THE SIGN OF A PERMUTATION

KEITH CONRAD

1. Introduction

Throughout this discussion, $n \geq 2$. Any cycle in S_n is a product of transpositions: the identity (1) is (12)(12), and a k-cycle with $k \geq 2$ can be written as

$$(i_1 i_2 \cdots i_k) = (i_1 i_2)(i_2 i_3) \cdots (i_{k-1} i_k).$$

For example, a 3-cycle (abc) – which means a, b, and c are distinct – can be written as

$$(abc) = (ab)(bc).$$

This is not the only way to write (abc) using transpositions, *e.g.*, $(abc) = (bc)(ac) = (ac)(ab)$.

Since any permutation in S_n is a product of cycles and any cycle is a product of transpositions, any permutation in S_n is a product of transpositions.[1] Unlike the unique decomposition of a permutation into a product of disjoint cycles, the decomposition of a permutation as a product of transpositions is almost never into disjoint transpositions: there will usually be overlaps in the numbers moved by different transpositions.

Example 1.1. Let $\sigma = (15243)$. Then two expressions for σ as a product of transpositions are

$$\sigma = (15)(52)(24)(43)$$

and

$$\sigma = (12)(34)(23)(12)(23)(34)(45)(34)(23)(12).$$

Example 1.2. Let $\sigma = (13)(132)(243)$. Note the cycles here are not disjoint. Expressions of σ as a product of transpositions include

$$\sigma = (24)$$

and

$$\sigma = (13)(12)(13)(34)(23).$$

Write a general permutation $\sigma \in S_n$ as

$$\sigma = \tau_1 \tau_2 \cdots \tau_r,$$

where the τ_i's are transpositions and r is the number of transpositions. Although the τ_i's are not determined uniquely, there is a fundamental parity constraint: $r \bmod 2$ is determined uniquely. For instance, the two expressions for (15243) in Example 1.1 involve 4 and 10 transpositions, which are both even. It is impossible to write (15243) as the product of an odd number of transpositions. In Example 1.2, the permutation (13)(132)(243) is

[1] We can prove that every permutation in S_n is a product of transpositions without mentioning cycles, by using *biology*. If n objects were placed in front of you and you were asked to rearrange them in any particular way, you could do it by swapping objects two at a time with your two hands. I heard this argument from Ryan Kinser.

written as a product of 1 and 5 transpositions, which are both odd. It impossible to write (13)(132)(243) as a product of an even number of transpositions.

Once we see that $r \bmod 2$ is intrinsic to σ, we will be able to assign a label (even or odd) or a sign (1 or -1) to each permutation. This will lead to an important subgroup of S_n, the alternating group A_n, whose size is $n!/2$.

2. Definition of the sign

Theorem 2.1. *Write $\sigma \in S_n$ as a product of transpositions in two ways:*

$$\sigma = \tau_1\tau_2\cdots\tau_r = \tau_1'\tau_2'\cdots\tau_{r'}'.$$

Then $r \equiv r' \bmod 2$.

Proof. We can combine the products to get a representation of the identity permutation as a product of $r + r'$ transpositions:

$$(1) = \sigma\sigma^{-1} = \tau_1\tau_2\cdots\tau_r\tau_{r'}'\tau_{r'-1}'\cdots\tau_1'.$$

(Note $\tau^{-1} = \tau$ for any transposition τ and inverting a product reverses the order of multiplication.) Thus, it suffices to show the identity permutation can only be written as a product of an *even* number of transpositions. Then $r + r'$ is even, so we will have $r \equiv r' \bmod 2$.

Starting anew, in S_n write the identity as some product of transpositions:

$$(1) = (a_1b_1)(a_2b_2)\cdots(a_kb_k), \tag{2.1}$$

where $k \geq 1$ and $a_i \neq b_i$ for all i. We will prove k is even.

The product on the right side of (2.1) can't have $k = 1$ since it is the identity. It could have $k = 2$. Suppose, by induction, that $k \geq 3$ and we know any product of fewer than k transpositions that equals the identity involves an even number of transpositions.

One of the transpositions (a_ib_i) for $i = 2, 3, \ldots, k$ has to move a_1 (otherwise the overall product on the right side of (2.1) is not the identity permutation). That is, a_1 must be one of the a_i's for $i > 1$ (after interchanging the roles of a_i and b_i if necessary). Using different letters to denote different numbers, the formulas

$$(cd)(ab) = (ab)(cd), \quad (bc)(ab) = (ac)(bc)$$

show any product of two transpositions in which the second factor moves a and the first factor does not move a can be rewritten as a product of two transpositions in which the first factor moves a and the second factor does not move a. Therefore, *without changing the number of transpositions* in (2.1), we can push the position of the second most left transposition in (2.1) that moves a_1 to the position right after (a_1b_1), and thus we can *assume* $a_2 = a_1$.

If $b_2 = b_1$, then the product $(a_1b_1)(a_2b_2)$ in (2.1) is the identity and we can remove it. This reduces (2.1) to a product of $k - 2$ transpositions. By induction, $k - 2$ is even so k is even.

If instead $b_2 \neq b_1$ then the product of the first two terms in (2.1) is $(a_1b_1)(a_1b_2)$ with $b_1 \neq b_2$, and this is equal to $(a_1b_2)(b_1b_2)$. Therefore (2.1) can be rewritten as

$$(1) = (a_1b_2)(b_1b_2)(a_3b_3)\cdots(a_kb_k), \tag{2.2}$$

where only the first two factors on the right have been changed. Now run through the argument again with (2.2) in place of (2.1). It involves the same number k of transpositions, but there are fewer transpositions in the product that move a_1 since we used to have (a_1b_1)

and (a_1b_2) in the product and now we have (a_1b_2) and (b_1b_2).[2] Some transposition other than (a_1b_2) in the new product (2.2) must move a_1, so by the same argument as before either we will be able to reduce the number of transpositions by 2 and be done by induction or we will be able to rewrite the product to have the same total number of transpositions but drop by 1 the number of them that move a_1. This rewriting process eventually has to fall into the case where the first two transpositions cancel out, since we can't wind up with (1) as a product of transpositions where only the first one moves a_1. Thus we will be able to see that k is even. □

Remark 2.2. The bibliography at the end contains references to many different proofs of Theorem 2.1. The proof given above is adapted from [12].

Definition 2.3. When a permutation in S_n can be written as a product of r transpositions, we call $(-1)^r$ its *sign*:

$$\sigma = \tau_1\tau_2\cdots\tau_r \Longrightarrow \operatorname{sgn}(\sigma) = (-1)^r.$$

Permutations with sign 1 are called *even* and those with sign -1 are called *odd*. This label is also called the *parity* of the permutation.

Theorem 2.1 tells us that the r in Definition 2.3 has a well-defined value modulo 2, so the sign of a permutation does make sense.

Example 2.4. The permutation in Example 1.1 has sign 1 (it is even) and the permutation in Example 1.2 has sign -1 (it is odd).

Example 2.5. Any transposition in S_n has sign -1 and is odd.

Example 2.6. The identity is (12)(12), so it has sign 1 and is even.

Example 2.7. The permutation (143)(26) is (14)(43)(26), a product of three transpositions, so it has sign -1.

Example 2.8. The 3-cycle (123) is (12)(23), a product of 2 transpositions, so $\operatorname{sgn}(123) = 1$.

Example 2.9. What is the sign of a k-cycle? Since

$$(i_1i_2\cdots i_k) = (i_1i_2)(i_2i_3)\cdots(i_{k-1}i_k),$$

which involves $k-1$ transpositions,

$$\operatorname{sgn}(i_1i_2\cdots i_k) = (-1)^{k-1}.$$

In words, if a cycle has even length then its sign is -1, and if a cycle has odd length its sign is 1. This is because the exponent in the sign formula is $k-1$, not k. To remember that the parity of a cycle is 'opposite' to the parity of its length (a cycle of odd length is even and a cycle of even length is odd), just remember that 2-cycles (the transpositions) are odd.

The sign is a function $S_n \to \{\pm 1\}$. It takes on both values (when $n \geq 2$): the identity has sign 1 and any transposition has sign -1. Moreover, the sign is multiplicative in the following sense.

Theorem 2.10. *For $\sigma, \sigma' \in S_n$, $\operatorname{sgn}(\sigma\sigma') = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma')$.*

[2] Since (a_1b_1) and (a_1b_2) were assumed all along to be honest transpositions, b_1 and b_2 do not equal a_1, so (b_1b_2) doesn't move a_1.

Proof. If σ is a product of k transpositions and σ' is a product of k' transpositions, then $\sigma\sigma'$ can be written as a product of $k+k'$ transpositions. Therefore

$$\mathrm{sgn}(\sigma\sigma') = (-1)^{k+k'} = (-1)^k(-1)^{k'} = \mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma').$$

□

Corollary 2.11. *Inverting and conjugating a permutation do not change its sign.*

Proof. Since $\mathrm{sgn}(\sigma\sigma^{-1}) = \mathrm{sgn}(1) = 1$,

$$\mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma^{-1}) = 1.$$

Therefore $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1} = \mathrm{sgn}(\sigma)$. Similarly, if $\sigma' = \pi\sigma\pi^{-1}$, then

$$\mathrm{sgn}(\sigma') = \mathrm{sgn}(\pi)\mathrm{sgn}(\sigma)\mathrm{sgn}(\pi^{-1}) = \mathrm{sgn}(\sigma).$$

□

Theorem 2.10 lets us compute signs without having to decompose permutations into products of transpositions or into a product of disjoint cycles. *Any* decomposition of the permutation into a product of cycles will suffice: disjointness of the cycles is not necessary! Just remember the parity of a cycle is determined by its length and has opposite parity to the length (*e.g.*, transpositions have sign -1). For instance, in Example 1.1, σ is a 5-cycle, so $\mathrm{sgn}(\sigma) = 1$. In Example 1.2,

$$\mathrm{sgn}((13)(132)(243)) = \mathrm{sgn}(13)\mathrm{sgn}(132)\mathrm{sgn}(243) = (-1)(1)(1) = -1.$$

3. A second description of the sign

One place signs of permutations show up elsewhere in mathematics is in a formula for the determinant. Given an $n \times n$ matrix (a_{ij}), its determinant is a long sum of products taken n terms at a time, and assorted plus and minus sign coefficients. These plus and minus signs are exactly signs of permutations:

$$\det(a_{ij}) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

For example, taking $n = 2$,

$$\det\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \mathrm{sgn}(1)a_{11}a_{22} + \mathrm{sgn}(12)a_{12}a_{21} = a_{11}a_{22} - a_{12}a_{21}.$$

In fact, determinants provide an alternate way of thinking about the sign of a permutation. For $\sigma \in S_n$, let $T_\sigma \colon \mathbf{R}^n \to \mathbf{R}^n$ by the rule

$$T_\sigma(c_1\mathbf{e}_1 + \cdots + c_n\mathbf{e}_n) = c_1\mathbf{e}_{\sigma(1)} + \cdots + c_n\mathbf{e}_{\sigma(n)}.$$

In other words, send $\mathbf{e}_i$ to $\mathbf{e}_{\sigma(i)}$ and extend by linearity to all of $\mathbf{R}^n$. This transformation permutes the standard basis of $\mathbf{R}^n$ according to the way σ permutes $\{1, 2, \ldots, n\}$. Writing T_σ as a matrix provides a realization of σ as a matrix where each row and each column has a single 1. These are called permutation matrices.

Example 3.1. Let $\sigma = (123)$ in S_3. Then $T_\sigma(\mathbf{e}_1) = \mathbf{e}_2$, $T_\sigma(\mathbf{e}_2) = \mathbf{e}_3$, and $T_\sigma(\mathbf{e}_3) = \mathbf{e}_1$. As a matrix,

$$[T_\sigma] = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Example 3.2. Let $\sigma = (13)(24)$ in S_4. Then

$$[T_\sigma] = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The correspondence $\sigma \mapsto T_\sigma$ is multiplicative: $T_{\sigma_1}(T_{\sigma_2}\mathbf{e}_i) = T_{\sigma_1}(\mathbf{e}_{\sigma_2(i)}) = \mathbf{e}_{\sigma_1(\sigma_2(i))}$, which is $T_{\sigma_1\sigma_2}(\mathbf{e}_i)$, so by linearity $T_{\sigma_1}T_{\sigma_2} = T_{\sigma_1\sigma_2}$. Taking determinants, $\det(T_{\sigma_1})\det(T_{\sigma_2}) = \det(T_{\sigma_1\sigma_2})$. What is $\det(T_\sigma)$? Since T_σ has a single 1 in each row and column, the sum for $\det(T_\sigma)$ contains a single non-zero term corresponding to the permutation of $\{1, 2, \ldots, n\}$ associated to σ. This term is $\operatorname{sgn}(\sigma)$, so $\det(T_\sigma) = \operatorname{sgn}(\sigma)$. In words, *the sign of a permutation is the determinant of the associated permutation matrix*. Since the permutation matrices are multiplicative, as is the determinant, we have a new way of understanding why the sign is multiplicative.

4. A third description of the sign

While the sign on S_n was defined in terms of concrete computations, its algebraic property in Theorem 2.10 turns out to characterize it.

Theorem 4.1. *For $n \geq 2$, let $h\colon S_n \to \{\pm 1\}$ satisfy $h(\sigma\sigma') = h(\sigma)h(\sigma')$ for all $\sigma, \sigma' \in S_n$. Then $h(\sigma) = 1$ for all σ or $h(\sigma) = \operatorname{sgn}(\sigma)$ for all σ. Thus, if h is multiplicative and not identically 1, then $h = \operatorname{sgn}$.*

Proof. The main idea is to show h is determined by its value at a single transposition, say $h(12)$. We may suppose $n > 2$, as the result is trivial if $n = 2$.

Step 1: For any transposition τ, $h(\tau) = h(12)$.

Any transposition other than (12) moves at most one of 1 and 2. First we treat transpositions moving either 1 or 2 (but not both). Then we treat transpositions moving neither 1 nor 2.

Any transposition that moves 1 but not 2 has the form $(1b)$, where $b > 2$. Check that

$$(1b) = (2b)(12)(2b),$$

so applying h to both sides of this equation gives us

$$h(1b) = h(2b)h(12)h(2b) = (h(2b))^2 h(12) = h(12).$$

Notice that, although (12) and $(2b)$ do not commute in S_n, their h-values do commute since h takes values in $\{\pm 1\}$, which is commutative. The case of a transposition moving 2 but not 1 is analogous.

Now suppose our transposition moves neither 1 nor 2, so it is (ab), where a and b both exceed 2. Check that

$$(ab) = (1a)(2b)(12)(2b)(1a).$$

Applying h to both sides,

$$h(ab) = h(1a)h(2b)h(12)h(2b)h(1a) = h(1a)^2 h(2b)^2 h(12) = h(12).$$

Step 2: Computation of $h(\sigma)$ for any σ.

Suppose σ is a product of k transpositions. By Step 1, all transpositions have the same h-value, say $u \in \{\pm 1\}$, so $h(\sigma) = u^k$ If $u = 1$, then $h(\sigma) = 1$ for all σ. If $u = -1$, then $h(\sigma) = (-1)^k = \operatorname{sgn}(\sigma)$ for all σ. $\square$

5. The Alternating Group

The n-th *alternating group* A_n is the group of even permutations in S_n. That is, a permutation is in A_n when it is a product of an even number of transpositions. Such products are clearly closed under multiplication and inversion, so A_n is a subgroup of S_n. Alternatively,

$$A_n = \{\sigma \in S_n : \operatorname{sgn}(\sigma) = 1\}.$$

Therefore by Theorem 2.10 it is easy to see that A_n is a group.

Example 5.1. Take $n = 2$. Then $S_2 = \{(1), (12)\}$ and $A_2 = \{(1)\}$.

Example 5.2. Take $n = 3$. Then $A_3 = \{(1), (123), (132)\}$, which is cyclic (either non-identity element is a generator).

Example 5.3. The group A_4 consists of 12 permutations of $1, 2, 3, 4$:

$$(1),\ (123),\ (132),\ (124),\ (142),\ (134),\ (143),\ (234),\ (243),\ (12)(34),\ (13)(24),\ (14)(23).$$

Example 5.4. Any 3-cycle is even, so A_n contains all 3-cycles when $n \geq 3$. In particular, A_n is non-abelian for $n \geq 4$ since (123) and (124) do not commute.

Although we have not defined the sign on S_1, the group S_1 is trivial so let's just declare the sign to be 1 on S_1. Then $A_1 = S_1$.

Remark 5.5. The reason for the label 'alternating' in the name of A_n is connected with the behavior of the multi-variable polynomial

$$\prod_{1 \leq i < j \leq n} (X_j - X_i) \tag{5.1}$$

under a permutation of its variables. Here is what it looks like when $n = 2, 3, 4$:

$$X_2 - X_1, \quad (X_3 - X_2)(X_3 - X_1)(X_2 - X_1),$$

$$(X_4 - X_3)(X_4 - X_2)(X_4 - X_1)(X_3 - X_2)(X_3 - X_1)(X_2 - X_1).$$

The polynomial (5.1) is a product of $\binom{n}{2}$ terms.

When the variables are permuted, the polynomial will change at most by an overall sign. For example, if we exchange X_1 and X_2 then $(X_3 - X_2)(X_3 - X_1)(X_2 - X_1)$ becomes $(X_3 - X_1)(X_3 - X_2)(X_1 - X_2)$, which is $-(X_3 - X_2)(X_3 - X_1)(X_2 - X_1)$; the 3rd alternating polynomial changed by a sign. In general, rearranging the variables in (5.1) by a permutation $\sigma \in S_n$ changes the polynomial by the sign of that permutation:

$$\prod_{i<j} (X_{\sigma(j)} - X_{\sigma(i)}) = \operatorname{sgn}(\sigma) \prod_{i<j} (X_j - X_i).$$

A polynomial whose value changes by an overall sign, either 1 or -1, when any two variables are permuted is called an *alternating* polynomial. The product (5.1) is the most basic example of an alternating polynomial in n variables. A permutation of the variables leaves (5.1) unchanged precisely when the sign of the permutation is 1. This is why the group of permutations of the variables that preserve (5.1) is called the alternating group.

How large is A_n?

Theorem 5.6. *For $n \geq 2$, $\#A_n = n!/2$.*

Proof. Pick a transposition, say $\tau = (12)$. Then $\tau \notin A_n$. If $\sigma \notin A_n$, then $\mathrm{sgn}(\sigma\tau) = (-1)(-1) = 1$, so $\sigma\tau \in A_n$. Therefore $\sigma \in A_n\tau$, where we write $A_n\tau$ to mean the set of permutations of the form $\pi\tau$ for $\pi \in A_n$. Thus, we have a decomposition of S_n into two parts:

$$S_n = A_n \cup A_n\tau. \tag{5.2}$$

This union is disjoint, since every element of A_n has sign 1 and every element of $A_n\tau$ has sign -1. Moreover, $A_n\tau$ has the same size as A_n (multiplication on the right by τ swaps the two subsets), so (5.2) tells us $n! = 2\#A_n$. □

Here are the sizes of the smallest symmetric and alternating groups.

n	1	2	3	4	5	6	7
$\#S_n$	1	2	6	24	120	720	5040
$\#A_n$	1	1	3	12	60	360	2520

References

[1] T. L. Bartlow, An historical note on the parity of permutations, *Amer. Math. Monthly* **79** (1972), 766–769.

[2] J. L. Brenner, A new proof that no permutation is both even and odd, *Amer. Math. Monthly* **74** (1957), 499–500.

[3] P. Cartier, Remarques sur la signature d'une permutation, *Enseign. Math.* **16** (1970), 7–19.

[4] E. L. Gray, An alternate proof for the invariance of parity of a permutation written as a product of transpositions, *Amer. Math. Monthly* **70** (1963), 995.

[5] I. Halperin, Odd and even permutations, *Canadian Math. Bull.* **3** (1960), 185–186.

[6] D. Higgs and P. de Witte, On products of transpositions and their graphs, *Amer. Math. Monthly* **86** (1979), 376–380.

[7] H. Liebeck, Even and odd permutations, *Amer. Math. Monthly* **76** (1969), 668.

[8] W. I. Miller, Even and odd permutations, *MATYC Journal* **5** (1971), 32.

[9] S. Nelson, Defining the sign of a permutation, *Amer. Math. Monthly* **94** (1987), 543–545.

[10] R. K. Oliver, On the parity of a permutation, *Amer. Math. Monthly* **118** (2011), 734–735.

[11] W. Phillips, On the definition of even and odd permutations, *Amer. Math. Monthly* **74** (1967), 1249–1251.

[12] E. L. Spitznagel, Note on the alternating group, *Amer. Math. Monthly* **75** (1968), 68–69.

[13] C. Weil, Another approach to the alternating subgroup of the symmetric group, *Amer. Math. Monthly* **71** (1964), 545–546.