if and only if $a = 3$. Therefore, by the monotonicity of $f_a(n)$, the condition (4) does not hold for $a \geq 4$; while, for the case $a = 3$, the condition (4) holds if and only if $n = 2a = 6$. Hence, this lemma holds. \square

Theorem 1. *For $n \neq 6$, every automorphism of S_n is an inner automorphism.*

Proof. By Lemma 4 and the argument just before the lemma, if $n \neq 6$, then for any automorphism F of S_n , the image by F of any transposition in S_n has cycle type $(1^{n-2}2^1)$, i.e., it is a transposition as well. Therefore, F is an inner automorphism by Lemma 1. Hence, this theorem holds. \square

4 The Outer Automorphism of S_6

In this section, we show that an outer automorphism of S_6 exists, and it is “essentially” unique. Here, the “essentially” means that the outer automorphism of S_6 is uniquely determined except the difference of inner automorphisms; more precisely, we have the following result:

Theorem 2. *If F and G are outer automorphisms of S_6 , then we have $G = F \circ I$ for some inner automorphism I .*

Proof. First, in a way similar to the proof of Theorem 1, Lemma 4 and the argument just before the lemma imply that the images by F and by G of a transposition have cycle type (1^42^1) (i.e., it is a transposition) or (1^02^3) . Now in the first case, Lemma 1 implies that either F or G is an

inner automorphism, contradicting the assumption of the theorem. Hence, the images of any transposition by F and by G have cycle type $(1^0 2^3)$. Moreover, by the argument just before Lemma 4, the transpositions in S_6 are in one-to-one correspondence with the elements of S_6 with cycle type $(1^0 2^3)$ via both F and G . Now the automorphism $F^{-1} \circ G$ of S_6 maps any transposition to a transposition, therefore $F^{-1} \circ G$ is an inner automorphism by Lemma 1. By writing the $F^{-1} \circ G$ as I , we have $F \circ I = G$, therefore this theorem holds. \square

From now on, we show that the automorphism F mentioned in Section 1 indeed exists. Once it is done, the F is an outer automorphism by definition, and Theorem 2 implies that this is the unique outer automorphism except the difference of inner automorphisms. Now we note that, if such an F exists, then the property of the automorphism F implies the following:

(*) For any $f \in S_6$, if $f = t_1 t_2 \cdots t_k$ with adjacent transpositions t_i , then $F(f) = F(t_1)F(t_2) \cdots F(t_k)$ holds, where each $F(t_i)$ is the element of S_6 specified in Section 1.

We are going to define the desired map F by the condition (*). Owing to Proposition 3, such an element $f \in S_6$ can be written as $f = t_1 t_2 \cdots t_k$ as in the condition (*). The remaining task is to verify that, for any other expression $f = t'_1 t'_2 \cdots t'_{k'}$ as above, the resulting images of f defined by the two expressions of f coincide with each other. As mentioned in Section 2, the difference of the two expressions of f is deduced from combinations of the three kinds of relations (1), (2) and (3). On the other hand, a straightforward calculation using the precise values of $F(s_i)$ specified in the definition of F implies that, the left-hand sides of these relations are all mapped by the F to the identity permutation id . Namely,

$$\begin{aligned} \text{for (1): } & F(s_i)F(s_i) = \text{id} , \\ \text{for (2): } & F(s_{i-1})F(s_i)F(s_{i-1})F(s_i)F(s_{i-1})F(s_i) = \text{id} , \\ \text{for (3): } & F(s_i)F(s_j)F(s_i)F(s_j) = \text{id} . \end{aligned}$$

Then, the difference of the two expressions of f vanishes when these are mapped by F , therefore we have

$$F(t_1)F(t_2) \cdots F(t_k) = F(t'_1)F(t'_2) \cdots F(t'_{k'}) .$$

Hence, it follows that the automorphism F specified in Section 1 indeed exists.⁵ The argument above has derived the following theorem:

⁵This argument can of course be formalized by using terminology of group theory, but we omit it here for the sake of simplicity.

Theorem 3. *An outer automorphism of S_6 exists, and it is essentially unique in the sense as in Theorem 2.*

From now, we give some calculation results about the outer automorphism F . We quote the definition of F here for the sake of convenience (where we abbreviate the relation $F(x) = y$ to $x \mapsto y$):

$$\begin{aligned}(12) &\mapsto (12)(34)(56) \\ (23) &\mapsto (16)(24)(35) \\ (34) &\mapsto (14)(23)(56) \\ (45) &\mapsto (16)(25)(34) \\ (56) &\mapsto (13)(24)(56)\end{aligned}$$

First, we calculate the images by F of the other transpositions:

$$\begin{aligned}(13) &= (12)(23)(12) \mapsto (12)(34)(56) \cdot (16)(24)(35) \cdot (12)(34)(56) = (13)(25)(46) \\ (24) &= (23)(34)(23) \mapsto (16)(24)(35) \cdot (14)(23)(56) \cdot (16)(24)(35) = (13)(26)(45) \\ (35) &= (34)(45)(34) \mapsto (14)(23)(56) \cdot (16)(25)(34) \cdot (14)(23)(56) = (12)(36)(45) \\ (46) &= (45)(56)(45) \mapsto (16)(25)(34) \cdot (13)(24)(56) \cdot (16)(25)(34) = (12)(35)(46) \\ (14) &= (12)(24)(12) \mapsto (12)(34)(56) \cdot (13)(26)(45) \cdot (12)(34)(56) = (15)(24)(36) \\ (25) &= (23)(35)(23) \mapsto (16)(24)(35) \cdot (12)(36)(45) \cdot (16)(24)(35) = (15)(23)(46) \\ (36) &= (34)(46)(34) \mapsto (14)(23)(56) \cdot (12)(35)(46) \cdot (14)(23)(56) = (15)(26)(34) \\ (15) &= (12)(25)(12) \mapsto (12)(34)(56) \cdot (15)(23)(46) \cdot (12)(34)(56) = (14)(26)(35) \\ (26) &= (23)(36)(23) \mapsto (16)(24)(35) \cdot (15)(26)(34) \cdot (16)(24)(35) = (14)(25)(36) \\ (16) &= (12)(26)(12) \mapsto (12)(34)(56) \cdot (14)(25)(36) \cdot (12)(34)(56) = (16)(23)(45)\end{aligned}$$

Secondly, for each possible cycle type of elements of S_6 , we calculate the image by F of an element of S_6 having the cycle type:

$$\begin{aligned}(12)(34) &= (12) \cdot (34) \mapsto (12)(34)(56) \cdot (14)(23)(56) = (13)(24) \\ (12)(34)(56) &= (12)(34) \cdot (56) \mapsto (13)(24) \cdot (13)(24)(56) = (56) \\ (123) &= (12) \cdot (23) \mapsto (12)(34)(56) \cdot (16)(24)(35) = (154)(236) \\ (123)(45) &= (123) \cdot (45) \mapsto (154)(236) \cdot (16)(25)(34) = (124653) \\ (123)(456) &= (123)(45) \cdot (56) \mapsto (124653) \cdot (13)(24)(56) = (263) \\ (1234) &= (123) \cdot (34) \mapsto (154)(236) \cdot (14)(23)(56) = (2645) \\ (1234)(56) &= (1234) \cdot (56) \mapsto (2645) \cdot (13)(24)(56) = (13)(2546) \\ (12345) &= (1234) \cdot (45) \mapsto (2645) \cdot (16)(25)(34) = (14356) \\ (123456) &= (12345) \cdot (56) \mapsto (14356) \cdot (13)(24)(56) = (15)(234)\end{aligned}$$

By these results and Lemma 2, the cycle types of elements of S_6 are changed by applying the map F as follows: Types $(1^4 2^1)$ and (2^3) are exchanged; types $(1^3 3^1)$ and (3^2) are exchanged; types $(1^1 2^1 3^1)$ and (6^1) are exchanged; and any other type is not changed.

Acknowledgements. This note is motivated by a calculation during a discussion with Dr. Yasuhide Numata at Shinshu University (I remember that the explicit calculation to derive the outer automorphism was fairly complicated), so I would like to thank him.