# THE SIGN OF A PERMUTATION 

KEITH CONRAD

## 1. Introduction

Throughout this discussion, $n \geq 2$. Each 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

$$
\left(i_{1} i_{2} \cdots i_{k}\right)=\left(i_{1} i_{2}\right)\left(i_{2} i_{3}\right) \cdots\left(i_{k-1} i_{k}\right)
$$

For example, a 3-cycle $(a b c)$ - which implicitly means $a, b$, and $c$ are distinct - is a product of two transpositions:

$$
(a b c)=(a b)(b c)
$$

This is not the only way to write $(a b c)$ using transpositions, e.g., $(a b c)=(b c)(a c)=(a c)(a b)$.
Since each permutation in $S_{n}$ is a product of cycles and each cycle is a product of transpositions, each permutation in $S_{n}$ is a product of transpositions. ${ }^{1}$ Although every permutation is a product of disjoint cycles and those cycles are unique up to order (they commute), a permutation is almost never a product of disjoint transpositions since a product of disjoint transpositions has order at most 2 .

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

$$
\sigma=(24)
$$

and

$$
\sigma=(13)(13)(32)(24)(43)
$$

Write a general permutation $\sigma \in S_{n}$ as

$$
\sigma=\tau_{1} \tau_{2} \cdots \tau_{r}
$$

where the $\tau_{i}$ 's are transpositions and $r$ is the number of transpositions. Although the $\tau_{i}$ 's are not determined uniquely, there is a fundamental parity constraint: $r$ mod 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

[^0]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 uniquely determined for $\sigma$, it will make sense to refer to $\sigma$ as an even permutation if $r$ is even and an odd permutation if $r$ is odd. 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:

$$
\begin{equation*}
\sigma=\tau_{1} \tau_{2} \cdots \tau_{r}=\tau_{1}^{\prime} \tau_{2}^{\prime} \cdots \tau_{r^{\prime}}^{\prime} \tag{2.1}
\end{equation*}
$$

Then $r \equiv r^{\prime} \bmod 2$.
Proof. The two products of transpositions that equal $\sigma$ in (2.1) lead to an expression of the identity permutation as a product of $r+r^{\prime}$ transpositions:

$$
\text { (1) }=\sigma \sigma^{-1}=\tau_{1} \tau_{2} \cdots \tau_{r} \tau_{r^{\prime}}^{\prime} \tau_{r^{\prime}-1}^{\prime} \cdots \tau_{1}^{\prime} .
$$

(Note $\tau^{-1}=\tau$ for transpositions $\tau$ and inverting a product reverses the order of multiplication.)

Claim: A product of transpositions that is (1) must use an even number of transpositions. This claim forces $r+r^{\prime}$ above to be even, so $r \equiv r^{\prime} \bmod 2$, which is what we wanted.
To prove the claim, write (1) in $S_{n}$ as a product of $k$ transpositions:

$$
\begin{equation*}
(1)=\left(a_{1} b_{1}\right)\left(a_{2} b_{2}\right) \cdots\left(a_{k} b_{k}\right), \tag{2.2}
\end{equation*}
$$

where $k \geq 1$ and $a_{i} \neq b_{i}$ for all $i$. We want to show $k$ is even and will prove this by induction on $k .^{2}$

The product on the right side of (2.2) can't have $k=1$ since a single transposition is not (1). We could have $k=2$, which is even. Suppose, by induction, that $k \geq 3$ and every product of fewer than $k$ transpositions that equals (1) uses an even number of transpositions.

In (2.2), some transposition $\left(a_{i} b_{i}\right)$ for $i>1$ has to move $a_{1}$ (otherwise the overall product on the right side of (2.2) sends $a_{1}$ to $b_{1}$, which is not the identity permutation). So $a_{1}$ must be an $a_{i}$ or $b_{i}$ for $i>1$. Since $\left(a_{i} b_{i}\right)=\left(b_{i} a_{i}\right)$, we can suppose $a_{i}$ is $a_{1}$. The two equations

$$
(c d)(a b)=(a b)(c d), \quad(b c)(a b)=(a c)(b c),
$$

where different letters are different numbers, show a product of two transpositions where the one on the right moves $a$ and the one on the left does not move $a$ can be rewritten as a product of two transpositions in which the one on the left moves $a$ and the one on the right does not move $a$. Call these two equations rewriting rules. In (2.2) they let us rewrite the overall product without changing the number of transpositions so that the transposition $\left(a_{2} b_{2}\right)$ moves $a_{1}$, meaning $a_{2}$ or $b_{2}$ is $a_{1}$. Without loss of generality, $a_{2}=a_{1}$. Now consider the cases $b_{2}=b_{1}$ and $b_{2} \neq b_{1}$.

Case 1: $b_{2}=b_{1}$. The product $\left(a_{1} b_{1}\right)\left(a_{2} b_{2}\right)$ in (2.2) is $\left(a_{1} b_{1}\right)\left(a_{1} b_{1}\right)$, which is the identity and can be removed. This turns the right side of (2.2) into a product of $k-2$ transpositions. By induction, $k-2$ is even so $k=(k-2)+2$ is even.

Case 2: $b_{2} \neq b_{1}$. Check $\left(a_{1} b_{1}\right)\left(a_{2} b_{2}\right)$ in (2.2), which is $\left(a_{1} b_{1}\right)\left(a_{1} b_{2}\right)$, can be written as $\left(a_{1} b_{2}\right)\left(b_{1} b_{2}\right)$ since $a_{1}, b_{1}$, and $b_{2}$ are all different. Then (2.2) can be rewritten as

$$
\begin{equation*}
(1)=\left(a_{1} b_{2}\right)\left(b_{1} b_{2}\right)\left(a_{3} b_{3}\right) \cdots\left(a_{k} b_{k}\right), \tag{2.3}
\end{equation*}
$$

[^1]where only the first two transpositions have been changed. The product on the right involves the same number $k$ of transpositions as before, but there are fewer transpositions in (2.3) that move $a_{1}$ than we had in (2.2) since the start of the product in (2.2) is $\left(a_{1} b_{1}\right)\left(a_{1} b_{2}\right)$ and in $(2.3)$ it is $\left(a_{1} b_{2}\right)\left(b_{1} b_{2}\right) .{ }^{3}$

Since the overall product in (2.3) is (1), some transposition besides $\left(a_{1} b_{1}\right)$ moves $a_{1}$. The transposition $\left(b_{1} b_{2}\right)$ in (2.3) does not move $a_{1}$, so by using the rewriting rules above with (2.3) in place of (2.2), we land again in either Case 1, which lets us drop the number of transpositions by 2 and then we're done by induction, or in Case 2, which lets us lower the overall number of transpositions moving $a_{1}$ by 1 without changing the total number $k$ of transpositions.

When (1) is a product of transpositions with the leftmost transposition moving $a_{1}$, there is always another transposition in the product moving $a_{1}$. Since Case 2 reduces that number by 1 without changing the number of transpositions, after enough steps we can't be in Case 2 anymore, so we have to be in Case 1 and then we are done by induction.

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 [15].

Definition 2.3. When a permutation $\sigma$ in $S_{n}$ can be written as a product of $r$ transpositions, we call $(-1)^{r}$ the sign of $\sigma$ :

$$
\operatorname{sgn}(\sigma)=(-1)^{r} \text { if } \sigma=\tau_{1} \tau_{2} \cdots \tau_{r}
$$

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. ${ }^{4}$

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 makes 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. Each 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

$$
\left(i_{1} i_{2} \cdots i_{k}\right)=\left(i_{1} i_{2}\right)\left(i_{2} i_{3}\right) \cdots\left(i_{k-1} i_{k}\right)
$$

which involves $k-1$ transpositions,

$$
\operatorname{sgn}\left(i_{1} i_{2} \cdots i_{k}\right)=(-1)^{k-1}
$$

[^2]In words, a cycle with even length has sign -1 and a cycle with odd length has sign 1 . This is because the exponent in the sign formula above 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), remember that 2-cycles (transpositions) are odd.

The sign is a function $S_{n} \rightarrow\{ \pm 1\}$. It has both values (when $n \geq 2$ ): the identity has sign 1 and a transposition has sign -1 . Also, the sign is multiplicative in the following sense.

Theorem 2.10. For $\sigma, \sigma^{\prime} \in S_{n}, \operatorname{sgn}\left(\sigma \sigma^{\prime}\right)=\operatorname{sgn}(\sigma) \operatorname{sgn}\left(\sigma^{\prime}\right)$.
Proof. If $\sigma$ is a product of $k$ transpositions and $\sigma^{\prime}$ is a product of $k^{\prime}$ transpositions, then $\sigma \sigma^{\prime}$ can be written as a product of $k+k^{\prime}$ transpositions. Therefore

$$
\operatorname{sgn}\left(\sigma \sigma^{\prime}\right)=(-1)^{k+k^{\prime}}=(-1)^{k}(-1)^{k^{\prime}}=\operatorname{sgn}(\sigma) \operatorname{sgn}\left(\sigma^{\prime}\right)
$$

Corollary 2.11. Inverting and conjugating a permutation do not change its sign.
Proof. Since $\operatorname{sgn}\left(\sigma \sigma^{-1}\right)=\operatorname{sgn}(1)=1, \operatorname{sgn}(\sigma) \operatorname{sgn}\left(\sigma^{-1}\right)=1$, $\operatorname{so} \operatorname{sgn}\left(\sigma^{-1}\right)=\operatorname{sgn}(\sigma)^{-1}=$ $\operatorname{sgn}(\sigma)$. Similarly, if $\sigma^{\prime}=\pi \sigma \pi^{-1}$, then

$$
\operatorname{sgn}\left(\sigma^{\prime}\right)=\operatorname{sgn}(\pi) \operatorname{sgn}(\sigma) \operatorname{sgn}\left(\pi^{-1}\right)=\operatorname{sgn}(\sigma)
$$

Theorem 2.10 lets us compute signs of permutations using any decomposition into a product of cycles: disjointness of the cycles is not needed. Just remember that a cycle's parity is determined by its length and is opposite to the parity of its length (e.g., transpositions have length 2 and sign -1 ). For instance, in Example 1.1, $\sigma$ is a 5 -cycle, $\operatorname{so} \operatorname{sgn}(\sigma)=1$. In Example 1.2,

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

## 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 ( $a_{i j}$ ), 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 signs of permutations:

$$
\operatorname{det}\left(a_{i j}\right)=\sum_{\sigma \in S_{n}} \operatorname{sgn}(\sigma) a_{1, \sigma(1)} a_{2, \sigma(2)} \cdots a_{n, \sigma(n)} .
$$

For example, taking $n=2$,

$$
\operatorname{det}\left(\begin{array}{ll}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{array}\right)=\operatorname{sgn}(1) a_{11} a_{22}+\operatorname{sgn}(12) a_{12} a_{21}=a_{11} a_{22}-a_{12} a_{21}
$$

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

$$
T_{\sigma}\left(x_{1} \mathbf{e}_{1}+\cdots+x_{n} \mathbf{e}_{n}\right)=x_{1} \mathbf{e}_{\sigma(1)}+\cdots+x_{n} \mathbf{e}_{\sigma(n)}
$$

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 $\sigma$ permutes $\{1,2, \ldots, n\}$. Writing $T_{\sigma}$ as a matrix provides a realization of $\sigma$ 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 $T_{\sigma}\left(\mathbf{e}_{1}\right)=\mathbf{e}_{2}, T_{\sigma}\left(\mathbf{e}_{2}\right)=\mathbf{e}_{3}$, and $T_{\sigma}\left(\mathbf{e}_{3}\right)=\mathbf{e}_{1}$. As a matrix,

$$
\left[T_{\sigma}\right]=\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0
\end{array}\right)
$$

Example 3.2. Let $\sigma=(13)(24)$ in $S_{4}$. Then

$$
\left[T_{\sigma}\right]=\left(\begin{array}{llll}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{array}\right)
$$

The correspondence $\sigma \mapsto T_{\sigma}$ is multiplicative: $T_{\sigma_{1}}\left(T_{\sigma_{2}} \mathbf{e}_{i}\right)=T_{\sigma_{1}}\left(\mathbf{e}_{\sigma_{2}(i)}\right)=\mathbf{e}_{\sigma_{1}\left(\sigma_{2}(i)\right)}$, which is $T_{\sigma_{1} \sigma_{2}}\left(\mathbf{e}_{i}\right)$, so by linearity $T_{\sigma_{1}} T_{\sigma_{2}}=T_{\sigma_{1} \sigma_{2}}$. Taking determinants, $\operatorname{det}\left(T_{\sigma_{1}}\right) \operatorname{det}\left(T_{\sigma_{2}}\right)=$ $\operatorname{det}\left(T_{\sigma_{1} \sigma_{2}}\right)$. What is $\operatorname{det}\left(T_{\sigma}\right)$ ? Since $T_{\sigma}$ has a single 1 in each row and column, the sum for $\operatorname{det}\left(T_{\sigma}\right)$ contains a single nonzero term corresponding to the permutation of $\{1,2, \ldots, n\}$ associated to $\sigma$. This term is $\operatorname{sgn}(\sigma)$, so $\operatorname{det}\left(T_{\sigma}\right)=\operatorname{sgn}(\sigma)$. In words, the sign of a permutation is the determinant of the associated permutation matrix. Since permutation matrices are multiplicative, as is the determinant, this gives us a new way of understanding why the sign of permutations 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 $h: S_{n} \rightarrow\{ \pm 1\}$ satisfy $h\left(\sigma \sigma^{\prime}\right)=h(\sigma) h\left(\sigma^{\prime}\right)$ for all $\sigma, \sigma^{\prime} \in S_{n}$. Then $h(\sigma)=1$ for all $\sigma$ or $h(\sigma)=\operatorname{sgn}(\sigma)$ for all $\sigma$. Thus, if $h$ is multiplicative and not identically 1, then $h=$ 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 every transposition $\tau, h(\tau)=h(12)$.
$\overline{\mathrm{A} \text { transposition other than (12) moves at most one of } 1 \text { and 2. First we treat transposi- }}$ tions moving either 1 or 2 (but not both). Then we treat transpositions moving neither 1 nor 2.

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

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

so applying $h$ to both sides of this equation gives us

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

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 ( $a b$ ), where $a$ and $b$ both exceed 2. Check that

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

Applying $h$ to both sides,

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

Step 2: Computation of $h(\sigma)$ for each $\sigma$.
Suppose $\sigma$ 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 $\sigma$. If $u=-1$, then $h(\sigma)=(-1)^{k}=\operatorname{sgn}(\sigma)$ for all $\sigma$.

Theorem 4.1 has an application to physics. In quantum mechanics, each state of a system is modeled by a one-dimensional subspace of a certain vector space. In a quantum system of $n$ identical particles (such as $n$ electrons) rearrangements of the particles are indistinguishable, so the one-dimensional subspace representing the system leads by the axioms of quantum mechanics to a multiplicative function $S_{n} \rightarrow\{ \pm 1\}$. By Theorem 4.1 this function is either identically 1 or the sign, which is related to the classification of particles into two symmetry types: bosons and fermions.

## 5. The Alternating Group

The identity permutation is even, and by Theorem 2.10 the product of even permutations is even. A permutation and its inverse are a product of the same number of transpositions (why?), so the inverse of an even permutation is even. This means the set of even permutations in $S_{n}$ is a subgroup. Its called the $n$-th alternating group $A_{n}$ :

$$
A_{n}=\left\{\sigma \in S_{n}: \operatorname{sgn}(\sigma)=1\right\}
$$

Remember: a permutation is in $A_{n}$ when it is a product of an even number of transpositions.
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 nonidentity 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. Every 3 -cycle is even, so $A_{n}$ contains all 3 -cycles when $n \geq 3$. In particular, $A_{n}$ is nonabelian 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

$$
\begin{equation*}
\prod_{1 \leq i<j \leq n}\left(X_{j}-X_{i}\right) \tag{5.1}
\end{equation*}
$$

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

$$
\begin{gathered}
X_{2}-X_{1}, \quad\left(X_{3}-X_{2}\right)\left(X_{3}-X_{1}\right)\left(X_{2}-X_{1}\right), \\
\left(X_{4}-X_{3}\right)\left(X_{4}-X_{2}\right)\left(X_{4}-X_{1}\right)\left(X_{3}-X_{2}\right)\left(X_{3}-X_{1}\right)\left(X_{2}-X_{1}\right) .
\end{gathered}
$$

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 $\left(X_{3}-X_{2}\right)\left(X_{3}-X_{1}\right)\left(X_{2}-X_{1}\right)$ becomes $\left(X_{3}-X_{1}\right)\left(X_{3}-X_{2}\right)\left(X_{1}-X_{2}\right)$, which is $-\left(X_{3}-X_{2}\right)\left(X_{3}-X_{1}\right)\left(X_{2}-X_{1}\right)$; 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:

$$
\prod_{i<j}\left(X_{\sigma(j)}-X_{\sigma(i)}\right)=\operatorname{sgn}(\sigma) \prod_{i<j}\left(X_{j}-X_{i}\right)
$$

A polynomial whose value changes by an overall sign, either 1 or -1 , when each pair of its variables is 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 $n \geq 2,\left|A_{n}\right|=n!/ 2$.
Proof. Pick a transposition, say $\tau=(12)$. Then $\tau \notin A_{n}$. If $\sigma \notin A_{n}$, then $\operatorname{sgn}(\sigma \tau)=$ $(-1)(-1)=1$, 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:

$$
\begin{equation*}
S_{n}=A_{n} \cup A_{n} \tau \tag{5.2}
\end{equation*}
$$

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 $\tau$ swaps the two subsets), so (5.2) tells us $n!=2\left|A_{n}\right|$.

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

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\left\|S_{n}\right\|$ | 1 | 2 | 6 | 24 | 120 | 720 | 5040 |
| $\left\|A_{n}\right\|$ | 1 | 1 | 3 | 12 | 60 | 360 | 2520 |

That all elements of $S_{n}$ are products of transpositions has an analogue in $A_{n}$ : they are all products of 3 -cycles.

Theorem 5.7. For $n \geq 3$, each element of $A_{n}$ is a product of 3-cycles.
Proof. The identity (1) is (123)(132), which is a product of 3-cycles. Now pick a non-identity element of $A_{n}$, say $\sigma$. Write it as a product of transpositions in $S_{n}$ :

$$
\sigma=\tau_{1} \tau_{2} \cdots \tau_{r}
$$

The left side has sign 1 and the right side has sign $(-1)^{r}$, so $r$ is even. Therefore we can collect the products on the right into successive transpositions $\tau_{i} \tau_{i+1}$, where $i=1,3, \ldots$ is odd. We will now show every product of two transpositions in $S_{n}$ is a product of two 3 -cycles, so $\sigma$ is a product of 3 -cycles.

Case 1: $\tau_{i}$ and $\tau_{i+1}$ are equal. Then $\tau_{i} \tau_{i+1}=(1)=(123)(132)$, so we can replace $\tau_{i} \tau_{i+1}$ with a product of two 3 -cycles.

Case 2: $\tau_{i}$ and $\tau_{i+1}$ have exactly one element in common. Let the common element be $a$, so we can write $\tau_{i}=(a b)$ and $\tau_{i+1}=(a c)$, where $b \neq c$. Then

$$
\tau_{i} \tau_{i+1}=(a b)(a c)=(a c b)=(a b c)(a b c)
$$

so we can replace $\tau_{i} \tau_{i+1}$ with a product of two 3 -cycles.

Case 3: $\tau_{i}$ and $\tau_{i+1}$ have no elements in common. This means $\tau_{i}$ and $\tau_{i+1}$ are disjoint, so we can write $\tau_{i}=(a b)$ and $\tau_{i+1}=(c d)$ where $a, b, c, d$ are distinct (so $n \geq 4$ ). Then

$$
\tau_{i} \tau_{i+1}=(a b)(c d)=(a b)(b c)(b c)(c d)=(b c a)(c d b)=(a b c)(b c d),
$$

so we can replace $\tau_{i} \tau_{i+1}$ with a product of two 3 -cycles.
Remark 5.8. Although there is a parity constraint on writing a permutation as a product of transpositions, there is no similar restriction on the number of 3 -cycles whose product is some element of $A_{n}$. To illustrate this, we'll show (1) is a product of $m 3$-cycles for every $m \geq 2$. First, from

$$
(1)=(123)(132)=(123)(123)(123)=(123)(132)(123)(132),
$$

we can write (1) as a product of 2,3 , and 43 -cycles. Multiplying each of these products by $(123)^{3 k}$, where $k \geq 1$, expresses (1) as a product of $3 k+2,3 k+3=3(k+1)$, and $3 k+4=3(k+1)+13$-cycles, so (1) is a product of any number of 3 -cycles except for a single 3 -cycle.

## 6. Minimal number of transpositions for a permutation

For $\sigma \in S_{n}$, what is the fewest number of transpositions in $S_{n}$ with product $\sigma$ ? For example, the 7 -cycle (1234567) can be written as a product of 6 transpositions:

$$
\begin{equation*}
(1234567)=(12)(23)(34)(45)(56)(67) . \tag{6.1}
\end{equation*}
$$

That shows the 7 -cycle is even, but it is not a product of 2 transpositions even though 2 is even, since a product of 2 transpositions moves at most 4 things while (1234567) moves 7 things. Can we use 4 transpositions? No. It turns out 6 transpositions is the minimal number for a 7 -cycle.
Theorem 6.1. Let $\sigma \in S_{n}$ be a product of $m$ disjoint cycles, including 1-cycles. If we write $\sigma=\tau_{1} \tau_{2} \cdots \tau_{r}$ where each $\tau_{i}$ is a transposition, then the smallest value of $r$ is $n-m$.
Example 6.2. Let $\sigma=(1234567)$ in $S_{7}$. Then $n=7, m=1$, and $n-m=6$. We have expressed $\sigma$ as a product of 6 transpositions in (6.1). If we view $\sigma$ in $S_{10}$ as (1234567)(8)(9)(10) then $n=10, m=4$, and $n-m=6$ again. This shows 1 -cycles are a nice accounting tool.

Example 6.3. Let $\sigma=(123)(4567)$ in $S_{7}$. Then $n=7, m=2$, and $n-m=5$. An expression of $\sigma$ as a product of 5 transpositions is (12)(23)(45)(56)(67).

Example 6.4. It is important in Theorem 6.1 that we are using disjoint cycles, which is a canonical way to decompose permutations into cycles. For instance, $\sigma=(12)(23)(34)$ is a product of 3 cycles in $S_{4}$ that are not disjoint, and if we use $n=4$ and $m=3$ (incorrect) then $n-m=1$ and $\sigma$ is not a transposition: it is the 4 -cycle (1234).

Now we prove Theorem 6.1.
Proof. First we show $\sigma$ can be written as a product of $n-m$ transpositions. By assumption, $\sigma=c_{1} \cdots c_{m}$ where the $c_{j}$ 's are disjoint cycles. Throw in 1-cycles for missing numbers (those fixed by $\sigma$ ) and that makes the sum of the lengths of the different cycles equal to $n$. Let $\ell_{j}$ be the length of $c_{j}: c_{j}=\left(a_{1 j} a_{2 j} \cdots a_{\ell_{j} j}\right)$. Each $c_{j}$ is a product of $\ell_{j}-1$ transpositions:

$$
\left(a_{1 j} a_{2 j} \cdots a_{\ell_{j} j}\right)=\left(a_{1 j} a_{2 j}\right)\left(a_{2 j} a_{3 j}\right) \cdots\left(a_{\ell_{j}-1 j} a_{\ell_{j} j}\right)
$$

Multiplying these together for $j=1, \ldots, r$ expresses $\sigma$ as a product of $\sum_{j=1}^{m}\left(\ell_{j}-1\right)=$ $\sum_{j=1}^{m} \ell_{j}-m=n-m$ transpositions. In Example 6.3, for instance, $\ell_{1}=3$ and $\ell_{2}=4$.

It remains to prove $\sigma$ is not a product of less than $n-m$ transpositions. To do this we will use an argument based on linear maps and hyperplanes due to Mackiw [9].

For each permutation $\sigma$ in $S_{n}$, associate a linear map $L_{\sigma}: \mathbf{R}^{n} \rightarrow \mathbf{R}^{n}$ that permutes the standard basis $\mathbf{e}_{1}, \ldots, \mathbf{e}_{n}$ of $\mathbf{R}^{n}$ according to $\sigma$ and extend this by linearity:

$$
L_{\sigma}\left(\mathbf{e}_{i}\right)=\mathbf{e}_{\sigma(i)}, \quad L_{\sigma}\left(\sum_{k=1}^{n} x_{k} \mathbf{e}_{k}\right)=\sum_{k=1}^{n} x_{k} \mathbf{e}_{\sigma(k)} \text { for } x_{k} \in \mathbf{R} .
$$

For example, if $\sigma=(123)$ then

$$
L_{\sigma}\left(x_{1}, x_{2}, x_{3}\right)=L_{\sigma}\left(x_{1} \mathbf{e}_{1}+x_{2} \mathbf{e}_{2}+x_{3} \mathbf{e}_{3}\right)=x_{1} \mathbf{e}_{2}+x_{2} \mathbf{e}_{3}+x_{3} \mathbf{e}_{1}=\left(x_{3}, x_{1}, x_{2}\right)
$$

Watch out: $L_{\sigma}\left(x_{1}, x_{2}, x_{3}\right)$ is not $\left(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}\right)$, which is $\left(x_{2}, x_{3}, x_{1}\right)$ ! Permuting the basis vectors by $\sigma$ amounts to permuting coordinates by $\sigma^{-1}$ :

$$
L_{\sigma}\left(\sum_{k=1}^{n} x_{k} \mathbf{e}_{k}\right)=\sum_{k=1}^{n} x_{k} \mathbf{e}_{\sigma(k)}=\sum_{k=1}^{n} x_{\sigma^{-1}(k)} \mathbf{e}_{k},
$$

so $L_{\sigma}\left(x_{1}, \ldots, x_{n}\right)=\left(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}\right)$. If $\sigma=\sigma^{-1}$ then this subtlety does not matter, and that includes the case when $\sigma$ is a transposition.

For two permutations $\sigma$ and $\sigma^{\prime}$ in $S_{n}, L_{\sigma \sigma^{\prime}}=L_{\sigma} \circ L_{\sigma^{\prime}}$ on $\mathbf{R}^{n}$ since the linear maps on both sides have the same value on the standard basis of $\mathbf{R}^{n}$, where each side has the effect $\mathbf{e}_{k} \mapsto \mathbf{e}_{\sigma\left(\sigma^{\prime}(k)\right)}$. Thus when $\sigma$ is a product $r$ transpositions, say $\sigma=\tau_{1} \cdots \tau_{r}$, we have

$$
L_{\sigma}=L_{\tau_{1}} \circ \cdots \circ L_{\tau_{r}}
$$

We showed at the start of this proof that $\sigma$ can be written as a product of $n-m$ transpositions, where $\sigma$ contains $m$ disjoint cycles. We want to show $r \geq n-m$ and will do this by looking at subspaces of $\mathbf{R}^{n}$. Let $W_{\sigma}=\left\{\mathbf{v} \in \mathbf{R}^{n}: L_{\sigma}(\mathbf{v})=\mathbf{v}\right\}$. For example, if $\sigma=(123)(4567)$ then

$$
W_{\sigma}=\{(a, a, a, b, b, b, b): a, b \in \mathbf{R}\}=\mathbf{R}(1,1,1,0,0,0,0)+\mathbf{R}(0,0,0,1,1,1,1),
$$

which has basis $\left\{\mathbf{e}_{1}+\mathbf{e}_{2}+\mathbf{e}_{3}, \mathbf{e}_{4}+\mathbf{e}_{5}+\mathbf{e}_{6}+\mathbf{e}_{7}\right\}$. More generally, when $\sigma=c_{1} \cdots c_{m}$ for disjoint cycles $c_{1}, \ldots, c_{m}$ we have $W_{\sigma}=\sum_{j=1}^{m} \mathbf{R} \mathbf{w}_{j}$, where $\mathbf{w}_{j}=\sum_{i \in c_{j}} \mathbf{e}_{i}$ : each $\mathbf{w}_{j}$ is the sum of the standard basis vectors $\mathbf{e}_{i}$ in $\mathbf{R}^{n}$ where $i$ is moved by $c_{j}$. The vectors $\mathbf{w}_{1}, \ldots, \mathbf{w}_{m}$ are sums of disjoint sets of standard basis vectors in $\mathbf{R}^{n}$, so they are linearly independent. Since they span $W_{\sigma}, \operatorname{dim}\left(W_{\sigma}\right)=m$. We will show $W_{\sigma}$ contains a subspace of dimension $n-r$, so $n-r \leq \operatorname{dim}\left(W_{\sigma}\right)=m$ and thus $r \geq n-m$, which is what we want.

For each transposition $\tau=(i j)$ in $S_{n}, L_{\tau}$ swaps the two basis vectors $\mathbf{e}_{i}$ and $\mathbf{e}_{j}$ and fixes the other basis vectors: $L_{\tau}\left(\mathbf{e}_{i}\right)=\mathbf{e}_{j}, L_{\tau}\left(\mathbf{e}_{j}\right)=\mathbf{e}_{i}$, and $L_{\tau}\left(\mathbf{e}_{k}\right)=\mathbf{e}_{k}$ for $k \neq i, j$. Then

$$
L_{\tau}\left(\sum_{k=1}^{n} x_{k} \mathbf{e}_{k}\right)=x_{i} \mathbf{e}_{j}+x_{j} \mathbf{e}_{i}+\sum_{k \neq i, j} x_{k} \mathbf{e}_{k}
$$

A vector is fixed by $L_{\tau}$ precisely when the coefficients of $\mathbf{e}_{i}$ and $\mathbf{e}_{j}$ agree, so the set of vectors fixed by $L_{\tau}$ form

$$
W_{\tau}=\mathbf{R}\left(\mathbf{e}_{i}+\mathbf{e}_{j}\right)+\sum_{k \neq i, j} \mathbf{R e}_{k},
$$

which is a hyperplane in $\mathbf{R}^{n}$ (subspace of dimension $n-1$ ). Since $\sigma=\tau_{1} \cdots \tau_{r}$,

$$
\bigcap_{i=1}^{r} W_{\tau_{i}} \subset W_{\sigma}
$$

An intersection of $r$ hyperplanes in $\mathbf{R}^{n}$ has dimension at least $n-r$, so

$$
m=\operatorname{dim}\left(W_{\sigma}\right) \geq n-r
$$

Therefore $r \geq n-m$.

## References

[1] T. L. Bartlow, An historical note on the parity of permutations, Amer. Math. Monthly 79 (1972), 766769.
[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] A. L. Cauchy https://gallica.bnf.fr/ark:/12148/bpt6k90193x/f73.item.
[5] 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.
[6] I. Halperin, Odd and even permutations, Canadian Math. Bull. 3 (1960), 185-186.
[7] D. Higgs and P. de Witte, On products of transpositions and their graphs, Amer. Math. Monthly 86 (1979), 376-380.
[8] H. Liebeck, Even and odd permutations, Amer. Math. Monthly 76 (1969), 668.
[9] G. Mackiw, Permutations as products of transpositions, Amer. Math. Monthly 102 (1995), 438-440.
[10] G. A. Miller, On the groups generated by two operators, Bull. Amer. Math. Soc. 7 (1901), 424-426. URL https://www.ams.org/journals/bull/1901-07-10/S0002-9904-1901-00826-9/S0002-9904-1901 -00826-9.pdf.
[11] W. I. Miller, Even and odd permutations, MATYC Journal 5 (1971), 32.
[12] S. Nelson, Defining the sign of a permutation, Amer. Math. Monthly 94 (1987), 543-545.
[13] R. K. Oliver, On the parity of a permutation, Amer. Math. Monthly 118 (2011), 734-735.
[14] W. Phillips, On the definition of even and odd permutations, Amer. Math. Monthly 74 (1967), 12491251.
[15] E. L. Spitznagel, Jr., Note on the Alternating Group, Amer. Math. Monthly 75 (1968), 68-69.
[16] C. Weil, Another approach to the alternating subgroup of the symmetric group, Amer. Math. Monthly 71 (1964), 545-546.


[^0]:    ${ }^{1}$ We can prove that every permutation in $S_{n}$ is a product of transpositions without mentioning cycles, by using biology. If $n$ objects are placed in front of you and you are asked to rearrange them in a particular way, you could do it by swapping objects two at a time with your two hands. I heard this argument from Ryan Kinser.

[^1]:    ${ }^{2}$ A visualization of this proof is in https://www. youtube.com/watch?v=p6kCYbKIMak starting at 13:50.

[^2]:    ${ }^{3}$ Since $\left(a_{1} b_{1}\right)$ and ( $a_{1} b_{2}$ ) were assumed all along to be honest transpositions, $b_{1}$ and $b_{2}$ do not equal $a_{1}$, so ( $b_{1} b_{2}$ ) doesn't move $a_{1}$.
    ${ }^{4}$ As an example of old terminology, Miller [10] in 1901 called even permutations "positive" and odd permutations "negative".

