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

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

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

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

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

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 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

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

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 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.

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 mod 2 is uniquely determined for σ, it will make sense to refer to σ 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:*

$$\sigma = \tau_1\tau_2\cdots\tau_r = \tau_1'\tau_2'\cdots\tau_{r'}'. \tag{2.1}$$

Then $r \equiv r'$ mod 2.

Proof. The two products of transpositions that equal σ in (2.1) lead to an expression 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 transpositions τ and inverting a product reverses the order of multiplication.)

Claim: A product of transpositions equal to (1) must have an even number of transpositions.

This claim forces $r + r'$ above to be even, so $r \equiv r'$ mod 2.

To prove the claim, write the identity in S_n as a product of k transpositions:

$$(1) = (a_1b_1)(a_2b_2)\cdots(a_kb_k), \tag{2.2}$$

where $k \geq 1$ and $a_i \neq b_i$ for all i. We want to show k is even and will induct on k.

The product on the right side of (2.2) can't have $k = 1$ since a 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) has an even number of transpositions.

Some transposition (a_ib_i) for $i \neq 1$ 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 $i > 1$. We can suppose a_1 is a_i since $(a_ib_i) = (b_ia_i)$. The two equations

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

where different letters are different numbers, show a product of two transpositions where the second one moves a and the first one does not can be rewritten as a product of two transpositions in which the first one moves a and the second one does not. So in (2.2), *without changing the number of transpositions* we can arrange for a transposition moving a_1 other than (a_1b_1) to appear directly after (a_1b_1): we can *assume* $a_2 = a_1$. Now consider the cases $b_2 = b_1$ and $b_2 \neq b_1$.

Case 1: $b_2 = b_1$. The product $(a_1b_1)(a_2b_2)$ in (2.2) is $(a_1b_1)(a_1b_1)$, 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 is even.

Case 2: $b_2 \neq b_1$. Check $(a_1b_1)(a_2b_2)$ in (2.2), which is $(a_1b_1)(a_1b_2)$, can be written as $(a_1b_2)(b_1b_2)$ since a_1, b_1, and b_2 are all different. Then (2.2) can be rewritten as

$$(1) = (a_1b_2)(b_1b_2)(a_3b_3)\cdots(a_kb_k), \tag{2.3}$$

where only the first two transpositions have been changed. Now run through the above argument with (2.3) in place of (2.2). It involves the same number k of transpositions, but

there are fewer transpositions in (2.3) 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 in (2.3) other than the first term (a_1b_2) moves a_1, so by running through the above argument with (2.3) in place of (2.2) we land in either Case 1, which lets us drop the number of transpositions by 2 and we're done by induction, or Case 2, which lets us drop the number of transpositions moving a_1 by 1 without changing the total number of transpositions.

When (1) is a product of transpositions with the leftmost one moving a_1, there is always at least one more transposition in the product moving a_1 and Case 2 reduces that number by 1. So in finitely many steps we have to land in Case 1 and then we are done. □

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 [13].

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

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

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.

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

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

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 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), 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 each transposition has sign -1. Also, the sign is multiplicative in the following sense.

[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.

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

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

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

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

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

Theorem 2.10 lets us compute signs of permutations using *any* decomposition into a product of cycles: disjointness of the cycles is not necessary. Just remember that 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 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 nonzero term corresponding to the permutation of $\{1, 2, \ldots, n\}$ associated to σ. This term is $\mathrm{sgn}(\sigma)$, so $\det(T_\sigma) = \mathrm{sgn}(\sigma)$. 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 $h\colon S_n \to \{\pm 1\}$ satisfy $h(\sigma\sigma') = h(\sigma)h(\sigma')$ for all $\sigma, \sigma' \in S_n$. Then $h(\sigma) = 1$ for all σ or $h(\sigma) = \mathrm{sgn}(\sigma)$ for all σ. Thus, if h is multiplicative and not identically 1, then $h = \mathrm{sgn}$.*

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 τ, $h(\tau) = h(12)$.

A 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.

A 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 each 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 $h(\sigma) = (-1)^k = \mathrm{sgn}(\sigma)$ for all σ. $\square$

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 $S_n \to \{\pm 1\}$. 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 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,

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

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. 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

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

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:

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

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 $n \geq 2$, $|A_n| = n!/2$.*

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
$\lvert S_n\rvert$	1	2	6	24	120	720	5040
$\lvert A_n\rvert$	1	1	3	12	60	360	2520

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 σ? For example, the 7-cycle (1234567) can be written as a product of 6 transpositions:

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

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 τ_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 σ as a product of 6 transpositions in (6.1). If we view σ 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 σ 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 σ is not a transposition: it is the 4-cycle (1234).

Proof. First we show σ 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 σ) and that makes the sum of the lengths of the different cycles equal to n. Let ℓ_j be the length of c_j: $c_j = (a_{1j}a_{2j}\cdots a_{\ell_j j})$. This is a product of $\ell_j - 1$ transpositions:

$$(a_{1j}a_{2j}\cdots a_{\ell_j j}) = (a_{1j}a_{2j})(a_{2j}a_{3j})\cdots(a_{\ell_j-1\,j}a_{\ell_j j}).$$

Multiplying these together for $j = 1, \ldots, r$ expresses σ as a product of $\sum_{j=1}^m(\ell_j - 1) = \sum_{j=1}^m \ell_j - m = n - m$ transpositions. In Example 6.3, for instance, $\ell_1 = 3$ and $\ell_2 = 4$.

It remains to prove σ is never 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 [8].

For each permutation σ in S_n, associate a linear map $L_\sigma\colon \mathbf{R}^n \to \mathbf{R}^n$ that permutes the standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ of $\mathbf{R}^n$ according to σ and extend this by linearity:

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

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

$$L_\sigma(c_1, c_2, c_3) = L_\sigma(c_1\mathbf{e}_1 + c_2\mathbf{e}_2 + c_3\mathbf{e}_3) = c_1\mathbf{e}_2 + c_2\mathbf{e}_3 + c_3\mathbf{e}_1 = (c_3, c_1, c_2).$$

Watch out: $L_\sigma(c_1, c_2, c_3)$ is *not* $(c_{\sigma(1)}, c_{\sigma(2)}, c_{\sigma(3)})$, which is (c_2, c_3, c_1)! Permuting the basis vectors by σ amounts to permuting coordinates by σ^{-1}:

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

so $L_\sigma(c_1, \ldots, c_n) = (c_{\sigma^{-1}(1)}, \ldots, c_{\sigma^{-1}(n)})$. If $\sigma = \sigma^{-1}$ then this subtlety does not matter, and that includes the case when σ is a transposition.

For two permutations σ and σ' in S_n, $L_{\sigma\sigma'} = L_\sigma \circ L_{\sigma'}$ on $\mathbf{R}^n$: to check this equality of linear maps it suffices to check both sides have the same value on the standard basis of $\mathbf{R}^n$, where each side has the effect $\mathbf{e}_k \mapsto \mathbf{e}_{\sigma(\sigma'(k))}$. So when σ is a product of m disjoint cycles and r transpositions, say $\sigma = c_1 \cdots c_m = \tau_1 \cdots \tau_r$, we have

$$L_\sigma = L_{c_1} \circ \cdots \circ L_{c_m} = L_{\tau_1} \circ \cdots \circ L_{\tau_r}.$$

We showed at the start of this proof that σ can be written as a product of $n - m$ transpositions. To show that number is minimal, we will show $r \geq n - m$ by looking at subspaces of $\mathbf{R}^n$. Let $W_\sigma = \{\mathbf{v} \in \mathbf{R}^n : L_\sigma(\mathbf{v}) = \mathbf{v}\}$. 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 $\{\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, \mathbf{e}_4 + \mathbf{e}_5 + \mathbf{e}_6 + \mathbf{e}_7\}$. 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_σ, $\dim(W_\sigma) = m$. We will show W_σ contains a subspace of dimension $n - r$, so $n - r \leq \dim(W_\sigma) = m$ and thus $r \geq n - m$, which is what we want.

For each transposition $\tau = (ij)$ in S_n, L_τ swaps the two basis vectors $\mathbf{e}_i$ and $\mathbf{e}_j$ and fixes the other basis vectors: $L_\tau(\mathbf{e}_i) = \mathbf{e}_j$, $L_\tau(\mathbf{e}_j) = \mathbf{e}_i$, and $L_\tau(\mathbf{e}_k) = \mathbf{e}_k$ for $k \neq i, j$. Then

$$L_\tau\left(\sum_{k=1}^n c_k\mathbf{e}_k\right) = c_i\mathbf{e}_j + c_j\mathbf{e}_i + \sum_{k \neq i,j} c_k\mathbf{e}_k.$$

A vector is fixed by L_τ precisely when the coefficients of $\mathbf{e}_i$ and $\mathbf{e}_j$ agree, so the fixed vectors for L_τ form

$$W_\tau = \mathbf{R}(\mathbf{e}_i + \mathbf{e}_j) + \sum_{k \neq i,j} \mathbf{R}\mathbf{e}_k,$$

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

$$m = \dim(W_\sigma) \geq n - r.$$

Therefore $r \geq n - m$. □

References

[1] T. L. Bartlow, An historical note on the parity of permutations, *Amer. Math. Monthly* **79** (1972), 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] G. Mackiw, Permutations as products of transpositions, *Amer. Math. Monthly* **102** (1995), 438–440.

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

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

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

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

[13] E. L. Spitznagel, Jr., Note on the Alternating Group, *Amer. Math. Monthly* **75** (1968), 68–69.

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