Keeler's Theorem and products of distinct transpositions

Lihua Huang

Advisor: Ron Evans

Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0112

June 2012

Abstract

An acclaimed episode of the television series *Futurama* features a two-body mind-switching machine. The machine has a serious limitation: it will not work more than once on the same pair of bodies. After the Futurama community indulges in a mind-switching frenzy, the following question is raised: Can the switching be undone so as to restore all minds to their original bodies? Ken Keeler found an algorithm [2, pp. 18–19] that undoes any mind-scrambling permutation with the aid of two "outsiders". We refine Keeler's result by providing a more efficient algorithm that uses the smallest possible number of switches. James Grime has a corollary which is presented in his video [3] and in *The Commutator* magazine [2, p. 20]; we generalize the corollary and prove it is optimal. We present best possible algorithms for undoing two natural sequences of switches each effecting a cyclic mind-scrambling permutation in the symmetric group S_n. This happens to yield certain expressions for the identity permutation as a product of distinct transpositions, so it is natural to ask for necessary and sufficient conditions on m and n for the identity to be expressible as a product of m distinct transpositions in S_n. We close by finding such conditions.

Acknowledgements

First and foremost, I would like to thank my advisor, Professor Ron Evans. It has been a great pleasure to work with him, and I have learned a lot from him. This includes learning how to come up with conjectures and experience the journey of working extra hard to prove or disprove them, how to write a well-organized research paper, and how to become a better speaker. Our email conversations discussing ideas of conjectures and proofs drove me to work hard with passion late at night, sometimes until 3am, while my usual bed time was around midnight. I am very grateful for his inspiring and entertaining teaching, patience, and encouragements. In a word, this research project would not be possible without his guidance. I deeply appreciate everything he has done for me.

I would like also to express my gratefulness to Professor Martin Isaacs, for his help in improving our original proof of Lemma 3; to Tuan Nguyen, for his contributions in Lemma 1 and Theorem 4; to Artem Mavrin, for his help with typesetting with LaTeX; to my family, for their love and support; and to my friends, for their time discussing math with me.

Contents

1 Introduction

The Prisoner of Benda, an acclaimed episode of the animated television series *Futurama*, features a two-body mind-switching machine. Any pair can enter the machine to swap minds, but with one serious limitation: the machine will not work more than once on the same pair of bodies.

After the Futurama community indulges in a mind-switching frenzy, a question is raised: Can the switching be undone so as to restore all minds to their original bodies? The show provides an answer using what is known in the popular culture as "Keeler's Theorem". The theorem is the brainchild of the show's writer Ken Keeler [6], who earned a PhD in Mathematics from Harvard University in 1990 [7] before becoming a television writer/producer. For *The Prisoner of Benda*, Keeler garnered a 2011 Writers Guild Award [9]. Keeler's Theorem is discussed in [2, pp. 18–19].

The problem of undoing the switching can be modeled in terms of group theory. Represent the bodies involved in the switching frenzy by $\{1, 2, \cdots, n\}$. The symmetric group S_n consists of the $n!$ permutations of $\{1, 2, \cdots, n\}$. Let I denote the identity permutation. A 2-cycle (ab) is called a transposition; it represents the permutation which switches the minds of bodies a and b. The k-cycle $(a_1 \cdots a_k)$ is the permutation which sends a_1's mind to a_2, a_2's mind to a_3, $\cdots$, and a_k's mind to a_1. Following the convention in [1], we compute products (i.e., compositions) in S_n from right to left. For example, $(123) = (12)(23) = (13)(12) = (23)(13)$.

The successive swapping of minds during the switching frenzy can be represented by a product P of distinct transpositions in S_n. (The transpositions must be distinct due to the limitation of the machine.) In addition to viewing P formally as a product, we can also view P as a permutation. It will be assumed that this permutation is nontrivial, otherwise nothing needs to be undone. For an example of P, suppose that 2 switches minds with 3 and then 2 switches minds with 1; this corresponds to the product $P = (12)(23)$, yielding the mind-scrambling permutation $P = (123)$.

To restore all minds to their original bodies, one must find a product σ of distinct transpositions such that $\sigma P = I$ and such that the transposition factors in the product σ are distinct from those in the product P. Such a σ is said to *undo* P. From now on, the phrase "transposition factors" will be shortened simply to "factors".

A σ_1 that undoes a product P_1 may differ dramatically from a σ_2 that undoes a product P_2, even if P_1 and P_2 effect the same mind-scrambling permutation. For example, we will see (in Theorems 2 and 3) that while the products $P_1 = (12)(23)(34)(45)$ and $P_2 = (45)(35)(25)(15)$ both effect the permutation (12345), P_1 can be undone by a product in S_5, but P_2 cannot.

In the aftermath of a switching frenzy, the community may have no recollection of the sequence of switches that had taken place. It is then expedient to find a product σ that is guaranteed to undo the mind-scrambling permutation $P \in S_n$ *regardless* of which transpositions in S_n had effected P. Keeler's Theorem explicitly produces such a product $\sigma \in S_{n+2}$. Each factor in Keeler's σ contains at least one of the entries

$$x = n + 1, \quad y = n + 2,$$

so that the factors in σ are distinct from the transpositions that effected P. One can view x and y as altruistic outsiders who had never entered the machine during the frenzy, but who are subsequently willing to endure frequent mind switches in order to help others restore their minds to their original bodies.

Viewed as a permutation, P can be expressed (uniquely up to ordering) as the product $P = C_1 \cdots C_r$ of nontrivial disjoint cycles $C_1, \cdots, C_r$ in S_n [1, p. 77]. For each $i = 1, \cdots, r$, let k_i denote the length of cycle C_i. In discussing Keeler's Theorem and our refinement (Theorem 1), we will assume that

$$k_1 + \cdots + k_r = n.$$

This presents no loss of generality, since if $k_1 + \cdots + k_r = m < n$, then we could relabel the bodies and mimic the arguments using m in place of n.

1.1 Keeler's method

We now describe Keeler's method for constructing a product $\sigma \in S_{n+2}$ which undoes $P = C_1 \cdots C_r$. For convenience of notation, write $k = k_1$, so that C_1 is a k-cycle $(a_1 \cdots a_k)$ with each $a_i \in \{1, 2, \cdots, n\}$. It is easily checked that $\sigma_1 C_1 = (xy)$, where σ_1 is the product of $k + 2$ transpositions given by

$$\sigma_1 = (xa_1)(xa_2) \cdots (xa_{k-1}) \cdot (ya_k)(xa_k)(ya_1). \tag{1}$$

For each cycle C_i, we have analogous products σ_i of $k_i + 2$ transpositions for which

$$\sigma_i C_i = (xy), \quad i = 1, \cdots, r.$$

Note that every transposition in σ_i has the form (xu) or (yu) for some entry u in C_i. Since disjoint cycles commute, (xy) commutes with every transposition in S_n, so

$$\tau := \sigma_r \cdots \sigma_2 \sigma_1$$

is a product of distinct transpositions for which $\tau P = (xy)^r$. Taking

$$\sigma = \begin{cases} (xy)\tau, & \text{if } r \text{ is odd} \\ \tau, & \text{if } r \text{ is even,} \end{cases} \tag{2}$$

we find that σ undoes P and σ is a product of distinct transpositions in S_{n+2} each containing at least one of the entries x, y, as desired.

By (1) and (2), the number of factors in Keeler's σ is either $n + 2r + 1$ or $n + 2r$ according as r is odd or even. However, for each $r > 2$, the number of factors needed to undo P can be reduced. For example, for $r = 3$, $P = (12)(34)(56)$ is undone by Keeler's product of 13 transpositions

$$\sigma = (xy)(5x)(6y)(6x)(5y)(3x)(4y)(4x)(3y)(1x)(2y)(2x)(1y),$$

but in fact P can be undone by the product of 11 transpositions

$$(5x)(6y)(6x)(5y)(1x)(2x)(3x)(4y)(4x)(3y)(1y).$$

In Theorem 1 of the next section, we refine Keeler's method by showing that P can be undone via a product of only $n + r + 2$ distinct transpositions each containing at least one of the entries x, y. We show moreover that this result is "best possible" in the sense that $n + r + 2$ cannot be replaced by a smaller number.

1.2 Grime's Corollary

James Grime of University of Cambridge introduced Grime's Corollary in his video [3]. It is also discussed in [2, p. 20]. His corollary deals with the permutation $P = (12)(3456789)$ that is created by $(45)(89)(12)(39)(65)(37)(36)$. Keeler undoes P in 13 switches. Grime improves this by undoing P with a product σ of 9 distinct transpositions, where

$$\sigma = (19)(62)(31)(72)(41)(82)(51)(92)(61).$$

In the end of his video [3], Grime posed an open question, "Can you find a better way (with or without outsiders)?". We take the challenge and prove that Grime's Corollary is best possible in the sense that 9 cannot be replaced by a smaller number. In fact, we prove the optimality of a generalization of Grime's Corollary for $P = (12)(345 \cdots n)$ when $n \geq 4$.

In subsequent sections, we turn our attention to the problem of undoing, with a minimal number of outsiders, explicit products P of distinct transpositions in S_n which effect the cycle $(123 \cdots n)$. The product

$$P = (34)(24)(13)(14)(45)(23)(35)(12)(25)(15) \tag{3}$$

is an example of a product of distinct transpositions in S_5 which effects the cycle (12345). Can P be undone by a product σ that uses fewer than two outsiders? We proceed to show that the answer is no. There are ten transpositions in S_5. Each occurs as a factor in (3) and hence cannot occur as a factor in σ. Assume for the purpose of contradiction that P could be undone by a product $\sigma \in S_6$ (i.e., using the sole outsider 6). Then $P^{-1} = \sigma = (6a_1) \cdots (6a_s)$ for some set of distinct entries $a_1, \cdots, a_s \in \{1, 2, 3, 4, 5\}$. This yields a contradiction because $\sigma = (54321)$ fixes 6 while $(6a_1) \cdots (6a_s)$ fails to fix 6.

It may happen that two outsiders are required to undo a product P even when not all $\binom{n}{2}$ transpositions in S_n occur as factors of P. For example, consider the product

$$P = (23)(12)(34)(14)(24),$$

which is a product of distinct transpositions in S_4 effecting the cycle (1234). We leave it to the reader to show that P cannot be undone by a product $\sigma \in S_5$ (i.e., using the sole outsider 5).

With the aim of finding interesting classes of products that can be undone using *fewer* than two outsiders, we examined what are undoubtably the two most natural products P in S_n effecting $(12 \cdots n)$, namely [1, p. 81]

$$P_1 = (12)(23)(34) \cdots (n-1, n) \quad \text{and} \quad P_2 = (n-1, n) \cdots (3n)(2n)(1n).$$

Theorems 2 and 3 determine how many outsiders and how many mind switches are sufficient to undo each of these two products. Theorem 2 shows that for $n \geq 5$, P_1 can be undone without any outsiders, using only $n+1$ switches, where $n+1$ is best possible. Theorem 3 shows that for $n \geq 3$, P_2 can be undone using only one outsider, again with $n+1$ switches, where $n+1$ is best possible. We note that no σ can undo P_2 without outsiders;

otherwise, as P_2 doesn't fix n, such σ would contain a factor of the form (an) with $a < n$, which is impossible because P_2 contains all such factors.

Notice that if $P = (12 \cdots n)$ is not factored in the form of P_1 or P_2, then it is possible that P can be undone by a σ with fewer than $n + 1$ distinct transpositions, as illustrated by the following example.

Example 1. For $P = (1234567) = (23)(67)(17)(34)(15)(14)$, we have that $\sigma = (25)(26)(35)(45)(27)(12)$ undoes P. Observe that σ contains only $6 < n + 1 = 8$ distinct transpositions.

When $n \geq 5$, Theorem 2 provides equalities of the form $\sigma P_1 = I$ which express the identity I as a product of $2n$ distinct transpositions in S_n. For the case $n = 4$, I can be expressed as a product of 6 distinct transpositions in S_4, e.g.,

$$I = (34)(14)(23)(13)(24)(12).$$

Such equalities lead to the question: What are necessary and sufficient conditions on m and n for I to be expressible as a product of m distinct transpositions in S_n? Theorem 4 provides the answer: it is necessary and sufficient that m be an even integer with $6 \leq m \leq \binom{n}{2}$.

In order to prove Theorems 2–4, we require three lemmas about cycles. Lemma 1 is known [4, p. 77], but we provide an elementary proof for completeness. The proof of Lemma 3 is due to I. Martin Isaacs [5]. We are grateful for his permission to include it here, as our original proof was considerably less elegant.

We will need the well-known "Parity Theorem", which shows that that the identity permutation I cannot equal a product of an odd number of transpositions. Two proofs of the Parity Theorem may be found in [1, pp. 82, 149], and a nice recent version is due to Oliver [8]. We give Oliver's proof in the Appendix.

2 An optimal refinement of Keeler's method

Theorem 1. *Let $P = C_1 \cdots C_r$ be a product of r disjoint k_i-cycles C_i in S_n, with $k_i \geq 2,\ \ n = k_1 + \cdots + k_r$. Then P can be undone by a product λ of $n + r + 2$ distinct transpositions in S_{n+2} each containing at least one of the entries $x = n + 1$, $y = n + 2$. Moreover, this result is best possible in the sense that $n + r + 2$ cannot be replaced by a smaller number.*

Proof. Write $k = k_1$, so that C_1 is a k-cycle $(a_1 \cdots a_k)$. Corresponding to the cycle C_1, define the product

$$G_1(x) = (a_1x)(a_2x) \cdots (a_kx),$$

whose leftmost factor is

$$F_1(x) = (a_1x).$$

Corresponding to each cycle C_i, $\ i = 1, \cdots, r$, define $G_i(x)$ and $F_i(x)$ analogously. Set

$$\lambda = (xy) \cdot G_r(x) \cdots G_2(x) \cdot (a_kx)G_1(y)(a_1x) \cdot F_2(y) \cdots F_r(y).$$

It is readily checked that λ undoes P and that λ is a product of $n + r + 2$ distinct transpositions in S_{n+2} each containing at least one of the entries x, y.

It remains to prove optimality. Suppose for the purpose of contradiction that P can be undone by a product σ of $t < n + r + 2$ distinct transpositions in S_{n+2} each containing at least one of the entries x, y. Then by the Parity Theorem, $t \leq n + r$.

On the other hand, we have the lower bound $t \geq n$, since each of the n entries in P must occur (coupled with x or y) in a factor of σ. Let A denote the set of entries in $C_1 = (a_1 \cdots a_k)$, and let a denote the leftmost element of A appearing in the product σ. Since P maps a to some other element of A, it follows that a appears twice in σ, i.e., σ has both of the factors (ax) and (ay). The same argument shows that each of the r cycles C_i contains an entry which appears twice in σ. Thus the inequality $t \geq n$ can be strengthened to $t \geq n + r$. Consequently, $t = n + r$. It follows that each of the r cycles C_i contains exactly one entry which appears twice in σ, and the other $n - r$ entries appear only once. This accounts for all $n + r$ factors of σ, so in particular, (xy) cannot be a factor of σ.

Let a' denote the rightmost element of A appearing in the product σ. Since P maps some element of A to a', it follows that a' appears twice in σ. Since a is the only element of A that appears twice in σ, we must have $a = a'$. Consequently, we have shown the following two properties of C_1:
(i) there is a unique entry a in C_1 for which the transpositions (ax) and (ay) both occur as factors of σ, and
(ii) each entry of C_1 other than a occurs in exactly one factor of σ, and that factor must lie strictly between (ax) and (ay).
These two properties are similarly shared by each of the r cycles C_i.

Let N_1 denote the number of transpositions in σ that lie strictly between its factors (ax) and (ay). Define N_i similarly for each of the r cycles C_i. We may assume without loss of generality that

$$N_1 \leq N_i \quad \text{for all} \ \ i = 1, \cdots, r.$$

We may also assume that the factor (ax) in σ lies to the left of the factor (ay), and that $a = a_k$.

Let M_y denote the set of factors in σ which contain the entry y and which lie between $(a_k x)$ and $(a_k y)$ inclusive. Suppose for the purpose of contradiction that every transposition in M_y has the form $(a_i y)$ for some $a_i \in A$. Since σ must send a_{i+1} to a_i for each $i = 1, \cdots, k-1$, it follows that the elements of M_y have to occur in the following order in σ:

$$(a_1 y), \ (a_2 y), \ \cdots, \ (a_{k-1} y), \ (a_k y).$$

But then σ could not send a_1 to a_k, a contradiction. Thus some transposition in M_y must have the form (hy), where $h \notin A$. Consider the rightmost $(hy) \in M_y$ with $h \notin A$. For some fixed $j > 1$, h is an entry of the cycle C_j. Among all the elements $(a_i y) \in M_y$ that lie to the right of (hy), let $(a_m y)$ denote the one closest to (hy). As σ cannot send a_m to h, it follows that the entry h occurs twice between $(a_k x)$ and $(a_k y)$, i.e., σ has factors (hx) and (hy) both lying strictly between $(a_k x)$ and $(a_k y)$. Thus $N_j < N_1$. This violates the minimality of N_1, giving us the desired contradiction. □

Remark 1. As $\lambda P = I$, λP is even. It is easy to check directly that λP is even. Notice that for $k > 1$, a k-cycle can be written as a product of $k-1$ distinct transpositions (for example, P_1 and P_2 in Section 4). Hence, λ can be written as a product of $(k_1 - 1) + (k_2 - 1) + \cdots + (k_r - 1) = n - r$ transpositions. Thus, λP can be written as a product of $(n + r + 2) + (n - r) = 2(n + 1)$ transpositions, which implies λP is even.

Example 2. Let $P = (12)(345)(67) \in S_7$. Find $\sigma \in S_9$, a product of distinct transpositions such that each transposition contains at least one the the entries x, y and that σ undoes P.
Keeler's method:
$\sigma_1 = (xy)(x1)(y2)(x2)(y1)(x3)(x4)(y5)(x5)(y3)(x6)(y7)(x7)(y6)$.
There are $n + 2r + 1 = 7 + 6 + 1 = 14$ transpositions in σ_1, which undoes P.
Our best possible algorithm:

$\sigma_2 = (xy)(6x)(7x)(3x)(4x)(5x)(2x)(1y)(2y)(1x)(3y)(6y)$.
Notice that there are only $n + r + 2 = 7 + 3 + 2 = 12 < 14$ transpositions in σ_2, which also undoes P.

Example 3. Let $P = (12) \in S_2$. Undo P with $\sigma \in S_4$.
Keeler's method:
$\sigma_1 = (xy)(x1)(y2)(x2)(y1)$.
There are $n + 2r + 1 = 2 + 2 + 1 = 5$ transpositions in σ_1, which undoes P.
Our best possible algorithm:
$\sigma_2 = (xy)(2x)(1y)(2y)(1x)$.
There are $n + r + 2 = 2 + 1 + 2 = 5$ transpositions in σ_2, which also undoes P. (Observe that if one switches the disjoint transpositions $(x1)$ and $(y2)$ in σ_1 and then renames x, y as y, x, respectively, one can see that σ_1 becomes σ_2.)

Notice that one cannot find a σ which undoes (12) with less than five distinct transpositions, since identity cannot be written as a product of less than 6 distinct transpositions, which is shown in Theorem 4 in Section 5.

Remark 2. When $r = 1, 2$, both Keeler's method and our algorithm are best possible. However, when r is large, we have $n + r + 2$ is much less than $n + 2r$.

2.1 A variant of Theorem 1

Corollary 1. *Let $P = (12)C_2 \cdots C_r$ be a product of r disjoint k_i-cycles C_i in S_n, with $k_i \geq 2$, $n = k_1 + \cdots + k_r$. Suppose $r \geq 2$ and the entries $1, 2$ switch only with each other in the product of distinct transpositions that creates P. Then P can be undone by a product η of $n + r - 2$ distinct transpositions in S_n each containing at least one of the entries $1, 2$. Moreover, this result is best possible in the sense that $n + r - 2$ cannot be replaced by a smaller number.*

Proof. Notice that the entries $1, 2$ in P can play the roles of x, y in Theorem 1 since none of 1 or 2 switches with other entries in the sequence of switches that took place to create P. Write $k = k_2$, so that C_2 is a k-cycle $(b_1 \cdots b_k)$. Set

$$\eta = G_r(1) \cdots G_3(1) \cdot (b_k 1) G_2(2)(b_1 1) \cdot F_3(2) \cdots F_r(2). \tag{4}$$

It is readily checked that η undoes P and that η is a product of $n + r - 2$ distinct transpositions in S_n each containing at least one of the entries $1, 2$. Optimality is clear by the result of Theorem 1.

□

Remark 3. Corollary 1 (with $r = 2, n = 9$) shows that 9 factors for undoing Grime's P is best possible if each such factor is required to contain at least one of the entries $1, 2$. Corollary 2 below will show that 9 factors is best possible unconditionally.

2.2 The optimality of a generalization of Grime's Corollary

Corollary 2. *For $n \geq 4$, let $P = (12)(345 \cdots n)$ be an instance of P in Corollary 1 with $r = 2$. Then there exists a product σ of n distinct transpositions in S_n which undoes P. Moreover, this result is best possible in the sense that no σ which undoes P can have fewer than n distinct factors.*

Proof. The existence of such a σ as a product of n transpositions that undoes P is guaranteed by (4) in the proof of Corollary 1. It remains to prove optimality.

Suppose for the purpose of contradiction that P can be undone by a product τ of $k < n$ distinct transpositions. Since $\tau P = I$, the Parity Theorem shows that $k \leq n - 2$. Consider the rightmost factor (ab) of τ which has one of the entries $1, 2$. Without loss of generality, $a = 1$. Since $(n, n-1, \cdots 3)(12) = \tau$, we have $(n, n-1, \cdots 3)(12)(13) = \tau(13)$, which implies $(n, n-1, \cdots 321) = \tau(13)$, a product of $1 + k \leq n - 1$ transpositions. Lemma 1 gives $1 + k = n - 1$. Moreover, Lemma 2 shows that b is in $\{1, 2, \cdots, n\}$. Without loss of generality, $b = 3$. If not, we can rename the entries cyclically. We can move (13) to the right by interchanging disjoint transpositions and/or employing equalities of the form $(13)(3a) = (1a)(13)$. Doing this repeatedly, we have $\tau = \gamma(13)$, where γ is a product of $k - 1$ transpositions. Since τ undoes P, we have $\tau = P^{-1}$, which implies

$$\gamma(13) = (n, n-1, \cdots 3)(12).$$

Multiplying both sides of the above equality by (13), we obtain

$$\gamma = (n, n-1, \cdots 321).$$

Lemma 1 gives $k - 1 \geq n - 1$, which is a contradiction to $k \leq n - 2$. □

3 Three lemmas about cycles

3.1 Lemma 1

Lemma 1. *Let $2 \leq k \leq n$. Then no k-cycle in S_n can be a product of fewer than $k-1$ transpositions.*

Proof. The result is obvious for $k = 2, 3, 4$. Assume there exists a minimal $k \geq 5$ for which the result is false, i.e., some k-cycle $(a_1 \cdots a_k) \in S_n$ equals a product P of t transpositions in S_n, where $t < k-1$. If each of $a_1, \cdots, a_k$ occurred at least twice as an entry in the product P, then P would have at least k transpositions as factors, which is impossible since $k > t$. Thus some a_i occurs exactly once as an entry in P. We may assume without loss of generality that $i = k$, i.e., a_k occurs exactly once.

We can move the factor of P containing a_k to the left in the product P by interchanging disjoint transpositions and/or employing the equality $(cb)(ba_k) = (ca_k)(cb)$. Doing this repeatedly, we find that for some $x \in \{1, \cdots, n\}$,

$$(a_1 \cdots a_k) = P = (xa_k)\tau,$$

where τ is a product of $t-1$ transpositions, none of which contain the entry a_k. Since the permutation on the left sends a_k to a_1, we must have $x = a_1$. Multiplying on the left by the transposition $(a_1 a_k)$, we obtain

$$(a_1 \cdots a_{k-1}) = \tau.$$

Since τ is a product of $t-1 < k-2$ transpositions, the $(k-1)$-cycle on the left can be expressed as a product of fewer than $k-2$ transpositions. This contradicts the minimality of k. □

3.2 Lemma 2

Lemma 2. *Let $2 \leq k \leq n$. Suppose that $(a_1 \cdots a_k) \in S_n$ equals a product P of exactly $k-1$ transpositions in S_n. Then every entry in the product P is one of the a_i, $i = 1, 2, \cdots, k$.*

Proof. The result is obvious for $k = 2, 3$. Assume there exists a minimal $k \geq 4$ for which the result is false. Let A denote the set $\{a_1, \cdots, a_k\}$, and let $X = \{x_1, \cdots, x_r\}$ denote the set of entries in the product P which are not in the set A. Note that our choice of k shows that X is nonempty.

CASE 1: Every factor of P with an entry in X has both entries in X.
In this case, repeatedly use the equality $(a_i a_j)(x_i x_j) = (x_i x_j)(a_i a_j)$ if necessary to move all of the factors of the form $(x_i x_j)$ to the far left in P. Thus

$$(a_1 \cdots a_k) = P = \sigma\tau,$$

where all entries in the product σ lie in X and all entries in the product τ lie in A. Since X is nonempty, τ must be a product of fewer than $k-1$ transpositions. Since σ and τ are disjoint, the above equality is impossible unless σ is equal to the identity permutation. Thus

$$(a_1 \cdots a_k) = \tau.$$

This contradicts Lemma 1, since τ is the product of fewer than $k-1$ transpositions.
CASE 2: Some factor of P has the form (xa) with $x \in X$, $a \in A$.
Repeatly interchanging disjoint transpositions and/or using equalities of the form $(ya)(xa) = (xa)(xy)$ or $(yx)(xa) = (xa)(ya)$, we can move (xa) to the far left in P, so that

$$(a_1 \cdots a_k) = P = (xa)\tau,$$

where τ is a product of $k-2$ transpositions. Multiply on the left by (xa) to obtain

$$(a_1 \cdots a_{i-1} x a_i \cdots a_k) = \tau, \quad \text{where} \quad a_i = a.$$

The $(k+1)$-cycle on the left is thus equal to a product of $k-2$ transpositions, which contradicts Lemma 1. □

3.3 Lemma 3

Lemma 3. *Let $2 \leq k \leq n$. Suppose that the k-cycle $c = (a_1 \cdots a_k) \in S_n$ equals a product P of $k-1$ transpositions in S_n. Then at least one of these $k-1$ factors has the form*

$$(a_i a_{i+1}), \quad 1 \leq i < k. \tag{5}$$

Proof. The result is obvious for $k = 2$. For $k \geq 3$, we will induct on k. By Lemma 2, every entry in P is one of the a_i. Let $(a_u a_v)$ denote the rightmost factor of P with $u < v$. Write $w = v - u$. If $w = 1$, we are done, so assume that $w > 1$. Define the w-cycle

$$s = (a_{u+1} \cdots a_v)$$

and the $(k-w)$-cycle

$$t = (a_1 \cdots a_u, a_{v+1} \cdots a_k).$$

If $w = k-1$, then t is interpreted as the 1-cycle (a_1). It is easily checked that $c(a_u a_v) = ts$. Thus ts can be written as a product of $k-2$ transpositions, all factors of P.

Let F denote the set of w entries in s and let G denote the set of $k-w$ entries in t. Note that F and G are disjoint sets whose union is $\{a_1, \cdots, a_k\}$. Suppose for the purpose of contradiction that one of the $k-2$ transposition factors of ts were of the form (fg) with $f \in F$ and $g \in G$. Repeatedly interchanging disjoint transpositions and/or using equalities of the form $(fg)(af) = (ag)(fg)$ or $(fg)(ag) = (af)(fg)$, we can write ts as a product of $k-2$ transpositions with rightmost factor (fg). Thus $ts(fg)$ is a product of $k-3$ transpositions. On the other hand, since s and t are disjoint cycles where s has entry f and t has entry g, we see that $ts(fg)$ is a k-cycle (just as we saw above that $ts(a_u a_v)$ equals the k-cycle c). A k-cycle cannot be written as a product of $k-3$ transpositions by Lemma 1, so we have a contradiction.

We now know that the $k-2$ transposition factors in ts are of two disjoint types: those that switch elements of F and those that switch elements of G. Consequently,

$$ts = BA,$$

where A is a product of factors of the first type and B is a product of factors of the second type. Since $t^{-1}B$ and As^{-1} are disjoint permutations whose product is the identity, it follows that $s = A$ and $t = B$. By Lemma 1, the w-cycle s cannot be a product of fewer than $w-1$ transpositions, and similarly, t cannot be a product of fewer than $k-w-1$ transpositions. The combined number of factors in the products A and B is $k-2$, so the products A and B have exactly $w-1$ and $k-w-1$ factors, respectively. Since the w-cycle s is a product of $w-1$ transpositions, it follows from the induction hypothesis that s (and hence P) has a factor of the form (4). □

4 Optimal methods to undo P_1 and P_2

4.1 Undoing P_1

Theorem 2. *For $n \geq 5$, let P_1 denote the product of $n-1$ transpositions in S_n given by $P_1 = (12)(23)(34) \cdots (n-1, n)$. Then there exists a product*

σ of $n+1$ distinct transpositions in S_n which undoes P_1, and this result is best possible in the sense that no such σ can have fewer than $n+1$ distinct factors.

Proof. Define $\sigma = (3n)(2, n-1)(1n)(14)(2n)(13) \cdot (35) \cdots (3, n-1)$, where when $n = 5$, the empty product $(35) \cdots (3, n{-}1)$ is interpreted as the identity. It is easily checked that $\sigma P_1 = I$ and that σ is a product of $n+1$ distinct transpositions in S_n all distinct from the $n{-}1$ transpositions in P_1. It remains to prove optimality.

Suppose for the purpose of contradiction that there exists a product E of $k < n+1$ distinct transpositions in S_n for which $EP_1 = I$ and for which the k transpositions in E are distinct from the $n-1$ transpositions in P_1. Since $EP_1 = I$, the Parity Theorem shows that $k \leq n{-}1$. On the other hand, since $P_1 = (12 \cdots n)$, Lemma 1 gives $k \geq n{-}1$. Thus the number of transpositions in the product E is exactly $n-1$. Note that E^{-1} is a product of these same $n-1$ transpositions in reverse order, and $E^{-1} = P_1 = (12 \cdots n)$. Hence by Lemma 3, one of these $n-1$ transpositions in E has the form $(i, i+1)$ with $1 \leq i < n$. This contradicts the distinctness of the factors of E from those in P_1, since by definition, P_1 is a product of all $n-1$ transpositions $(i, i+1)$ with $1 \leq i < n$. □

The restriction $n \geq 5$ in Theorem 2 cannot be relaxed. Clearly P_1 cannot be undone in S_n when $n < 4$. Assume for the purpose of contradiction that for $n = 4$, there is a σ that undoes $P_1 = (12)(23)(34)$ in S_4. Then to avoid overlap, σ must be a product of the three unused transpositions in S_4, namely (14), (24), (13). Applying Lemma 2 to $\sigma^{-1} = (1234)$, we see that σ^{-1} and hence σ must contain one of the factors (12), (23), (34), a contradiction.

4.2 Undoing P_2

Theorem 3. *For $n \geq 3$, let P_2 denote the product of $n-1$ transpositions in S_n given by $P_2 = (n, n-1) \cdots (n3)(n2)(n1)$. Then there exists a product τ of $n+1$ distinct transpositions in S_{n+1} which undoes P_2, and this result is best possible in the sense that no such τ can have fewer than $n+1$ distinct factors.*

Proof. Define $\tau = (2, n+1)(3, n+1)(4, n+1) \cdots (n, n+1) \cdot (1, 2)(1, n+1)$. It is easily checked that $\tau P_2 = I$ and that τ is a product of $n+1$ distinct transpositions in S_{n+1} all distinct from the $n-1$ transpositions in P_2. It remains to prove optimality.

Suppose for the purpose of contradiction that there exists a product F of $k < n+1$ transpositions in S_{n+1} for which $FP_2 = I$ and for which the k transpositions in F are distinct from the $n-1$ transpositions in P_2. Since $FP_2 = I$, the Parity Theorem shows that $k \leq n-1$. On the other hand, since $P_2 = (12\cdots n)$, Lemma 1 gives $k \geq n-1$. Thus the number of transpositions in the product F is exactly $n-1$. Note that F^{-1} is a product of these same $n-1$ transpositions in reverse order, and $F^{-1} = P_2 = (12\cdots n)$. Hence by Lemma 2, the entries in these $n-1$ transpositions all lie in the set $\{1, 2, \cdots, n\}$. Since the permutation F moves n, it follows that one of these $n-1$ transpositions in F has the form (in) with $1 \leq i < n$. This contradicts the distinctness of the factors of F from those in P_2, since by definition, P_2 is a product of all $n-1$ transpositions (in) with $1 \leq i < n$. □

5 I as a product of m distinct transpositions in S_n

Theorem 4. *For the identity I to be expressible as a product of m distinct transpositions in S_n, it is necessary and sufficient that m be an even integer with $6 \leq m \leq \binom{n}{2}$.*

Proof. We begin by showing that the conditions are necessary. First, m must be even by the Parity Theorem. Clearly $m > 2$, and furthermore, m cannot exceed $\binom{n}{2}$, since $\binom{n}{2}$ is the number of distinct transpositions in S_n. To complete the proof of necessity, we now show that $m \neq 4$. Assume for the purpose of contradiction that $I = WXYZ$, where W, X, Y, Z are distinct transpositions. Then the product $WXYZ$ has at least 4 distinct entries, each occurring at least twice. (For if some entry z occurred only once, then $WXYZ$ could not map z to z.) Thus the product must have exactly four distinct entries a, b, c, d, each occurring exactly twice. Suppose first that X and W are not disjoint, so that say $W = (ab)$ and $X = (ac)$. Then $YZ = (abc)$, which is impossible because the entry a occurs once in W and once in X, so a cannot occur in either Y or Z. Thus X and W must be disjoint. Since $WX = ZY$, it follows that Z and Y are disjoint. Then either $W = Y$ or $W = Z$, contradicting the fact that W is distinct from Y and Z. This completes the proof of necessity. It remains to show sufficiency.

Define

$$f(a,b,c) = (ac)(ab)(bc),$$

which we view formally as a product of 3 transpositions, while noting that $f(a,b,c)$ equals (ab) when viewed as a permutation. If a product λ of transpositions has a factor (ab), then formally replacing (ab) by $f(a,b,c)$ increases the number of λ's factors by 2, without altering λ as a permutation.

We next show how to express I explicitly as a product of distinct transpositions in S_4, S_5, S_6, S_7, and S_8. Our treatment for S_5, S_6, S_7, and S_8 illustrates the general inductive procedure, but it may be skipped if desired. For $m = 6$, we have the base case

$$I = (12)(23)(14)(13)(24)(34) \quad \text{in } S_4.$$

This equality uses all six transpositions in S_4, so to consider the values $m = 8, 10$, we move up to S_5. For $m = 8$, replace the first transposition (12) above by $f(1,2,5)$ to obtain

$$I = (15)(12)(25)(23)(14)(13)(24)(34) \quad \text{in } S_5.$$

For $m = 10$, replace the transposition (34) above by $f(3,4,5)$ to obtain

$$I = (15)(12)(25)(23)(14)(13)(24)(35)(34)(45) \quad \text{in } S_5.$$

This equality uses all ten transpositions in S_5, so to consider the values $m = 12, 14$, we move up to S_6. For $m = 12$, replace (23) above by $f(2,3,6)$ to obtain

$$I = (15)(12)(25)(26)(23)(36)(14)(13)(24)(35)(34)(45) \quad \text{in } S_6.$$

For $m = 14$, replace (45) above by $f(4,5,6)$ to obtain

$$I = (15)(12)(25)(26)(23)(36)(14)(13)(24)(35)(34)(46)(45)(56) \quad \text{in } S_6.$$

This equality uses all of the fifteen transpositions in S_6 except for (16), so to consider values $m = 16, 18, 20$, we move up to S_7. For $m = 16, 18, 20$, successively replace (12) by $f(1,2,7)$, (34) by $f(3,4,7)$, and (56) by $f(5,6,7)$, respectively. This yields the following for $m = 20$:

$$\begin{aligned} I = {} & (15)(17)(12)(27)(25)(26)(23)(36)(14)(13)(24)(35)\times \\ & \times\ (37)(34)(47)(46)(45)(57)(56)(67) \quad \text{in } S_7. \end{aligned}$$

This equality uses all of the twenty-one transpositions in S_7 except for (16), so to consider values $m = 22, 24, 26, 28$, we move up to S_8. For $m = 22, 24, 26$, successively replace (23) by $f(2, 3, 8)$, (45) by $f(4, 5, 8)$, and (67) by $f(6, 7, 8)$, respectively. This yields the following for $m = 26$:

$$\begin{aligned} I = {} & (15)(17)(12)(27)(25)(26)(28)(23)(38)(36)(14)(13)(24)(35)(37)\times \\ & \times\ (34)(47)(46)(48)(45)(58)(57)(56)(68)(67)(78) \quad \text{in } S_8. \end{aligned}$$

This equality uses all twenty-eight transpositions in S_8 except (16) and (18). This suggests that we make the atypical replacement of (68) by $f(6, 8, 1)$ to obtain the following for $m = 28$:

$$\begin{aligned} I = {} & (15)(17)(12)(27)(25)(26)(28)(23)(38)(36)(14)(13)(24)(35)(37)\times \\ & \times\ (34)(47)(46)(48)(45)(58)(57)(56)(16)(68)(18)(67)(78) \quad \text{in } S_8. \end{aligned}$$

This equality uses all twenty-eight transpositions in S_8.

We now describe the general inductive procedure for constructing equalities in S_{4k+1} through S_{4k+4}, for $k \geq 1$. For the remainder of the proof, we use the notation $N = 4k$ and $b(m) = \binom{m}{2}$. (The motivation for working successively with blocks $\{S_{N+1}, S_{N+2}, S_{N+3}, S_{N+4}\}$, $N = 4, 8, 12, \cdots$ is that for all $n \geq 2$, the parities of $b(n)$ and $b(n + 4)$ are the same.)

Starting from the equality in S_N corresponding to

$$m = b(N),$$

successively replace (12) by $f(1, 2, N + 1)$, (34) by $f(3, 4, N + 1)$, $\cdots$, $(N - 1, N)$ by $f(N - 1, N, N + 1)$ to obtain the equalities in S_{N+1} for

$$m = b(N) + 2,\ b(N) + 4,\ \cdots,\ b(N) + N,$$

respectively.

Starting from the last equality in S_{N+1}, which corresponds to

$$m = b(N) + N = b(N + 1),$$

successively replace (23) by $f(2, 3, N + 2)$, (45) by $f(4, 5, N + 2)$, $\cdots$, $(N, N + 1)$ by $f(N, N + 1, N + 2)$ to obtain the equalities in S_{N+2} for

$$m = b(N + 1) + 2,\ b(N + 1) + 4,\ \cdots,\ b(N + 1) + N,$$

respectively. The last equality uses all $b(N+2)$ transpositions in S_{N+2} except $(1, N+2)$.

Starting from this last equality in S_{N+2}, which corresponds to

$$m = b(N+2) - 1,$$

successively replace (12) by $f(1, 2, N+3)$, (34) by $f(3, 4, N+3)$, $\cdots$, $(N+1, N+2)$ by $f(N+1, N+2, N+3)$ to obtain the equalities in S_{N+3} for

$$m = b(N+2) + 1,\ b(N+2) + 3,\ \cdots,\ b(N+2) + N + 1,$$

respectively. The last equality uses all $b(N+3)$ transpositions in S_{N+3} except $(1, N+2)$.

Starting from this last equality in S_{N+3}, which corresponds to

$$m = b(N+3) - 1,$$

successively replace (23) by $f(2, 3, N+4)$, (45) by $f(4, 5, N+4)$, $\cdots$, $(N+2, N+3)$ by $f(N+2, N+3, N+4)$ to obtain the equalities in S_{N+4} for

$$m = b(N+3) + 1,\ b(N+3) + 3,\ \cdots,\ b(N+3) + N + 1,$$

respectively. The last equality uses all $b(N+4)$ transpositions in S_{N+4} except $(1, N+2)$ and $(1, N+4)$. Finally, make the atypical replacement of the transposition $(N+2, N+4)$ by $f(N+2, N+4, 1)$ to obtain the equality in S_{N+4} for

$$m = b(N+3) + N + 3.$$

This equality uses all $m = b(N+4)$ transpositions in S_{N+4}. □

6 Appendix: A proof of the Parity Theorem

Recall that the Parity Theorem states the following. If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even in both cases or odd in both cases.

Proof. Let S_n denote the group of all permutations of the set

$$[n] = \{1, 2, \cdots, n\}.$$

For $\sigma \in S_n$, where $n \geq 2$, we define the set of inversions of $\sigma \in S_n$ by

$$I_\sigma = \left\{ \{i,j\} : i \neq j, \text{ and } \frac{\sigma(i) - \sigma(j)}{i - j} < 0 \right\}.$$

Then the number of inversions of σ is the cardinality of I_σ. Define the mapping $\epsilon : S_n \longrightarrow \{\pm 1\}$ by

$$\epsilon(\sigma) = \begin{cases} 1, & \text{if the number of inversions of } \sigma \text{ is even} \\ -1, & \text{if the number of inversions of } \sigma \text{ is odd.} \end{cases}$$

And define the parity of σ to be $\epsilon(\sigma) = (-1)^{|I_\sigma|}$. It is not hard to show that

$$I_{\sigma\tau} = I_\sigma \ \Delta \ \sigma^{-1}(I_\tau),$$

where Δ denotes the symmetric difference and $\sigma\{i,j\} = \{\sigma(i), \sigma(j)\}$ for $\{i,j\} \in [n]_2$, the set of 2-element subsets of $[n]$. Noting that $|\sigma^{-1}(I_\tau)| = |I_\tau|$, we have

$$\begin{aligned} |I_{\sigma\tau}| &= |I_\sigma| + |\sigma^{-1}(I_\tau)| - 2|I_\sigma \cap \sigma^{-1}(I_\tau)| \\ &= |I_\sigma| + |I_\tau| - 2|I_\sigma \cap I_\tau|. \end{aligned}$$

Thus, $|I_{\sigma\tau}| \equiv |I_\sigma| + |I_\tau| \pmod 2$, which implies

$$(-1)^{|I_{\sigma\tau}|} = (-1)^{|I_\sigma| + |I_\tau|} = (-1)^{|I_\sigma|} + (-1)^{|I_\tau|}$$

and hence $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$. Moreover, $\epsilon(I) = (-1)^0 = 1$. Therefore, the mapping ϵ is a homomorphism. When $\varsigma = (12)$, we have $\epsilon(\varsigma) = (-1)^1 = -1$. Notice that ς is order inverting on $\{1,2\}$ and order preserving on all other doubletons in $[n]_2$. Let $\sigma = (ij)$ be an arbitrary transposition in S_n, and let γ be a permutation in S_n such that γ maps $\{1,2\}$ onto $\{i,j\}$, then we have $\sigma = \gamma\varsigma\gamma^{-1}$. Thus, $\epsilon(\sigma) = \epsilon(\gamma\varsigma\gamma^{-1}) = \epsilon(\gamma)\epsilon(\varsigma)\epsilon(\gamma)^{-1} = -1$. Therefore, if we have a permutation $P = t_1 t_2 \cdots t_r = s_1 s_2 \cdots s_v$, then apply ϵ to both sides we obtain $\epsilon(t_1) \cdots \epsilon(t_r) = \epsilon(s_1) \cdots \epsilon(s_v)$, which implies $(-1)^r = (-1)^v$ and hence $r \equiv v \pmod 2$. Since r and v are both even or odd, the result follows. □

References

[1] J. Beachy and W. Blair, *Abstract Algebra*, 3rd edition, Waveland Press (2006).

[2] The Commutator, vol.2 issue 1
http://issuu.com/the-commutator/docs/the-commutator-vol2-issue1

[3] Futurama and Keeler's Theorem: Original Edit
http://www.youtube.com/watch?v=8M4dUj7vZJc

[4] I. Martin Isaacs, *Algebra: A Graduate Course*, Graduate Studies in Mathematics, vol. 100, Amer. Math. Soc. (1994).

[5] I. Martin Isaacs, email communication, January 23, 2012.

[6] A. G. Levine, The Futurama of physics with David X. Cohen, *Amer. Physical Soc. News* **19** (2010) 3;
http://www.aps.org/publications/apsnews/201005/profiles.cfm

[7] Mathematics Genealogy Project,
http://genealogy.math.ndsu.nodak.edu/id.php?id=129988

[8] R. K. Oliver, On the parity of a permutation, *Amer. Math. Monthly* **118** (2008) 734–735.

[9] Writers Guild of America,
http://wga.org/awards/awardssub.aspx?id=1517