MAKING DERANGEMENTS USING ELEMENT SWAPS

Pranjal Jain
thereligiousatheists@gmail.com

Abstract: The aim of the article is to show that there always exists a sequence of swaps of elements, which when applied to a derangement (of n>3 elements) will go through all derangements of n elements, with an additional constraint that all swaps in this sequence produce a derangement (not necessarily one which hasn't appeared before in the sequence).

August, 2020

1 Introduction

The Steinhaus-Johnson-Trotter Algorithm (SJTA henceforth) is an algorithm which uses swaps of adjacent elements to generate all permutations of a given set in $n! - 1$ swaps. The aim of this paper is to prove a similar result for derangements.

Problem definition

Let a 'switch' refer to the act of exchanging the positions of the elements in any pair chosen in any permutation of $S_n = \{1, 2, \dots, n\}$ (unlike the SJTA, where it would refer to the act of swapping any pair of **adjacent** elements).

We explore whether it is possible to cover all derangements using only switches, starting at the derangement $T_n = \{n, 1, 2, \dots, n-1\}$, with the additional constraint that any switch made in our sequence of switches must result in a **derangement**, and never in a non-derangement. Note that henceforth in this article, **any** sequence of switches which is referred to satisfies this condition even if it is not explicitly mentioned.

Note that in the absence of this constraint, the problem is a trivial application of the SJTA, and under the absence of the freedom of swapping **any** two elements (and restricting to swapping only adjacent elements), it is trivially impossible to have such a sequence, since no swap of adjacent elements can be used to convert T_n into another derangement.

2 Some lemmas regarding the setup

For convenience, let $p(n)$ be the proposition that all derangements can be covered as dictated by the above conditions starting at T_n, and let $q(n)$ be the proposition that the same task can be done by starting at **any** derangement. We will prove the following lemma regarding p and q.

Lemma 2.1

If $p(n)$ is true for some n, then so is $q(n)$.

Proof

Let $p(n)$ be true for some n, because there exists a sequence A of switches which goes through all derangements of S_n, starting at T_n.

Let D_n be the set of all derangements of S_n. Let Δ be the sequence of derangements obtained by applying A to T_n.

Let $X \in D_n$ be an arbitrary derangement of S_n, which appears at least once in Δ (by definition), and let A_X be the subsequence of A s.t. (such that) applying A_X to T_n gets us to X.

Since each switch has a corresponding 'inverse', s.t. applying a switch to some permutation and then applying its inverse leaves the permutation unchanged, we can also say that each sequence of switches has a corresponding inverse sequence, s.t. applying the sequence to some permutation and then applying its inverse leaves the permutation unchanged.

Hence, we can simply apply A_X^{-1} (inverse of A_X) to X to get to T_n, and then apply A to T_n to cover all elements of D_n, hence showing that a sequence of switches exists s.t. starting at X, we can cover all elements of D_n. ■

Lemma 2.2

Consider a derangement π of S_{n+1} ($n \geq 5$), s.t. $\pi(k) = n+1$ for some $k \neq n+1$, and let $p(n)$ and $p(n-1)$ (and hence, $q(n)$ and $q(n-1)$, by *Lemma 2.1*) be true. Then, there exists some sequence of switches A s.t. when it is applied to π,
(1) it goes through all derangements of S_{n+1} in which $n+1$ is at the k-th position.
(2) it never switches $n+1$ with any other element.

Proof

Let 'a' denote the element a of S_n, and let '$[a]$' denote the a-th position in any permutation (not the element at the a-th position, but the position itself).

Call $[a]$ the '*home*' of a for every $a \in S_n$. Hence, an alternative definition of a derangement of S_n is that it is a permutation of S_n in which none of the elements are at their respective *homes*.

Now, let's analyse π under this definition. If we neglect the element $n+1$ and $[k]$ in π (since we are not going to switch $n+1$ with anything), then we see that every element other than k has a *home*, and k has no *home*. This means that for any permutation of these elements to be a derangement, k can go to any position but the rest can only go to a position which is not their *home*.

Consider the following two cases which are mutually exclusive and cover all possibilities :
Case I : $\pi(n+1) \neq k$
Case II : $\pi(n+1) = k$

Case I : In this case, we will temporarily assign $[n+1]$ as the *home* of k. Hence, π (neglecting $n+1$ and $[k]$) is simply some derangement of n objects, since none of the objects are at their respective *home*. This means that we can use the fact that $q(n)$ is true to guarantee that there is some sequence of switches A_1 s.t. applying A_1 to π covers all derangements of S_{n+1} which have $n+1$ at $[k]$ and don't have k at $[n+1]$. After we apply A_1 to π, we will apply A_1^{-1} to get us back to π before proceeding.

This leaves only the derangements of S_{n+1} in which k is at $[n+1]$. To cover these, we will first perform one or more switches so that k moves over to $[n+1]$.

If $\pi(n+1) \neq \pi^{-1}(k)$, then this can simply be done using a single switch between k and $\pi(n+1)$.

If $\pi(n+1) = \pi^{-1}(k)$, then this switch can't be made since it will lead us to a non-derangement permutation ($\pi(n+1)$ will end up at its *home*). So, we will cover the possibility that $\pi(n+1) = \pi^{-1}(k)$ by considering the following four mutually exclusive cases which cover all possibilities:
Case Ia : $k \neq n$ (so $k \leq n-1$), and $\pi(n+1) \neq k+1$.
Case Ib : $k \neq n$ (so $k \leq n-1$), and $\pi(n+1) = k+1$.
Case Ic : $k = n$ and $\pi(n+1) \neq n-1$.
Case Id : $k = n$ and $\pi(n+1) = n-1$.

Case Ia : In this case, we will switch k and $\pi(k+1)$, and then we switch k with $\pi(n+1)$ ($\pi(k+1)$ acts as a 'middleman' of sorts). If we use the notation '$a \to [b]$' to indicate that a is at $[b]$, then we have the following chronology :

$$\text{Start}: \; k \to [\pi(n+1)],\, \pi(k+1) \to [k+1],\, \pi(n+1) \to [n+1]$$
$$\text{After first switch}: \; \pi(k+1) \to [\pi(n+1)],\, k \to [k+1],\, \pi(n+1) \to [n+1]$$
$$\text{After second switch}: \; \pi(k+1) \to [\pi(n+1)],\, \pi(n+1) \to [k+1],\, k \to [n+1]$$

This completes *Case Ia*.

Case Ib : In this case, we use the same idea of having a 'middleman', but we use $k-1$ in place of $k+1$ if $k \geq 2$, and we use $k+2$ if $k = 1$.

Case Ic : We use the same idea as in *Case Ia*, but with $k-1$ in place of $k+1$ (since now we have $k+1 = n+1$).

Case Id : We use the same idea as in *Case Ia*, but with $k-2$ in place of $k+1$.

Now that we have a derangement in which k is at $[n+1]$ and $n+1$ is at $[k]$ (let's name it π'), we will ignore $[n+1]$ and $[k]$ (and hence, the elements k and $n+1$), since none of the switches we make henceforth will involve those.

Now, notice that π' (neglecting $[k]$ and $[n+1]$) is simply a derangement of $n-1$ objects, since each object has a *home* and none of them are at their respective *homes*. Hence, using the fact that $q(n-1)$ is true, we can guarantee that there exists some sequence A_2 of switches which when applied to π' will go through all derangements of S_{n+1} in which k is at $[n+1]$ and $n+1$ is at $[k]$, which proves *Lemma 2* for *Case 1*.

Summary : First, we showed using $p(n)$ that there is some sequence of switches A_1, which when applied to π goes through all derangements of S_{n+1} in which $n+1$ is at $[k]$ and k is not at $[n+1]$. After applying A_1 to π, we applied A_1^{-1} to the resultant derangement in order to come back to π, for convenience.

Then, we made either 1 or 2 (depending on the circumstances) switches to bring k to $[n+1]$, and then used $p(n-1)$ to show that there is some sequence A_2 of switches, which when applied to the resultant derangement goes through all derangements of S_{n+1} in which $n+1$ is at $[k]$ and k is at $[n+1]$, hence proving *Lemma 2* for *Case 1*.

Case II : In *Case I*, we first covered the derangements with $n+1$ being at $[k]$ and k not being at $[n+1]$, and then we covered the derangements with $n+1$ being at $[k]$ and k being at $[n+1]$.

In this case, we first cover the derangements in which $n+1$ is at $[k]$ and k is at $[n+1]$ using $p(n-1)$, then we remove k from $[n+1]$ by switching it with any element which is not $n+1$, and then cover all derangements in which $n+1$ is at $[k]$ and k is not at $[n+1]$ using $p(n)$. ■

3 The Induction Step

We will now show using *Lemma 2.2* that $p(n)\hat{\ }p(n-1) \rightarrow p(n+1) = T$ (T denotes *true*) for $n \geq 5$.

Proof

We start off with $T_{n+1} = \{n+1, 1, 2, \ldots, n\}$, and then use *Lemma 2* with $k = 1$ to guarantee the existence of a sequence A_1, which when applied to T_{n+1} will cover all derangements with $n+1$ at [1]. Then, we apply A_1^{-1} to the resultant derangement to come back to T_{n+1}, for convenience.

Now, we switch $n+1$ and 2, and then we use *Lemma 2* with $k = 3$ to guarantee the existence of a sequence A_3, which when applied to T_{n+1} will cover all derangements with $n+1$ at [3]. Then, we apply A_3^{-1} to the resultant derangement to come back to T_{n+1}, for convenience.

We keep going this way till we cover all derangements with $n+1$ in odd positions, and then we reverse **all** the switches made so far and come back to T_{n+1}.

Now, we will cover the derangements with $n+1$ at even positions.

First, we switch $n+1$ with 2 (in T_{n+1}), and then we switch $n+1$ with 1, hence leaving us with the derangement $\tau = \{2, n+1, 1, 3, 4, \ldots, n\}$. Now, we use *Lemma 2* with $k = 2$ to guarantee the existence of a sequence A_2, which when applied to τ will cover all derangements with $n+1$ at [2]. Then, we apply A_2^{-1} to the resultant derangement to come back to τ, for convenience.

Now, we switch $n+1$ with 3, and then we use *Lemma 2* with $k = 4$ to guarantee the existence of a sequence A_4, which when applied to τ will cover all derangements with $n+1$ at [4]. Then, we apply A_4^{-1} to the resultant derangement to come back to τ, for convenience.

We keep going this way till we cover all derangements with $n+1$ in even positions, hence covering all derangements of S_{n+1} and proving the claim. $\blacksquare$

4 Proof for $n = 4$

Now that we have proved the induction step, we only need to prove the base cases (i.e. that $p(4) = p(5) = T$).

Note that $p(3)$ is trivially false, since there are only 2 elements in D_3 and it requires at least 2 switches to get from one to the other, that's why we are choosing $n = 4$ and $n = 5$ as our base cases.

For showing that $p(4)$ is true, we can simply draw a graph where the vertices are derangements of S_4 and 2 vertices are connected iff there exists a single switch which can change one into the other, and notice that the graph is *connected*, hence proving the claim.

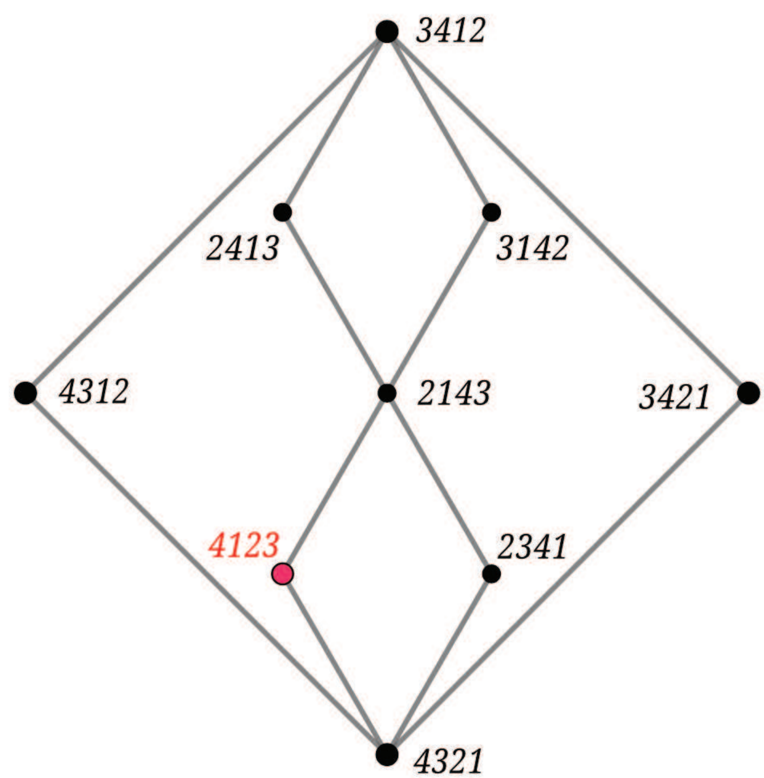

Figure 1: Graph for $n = 4$

5 Proof for $n = 5$

The proof that $p(5) = T$ can't be done by hand without immense room for error, since there would be 44 vertices if we drew a similar graph as before for $n = 5$, and each vertex would have either 5 or 6 edges (see *Section 6: Open Problem and Misc Results* $\rightarrow$ *Result 1* for the proof of this claim). Hence, I wrote a Java program in NetBeans IDE 8.2, which was linked with a database made in MySQL 5.5 to do the job for me.

Code logic : First, we make a table in MySQL which contains all derangements of S_5 (order is immaterial), except for T_5. This can be done using a different code (if you do it this way, you can actually skip making the database altogether and simply feed the derangements straight into the Java code), but I simply entered them by hand and then used the following measures to ensure that there were no errors in the entered data :
(1) Checked that there were exactly 43 entries.
(2) Ensured that every entry was unique (by declaring the derangement column as a primary key).
(3) Writing a simple code to check that each entry was in fact a derangement.

With the database in place, we first define a custom method which takes in a string and swaps the characters in the specified positions (note that this method was designed specifically for the purpose of making switches in derangements and it won't work on arbitrary strings in which there is repetition of characters).

Then, we link the code and the database and make a loop which goes through all the entries of the table in the database. For each entry in the table, we make at most 1001 (this bound can be changed) random switches in T_5 (ensuring that each switch results in a derangement). After each switch, we check if the resulting derangement is equal to the table entry in question. We keep making these switches till one of the following occurs :
(1) The derangement made using switches on T_5 equals the table entry in question.
(2) 1001 switches have been made without reaching the table entry in question, in which case we print out this particular entry for manual checking.

Once one of these events occurs, we move to checking the next entry of the table.

Hence, if at the end of execution we see that there is no text output, that means that the code found a path from T_5 to each entry in the table, meaning that in the graph for $n = 5$, we can always find a path starting at T_5 and ending at $D \in D_5$, for every D, hence proving that the graph is connected and $p(5) = T$. This is indeed what I received as the result.

You can view and copy my code and view the MySQL table here : `https://drive.google.com/drive/folders/11IYgcBCDXrya36ZB0bZefQwsu3wdl8DC?usp=sharing`.

In the next section, I propose an open problem and prove some miscellaneous results about the setup, and the reader may judge their usefulness in solving the open problem.

6 Open Problem and Misc Results

Let $\alpha(n)$ refer to the graph with vertices being derangements of S_n, and any pair of vertices is connected iff making a single switch in one derangement of the pair is sufficient to construct the other in the pair.

The **open problem** I wish to propose is that of finding the least number of switches it takes to cover all elements starting at T_n as a function of n, and to find how this function changes when one changes the starting point.

I feel that $\alpha(n)$ will be symmetric w.r.t. (with respect to) all the vertices which have the same number of edges, so the function will be the same for any pair of starting points which have the same number of edges. Note that this is pure speculation on my part.

Some miscellaneous results

Result 6.1 : Bounds on the number of edges at each vertex

For any given derangement D of S_n, let $f_n(D)$ be the number of edges at the vertex representing D in $\alpha(n)$. Then,

(1) For n even ($n \geq 4$),

$$^nC_2 - n \leq f_n(D) \leq {}^nC_2 - \tfrac{n}{2}.$$

(2) For n odd ($n \geq 3$),

$$^nC_2 - n \leq f_n(D) \leq {}^nC_2 - \tfrac{n+3}{2}.$$

Proof

Let D be some derangement of S_n. Define $\beta_n(D)$ to be the graph which has elements of S_n as vertices, where any pair of vertices is connected by an edge iff performing a switch on that pair in D results in a non-derangement permutation. Also, let $E(G)$ denote the number of edges in any graph G.

Since the total number of switches one can perform in any permutation of n elements is $^nC_2$, the number of switches in D which lead to a derangement is $^nC_2 - E(\beta_n(D))$. Note that this is also the value of $f_n(D)$.

Hence, our problem now reduces to finding a bound on $E(\beta_n(D))$.

Firstly, notice that every vertex in $\beta_n(D)$ has either 1 or 2 edges, since any $a \in S_n$ appearing at $[b]$ in D can't be switched with b and $D(a)$ (since doing so would result in a non-derangement). Hence, a has 2 edges in $\beta_n(D)$ iff $b \neq D(a)$, and a has 1 edge in $\beta_n(D)$ iff $b = D(a)$.

Further, notice that if some $a \in S_n$ has exactly 1 edge in $\beta_n(D)$, then it must be connected to some $b \in S_n$ which also has exactly 1 edge in $\beta_n(D)$. Hence, vertices with single edges come in pairs in $\beta_n(D)$, which also means that we can never have a vertex with exactly 1 edge connected to a vertex with exactly 2 edges.

Lemma

The set of all vertices in $\beta_n(D)$ with exactly 2 edges each forms a set of polygons.

Proof

Firstly, we can't have exactly 1 or exactly 2 vertices with exactly 2 edges each. Hence, there are 3 or more such vertices (or zero).

Let a_1 be an arbitrary such vertex, and let a_2 be one of the two vertices connected to a_1. Let a_3 be a vertex connected to a_2 ($a_3 \neq a_1$). Now, either a_3 is connected to a_1, in which case a_1 is the part of a complete polygon which is disconnected from the rest of the vertices, or a_3 connects to some $a_4 \neq a_1, a_2$.

Now, either a_4 connects to a_1, in which case a_1 is part of a polygon disconnected from the rest of the graph, or it connects to some $a_5 \neq a_1, a_3$. We can keep going this way, and eventually, we will either show that a_1 is part of a polygon which is disconnected from the rest of the vertices, or we will run out of more vertices to introduce, hence having to connect the last vertex to a_1 and showing that a_1 is part of a polygon.

Hence, we have shown that any arbitrary vertex with 2 edges must be part of a polygon, hence proving the lemma. ■

Now, let the number of vertices in $\beta_n(D)$ with exactly 1 edge be $2m$, for some non-negative integer m. Hence, we see that

$$E(\beta_n(D)) = m + (n - 2m) = n - m \ \ldots (i)$$

This is because m edges in $\beta_n(D)$ are contributed by the $2m$ vertices with exactly one edge each, and the remaining $n-2m$ vertices form polygons with a total vertex count of $n - 2m$, and hence, a total edge count of $n - 2m$. For n even we have $0 \leq m \leq \frac{n}{2}$, and for n odd we have $0 \leq m \leq \frac{n-3}{2}$ (since we can't have a single vertex with exactly 2 edges), hence proving the claimed inequality for $f_n(D)$. ■

Result 6.2 : The number of solutions in D given $\beta_n(D)$

Consider a graph G with n vertices, each representing a unique number in S_n, s.t.

(1) any vertex in this graph has either exactly 1 or exactly 2 edges.

(2) any vertex with exactly 1 edge is connected to another vertex with exactly 1 edge.

(3) no vertex is connected to itself.

(4) no pair of vertices is connected by more than one edge.

Let the number of polygons in this graph be k. Then, there are 2^k solutions in $D \in D_n$ for the equation

$$\beta_n(D) = G$$

Proof

Firstly, notice that the lemma proved as part of *Result 1* also applies to any G as defined above . Hence, we can guarantee that the we can partition the vertices in G into those that are vertices of a polygon and those that have only 1 edge which connects them to another vertex with only 1 edge.

First, let's consider an arbitrary pair of elements with exactly one edge each $(a, b) \in S_n^2$ s.t. a is connected to b. Since we want G to be $\beta_n(D)$ for some $D \in D_n$, this must mean that a and b can't be switched with each other and only each other in D (if we want the switch to result in a derangement), meaning that a is at $[b]$ and b is at $[a]$ in D (i.e. $D(a) = b$ and $D(b) = a$).

Since the choice of a and b was arbitrary, this means that we now know $D(a)$ for all $a \in S_n$ which has only 1 edge.

Now, we'll try to find $D(a)$ if a is the vertex of a polygon in G. Consider an arbitrary vertex a_1 of an arbitrary polygon with s sides in G. Let the vertices joined to a_1 be a_2 and a_s, those joined to a_2 be a_1 and a_3, and so on, all the way till a_s. Consider the following pair of mutually exclusive cases which cover all possibilities :
Case I : $D(a_1) = a_2$
Case II : $D(a_2) = a_1$

Case I : In this case, we now know that $D(a_2) = a_3, D(a_3) = a_4, \ldots, D(a_{s-1}) = a_s$ and $D(a_s) = a_1$, hence forcing us into one and only one choice for the value of D and D^{-1} over these s elements.

Case II : In this case, we know that $D(a_3) = a_2, D(a_4) = a_5, \ldots, D(a_s) = a_{s-1}$ and $D(a_1) = a_s$, hence forcing us into one and only one choice for the value of D and D^{-1} over these s elements.

Hence, we have exactly 2 distinct ways to choose the values which D takes over the vertices of any given polygon in G (and the choice for any polygon doesn't affect the choice for any other polygon), hence showing that there are exactly 2^k choices for $D \in D_n$ s.t. $\beta_n(D) = G$ (since there is only one way to choose the values which D takes over the vertices with exactly 1 edge each), hence proving the desired result. ■

It is also worth mentioning that this result gives us an expression for the number of vertices in $\alpha(n)$ with a given number of edges.

Result 6.3 : 'Rotations' of a derangement

Call a permutation (of S_n) π' a 'rotation' of a permutation (of S_n) π iff there is some $k \in \{0, 1, 2, \ldots, n-1\}$ s.t.

$$\pi(r) = \pi'[mod_n(r+k)]\,\forall\, r \in S_n$$

where $mod_n(a) \equiv a\,(mod\, n)$ and $mod_n(a) \in S_n\,\forall\, a \in \mathbb{Z}$.

Further, call a derangement $D \in D_n$ 'of level L' iff there are exactly L rotations of D which are derangements. Then,
(1) all rotations of D are of the same level as D.
(2) there are no derangements of level n in D_n.
(3) all derangements of level $n-1$ in D_n are rotations of S_n.

Proof

The proof for the first two claims is trivial, and so is left out.

It is easy to see that all rotations of S_n other than itself are derangements, and so they are all of level $n-1$. Also, a defining property of any rotation D of S_n is that the non-derangement rotation of D (i.e. S_n) is such that every element is at its *home*. Hence, showing that the non-derangement rotation of an arbitrary level $n-1$ derangement X must have the property that every element is at its *home* suffices to prove the claim.

We will show this using a proof by contradiction. Assume that the non-derangement rotation Y of X (where X is a derangement of level $n-1$) has some element a which is at $[b] \neq [a]$. Hence, if we consider the rotation Y' of Y (and hence of X, since any rotation of Y is also a rotation of X) defined as

$$Y(r) = Y'\{mod_n[r + mod_n(a-b)]\}\,\forall\, r \in S_n$$

we see that $a = Y(b) = Y'(a)$, meaning that Y' is not a derangement. However, this is contradictory to the assumption that X is a level $n-1$ derangement, since $Y' \neq Y$ (a consequence of the fact that $a \neq b$), meaning that there are 2 distinct rotations of X which are non-derangements. Hence, the claim is proved. ■

It may be worth noting that if n is odd, then $\beta_n(D)$ for any level $n-1$ derangement $D \in D_n$ is an n-gon (and hence, all such D have exacly ${}^nC_2 - n$ edges in $\alpha(n)$), and if n is even, the same is true for all level $n-1$ derangements $D \in D_n$, except for when D is defined as

$$D(r) = mod_n\left(r + \frac{n}{2}\right) \,\forall\, r \in S_n$$

since in this case, we have

$$D^{-1}(r) = mod_n\left(r - \frac{n}{2}\right) = mod_n\left(r + \frac{n}{2}\right) = D(r)$$

meaning that the 2 elements which r can't be switched with are equal. In this special case, D will have ${}^nC_2 - \frac{n}{2}$ edges in $\alpha(n)$.

Result 6.4 : Switches always change the parity of the permutation

It's obvious at first sight that any switch of adjacent elements always switches the parity of the permutation in which the switch was executed. However, I claim that the non-obvious result that a switch between **any** pair of elements changes the parity of the starting permutation holds as well.

Proof

Consider some permutation π of S_n, in which we wish to switch some a (which is originally at $[A]$) with some b (which is originally at $[B]$) $(A < B)$. Let the permutation obtained after making this switch be π'.

Let p be the be the number of values of $k \in S_n$ s.t. $k \in (A, B)$ and $\pi(k) > a$, and let q be the number of values of $k \in S_n$ s.t. $k \in (A, B)$ and $\pi(k) < b$.

Let N be the number of inversions in π, and likewise define N' for π' (an inversion is a pair $\{x, y\}$ s.t. $x > y$ and $\pi(x) < \pi(y)$).

Now, let us consider the new inversions which were created as a result of switching a and b, and those that were 'destroyed' as a result of the same.

Inversions involving an element at some $[C]$ (s.t. $C \in [1, A) \cup (B, n]$) and a or b are neither created nor destroyed, since the position of a and b w.r.t. an element at such a position is not changed by this switch.

If we look at inversions involving an element at some $[C]$ (s.t. $C \in (A, B)$) and a, then we see that p new inversions are created, and $(B - A - 1 - p)$ pre-existing inversions are destroyed. Likewise, considering the inversions involving an element at some $[C]$ (s.t. $C \in (A, B)$) and b, then we see that q new inversions are created, and $(B - A - 1 - q)$ pre-existing inversions are destroyed.

One inversion involving b and a is also created/destroyed (depending on whether it existed before the switch or not). Hence, we get that

$$N' = N + p + q - (B - A - 1 - p) - (B - A - 1 - q) \pm 1 \equiv N + 1 \ (mod\ 2)$$

(the ± 1 is to account for the inversion of a and b which is created/destroyed by the switch), hence proving the claim. ■

This result could prove relevant for the open problem because it tells us that any sequence of switches of odd length must end at a derangement of parity opposite to that of the starting derangement, and likewise, any sequence of switches of even length must end at a derangement with the same parity as the starting derangement.