Derangements and Rubik's Cubes

Nick Rui

Tuesday, June 3, 2025

Abstract

When a finite group G acts on a finite set X, it may be the case that some elements of G do nothing to some elements of X. We discuss this "fixture" phenomena, first proving Burnside's lemma which relates the average number of elements fixed by any $g \in G$ to the number of orbits of the group action. Then, we discuss derangements, which are elements of G that fix nothing in X, and prove that a transitive group action will always have a derangement. Finally, we explore examples of derangements in the symmetric group and the dihedral group, and also have fun analyzing group actions on Rubik's cubes.

1 Burnside's Lemma

Let G be a finite group acting on a finite set X. It may happen that some $g \in G$ "fixes" some element $x \in X$ in the sense that $g \cdot x = x$. By the definition of a group action, we know that $1 \cdot x = x$ for all $x \in X$, but when else can this occur? In this section, we build up a proof of Burnside's lemma, which relates the number of orbits of a group action with the average number of elements fixed by some $g \in G$.

Definition 1.1. For any $x \in X$, the *orbit* of x is $\mathcal{O}_x = \{g \cdot x : g \in G\}$.

Definition 1.2. For any $x \in X$, the *stabilizer* of x is $G_x = \{g \in G : g \cdot x = x\}$.

Definition 1.3. For any $g \in G$, the *fixed point set* of g is $X^g = \{x \in X : g \cdot x = x\}$.

The notions of stabilizers and fixed point sets capture the "fixture" property from different perspectives. On one hand, G_x takes some x and collects elements in G, while X^g takes some g and collects elements in X. So, the following relation is intuitive.

Lemma 1.4. *The sum of the sizes of all stabilizers is equal to the sum of the sizes of all fixed point sets. Explicitly,*

$$\sum_{x \in X} |G_x| = \sum_{g \in G} |X^g|.$$

Proof. Let's count how many pairs $(g, x) \in G \times X$ have the property that $g \cdot x = x$. One such way to count this is to consider every element of X and count the size of its stabilizer. This gives

$$\#\{(g, x) \in G \times X : g \cdot x = x\} = \sum_{x \in X} |G_x|.$$

Alternatively, we can also consider every element of G and count the size of its fixed point set, which gives

$$\#\{(g, x) \in G \times X : g \cdot x = x\} = \sum_{g \in G} |X^g|.$$

Combining both of these counting approaches proves the lemma. □

We know that this group action partitions X into a disjoint union of orbits. How many orbits does X partition into? Recall that the orbit-stabilizer theorem states $|G_x| = |G|/|\mathcal{O}_x|$. Combining this with Lemma 1.4 gives Burnside's lemma.

Theorem 1.5. *(Burnside's Lemma) The number of orbits of X is equal to the average size of all fixed point sets. Explicitly,*

$$\#\{\textit{orbits of } X\} = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof. By the orbit-stablizer theorem, Lemma 1.4 becomes

$$\sum_{x \in X} \frac{|G|}{|\mathcal{O}_x|} = \sum_{g \in G} |X^g|.$$

Let us reindex the summation on the left hand side to sum over orbits of X instead of elements of X. Denote the set of all orbits of X as $\mathcal{O} = \{\mathcal{O}_x : x \in X\}$. An arbitrary orbit $\mathcal{O}_x$ contains $|\mathcal{O}_x|$ elements in X, and so this orbit contributes $|\mathcal{O}_x|$ times in the summation. So, the left hand side simplifies to

$$\sum_{\mathcal{O}_x \in \mathcal{O}} |\mathcal{O}_x| \frac{|G|}{|\mathcal{O}_x|} = \sum_{\mathcal{O}_x \in \mathcal{O}} |G| = |\mathcal{O}||G|.$$

Substituting into the previous equation and dividing by $|G|$ gives

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

as desired. □

2 Derangements

The size of the fixed point set of some $g \in G$ gives a notion of how "disruptive" g is. For example, the identity fixes everything, so it is not disruptive at all. In contrast, some extremely disruptive elements may fix nothing. We call these elements derangements.

Definition 2.1. A *derangement* is an element $g \in G$ such that $|X^g| = 0$, i.e., g does not fix any element in X.

Theorem 2.2. *If G acts transitively on X and $|X| > 1$, then there exists a derangement.*

Proof. Suppose that $|X| > 1$, and that G acts transitively on X. By definition of transitivity, this action partitions X into a single orbit. Applying Burnside's Lemma gives

$$1 = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

This means the average size of a fixed point set is 1. So, if we show there exists a fixed point set with size > 1, then it follows that there must also exist a fixed point set of size 0 (in order to "average out" the size of fixed point sets to 1). Therefore, to show the existence of a derangement, it suffices to show the existence of a fixed point set with size > 1.

Consider the identity $1 \in G$. By definition of a group action, $1 \cdot x = x$ for all $x \in X$. Thus, the fixed point set of 1 is the entire set X itself. So, $|X^1| = |X|$ and since $|X| > 1$ we have found a fixed point set with size > 1. This proves the theorem. □

3 Examples

Example 3.1. Let the symmetric group S_n act naturally on the set $X = \{1, 2, \ldots, n\}$ (assume $n > 1$). We know that this action is transitive, since every permutation of elements in X can be permuted into any other permutation of elements in X by some element of S_n.

Theorem 2.2 tells us that there must exist a derangement. This is intuitive, since there are many ways to permute $\{1, 2, \ldots, n\}$ such that every element is "disturbed". For example, any n-cycle is a derangement. In fact, every element in S_n without 1-cycles in its cycle decomposition is a derangement.

How many derangements does S_n have? Let's use Burnside's Lemma as a sanity check. We know that the identity permutation $1 \in S_n$ fixes all n elements, and so $|X^1| = n$. Since this group action is transitive, Burnside's Lemma tells us that the average size of all fixed point sets is 1, and so there must be at least $n - 1$ elements that fix no points and are thus derangements (in order to "average out" the average size of fixed point sets to 1). In S_n, we clearly have more than $n - 1$ derangements, since the number of n-cycles is already $(n - 1)!$.

Explicitly determining the number of derangements is an interesting combinatorial problem. For a specific fixed n, one could determine all the possible ways to partition n into cycle lengths ≥ 2 and count how many such permutations can be created, but this doesn't generalize well into a formula for any n. Let's take another perspective.

Take F_i to be the set of all permutations that fix element i. So, F_i is the set of all permutations that permute among the $n-1$ elements that are not i, and so $|F_i| = (n-1)!$. Derangements, by definition, do not belong in F_i for any $i = 1, 2, \ldots, n$. So, the set of all derangements is

$$S_n \setminus \bigcup_{i=1}^{n} F_i.$$

Let $D(S_n)$ denote the number of derangements in S_n. We have

$$D(S_n) = \left| S_{2n} \setminus \bigcup_{i=1}^{n} F_i \right| = |S_n| - \left| \bigcup_{i=1}^{n} F_i \right|.$$

By the inclusion-exclusion principle, we can write

$$\left| \bigcup_{i=1}^{n} F_i \right| = \sum_i |F_i| - \sum_{i<j} |F_i \cap F_j| + \sum_{i<j<k} |F_i \cap F_j \cap F_k| - \cdots + (-1)^{n+1} |F_1 \cap \ldots \cap F_n|.$$

Let's break this down this term by term. The first summation is

$$\sum_i |F_i| = \sum_i (n-1)! = n(n-1)! = n!.$$

For the second summation, note we have $\binom{n}{2}$ intersections, and each intersection $F_i \cap F_j$ is the set of all permutations that fix i and j and permute among the rest of the $n-2$ elements. So, the size of $F_i \cap F_j$ is $(n-2)!$, and so

$$\sum_{i<j} |F_i \cap F_j| = \binom{n}{2}(n-2)! = \frac{n!(n-2)!}{2!(n-2)!} = \frac{n!}{2!}$$

For the third summation, there are $\binom{n}{3}$ intersections, each with size $(n-3)!$ by similar argument. So,

$$\sum_{i<j<k} |F_i \cap F_j \cap F_k| = \binom{n}{3}(n-3)! = \frac{n!(n-3)!}{3!(n-3)!} = \frac{n!}{3!}.$$

For the ℓ-th summation, there are $\binom{n}{\ell}$ intersections each with size $(n-\ell)!$, which will simplify to $n!/\ell!$. Thus, we have

$$\left| \bigcup_{i=1}^{n} F_i \right| = \sum_{\ell=1}^{n} (-1)^{\ell+1} \frac{n!}{\ell!} = n! \sum_{\ell=1}^{n} \frac{(-1)^{\ell+1}}{\ell!}.$$

So, the number of derangements is

$$D(S_n) = n! - n! \sum_{\ell=1}^{n} \frac{(-1)^{\ell+1}}{k!} = n! \sum_{\ell=0}^{n} \frac{(-1)^{\ell+1}}{\ell!}.$$

(Note that as $n \to \infty$, the summation converges to $1/e$. So, the number of derangements in S_n for large n can be approximated by $n!/e$.)

Example 3.2. Let the symmetric group S_n act naturally on k-element subsets of $\{1, 2, \ldots, n\}$. There are $N = \binom{n}{k}$ subsets that elements of S_n act on. Let us require $1 < k < n$, since the case of $k = 1$ is Example 3.1 and the case of $k = n$ is trivial, as there is only one n-element subset of $\{1, 2, \ldots, n\}$ which is the set itself. We easily see this action is transitive, since any k-element subset $\{i_1, \ldots, i_k\}$ can be sent to any other k-element subset $\{j_1, \ldots, j_k\}$ by the permutation in S_n that maps $i_1 \mapsto j_1, \ldots, i_k \mapsto j_k$. Thus, a derangement must exist. How many?

Taking the same inclusion-exclusion approach as in Example 3.1 leads to some complicated combinatorics. Let X_i be an arbitrary k-element subset of $\{1, 2, \ldots, n\}$. Let F_i be the set of all elements of S_n that fix X_i. Then, as in Example 3.1, the number of derangements of this action, denoted by $D_k(S_n)$, is

$$D_k(S_n) = \left| S_n \setminus \bigcup_{i=1}^{N} F_i \right| = |S_n| - \left(\sum_i |F_i| - \sum_{i<j} |F_i \cap F_j| + \cdots + (-1)^{N+1} |F_1 \cap \ldots \cap F_N| \right).$$

Since F_i is the set is all permutations that permute within the k elements in X_i and the $n - k$ elements not in X_i, it's easy to see that $|F_i| = k!(n-k)!$. However, since k-element subsets can intersect, calculating the size of the intersection of multiple F_i's becomes complicated. Even for $F_i \cap F_j$, counting this intersection requires counting elements that permute within the subsets $X_i \cap X_j$, $X_i \setminus X_j$, $X_j \setminus X_i$ and $\{1, 2, \ldots, n\} \setminus (X_i \cup X_j)$. Counting the intersection of large amounts of F_i becomes even more difficult, as these k-element subsets can intersect in many ways.

We take an alternative approach to count the number of derangements. For any $\sigma \in S_n$, write its cycle decomposition (including 1-cycles) as

$$\sigma = (a_1 a_2 \ldots a_{\ell_1})(b_1 b_2 \ldots b_{\ell_2}) \ldots,$$

where ℓ_i is the cycle length of the i-th cycle. We have a finite list of cycle lengths $\ell_1, \ell_2, \ldots, \ell_t$ such that $\ell_1 + \cdots + \ell_t = n$. Then, we see that if there exists some sublist $\ell_{i_1}, \ldots, \ell_{i_s}$ such that $\ell_{i_1} + \cdots + \ell_{i_s} = k$, then σ permutes within the elements involved in the $i_1, i_2, \ldots, i_s$-th cycles. Thus, σ permutes within some k-element subset, and so σ will fix this k element subset and thus not be a derangement. From this, it follows that

$$D_k(S_n) = \#\{\sigma \in S_n : \text{no combination of cycle lengths add to } k\}.$$

An explicit formula for $D_k(S_n)$ is not actually known (according to Sound).

As a concrete example, consider the case when $n = 4$ and $k = 2$. The 2-element subsets are

$$\{1, 2\},\ \{1, 3\},\ \{1, 4\},\ \{2, 3\},\ \{2, 4\},\ \{3, 4\}.$$

Let us analyze how elements of S_4 behave on these subsets. The identity fixes everything. Every 2-cycle will fix one of the subsets, and two disjoint 2-cycles will fix two of the subsets. Every 3-cycle and 4-cycle will be a derangement, since they involve cycling more than 2 elements and so no set of two elements can map to the same set of two numbers under these cycles. There are $\binom{4}{3}2! = 8$ 3-cycles and $3! = 6$ 4-cycles in S_4. So, we have 14 derangements.

Example 3.3. Let the dihedral group D_{2n} act naturally on the vertices of a regular n-gon. Because this action allows us to freely rotate the regular n-gon, we already see that this action is transitive, and thus derangements will exist. Again, we examine how many derangements exist.

Geometrically, it's easy to see that every rotation element r^i with $i = 1, 2, \ldots, n-1$ is a derangement. What about the reflection elements?

For odd n, note that every axis of symmetry of an n-gon always passes through a vertex. In this case, reflection elements will always fix the vertex the axis of symmetry passes through, and so no reflections can be derangements.

For even n, note that half of the axes of symmetry of an n-gon pass through two opposite vertices, and the other half pass through opposite edges. In this case, half of the reflections fix two vertices, while the other half are derangements.

So, for odd n the number of derangement is $n - 1$ (the number of rotation elements), but for even n the number of derangements is $n - 1 + n/2$ (all rotations and half of the reflections).

Example 3.4. Let G act on itself by conjugation (and suppose G is not the trivial group). Note that conjugating 1 by any $g \in G$ gives $g1g^{-1} = gg^{-1} = 1$, showing that every element fixes at least one element in G (namely, the identity). Thus, this group action has no derangements. By the contrapositive of Theorem 2.2, it follows that a group acting on itself by conjugation can never be a transitve action (this makes sense, as the identity will always form a conjugacy class of its own).

Example 3.5. A Rubik's cube (of any size, not necessarily $3 \times 3 \times 3$) has six faces that can be rotated. Let U, D, R, L, F, B denote 90 degree clockwise turns of a Rubik's cube of any size along the up, down, right, left, front, back faces. The set of all ways we can jumble a Rubik's cube forms a group generated by these moves. We define the group of moves on a Rubik's cube as

$$\mathcal{R} = \langle U, D, R, L, F, B \rangle.$$

Elements of this group are read from left to right. For example, the element $RUR^{-1}U^{-1}$ (colloquially called the "sexy move") represents the sequence of moves where the right face is rotated 90 degrees clockwise, then the up face is rotated 90 degress clockwise, then the right face is rotated 90 degrees counterclockwise, then the up face is rotated 90 degrees counterclockwise. Because of this, the notion of bracketing is not very useful, so the notion of associativity—for practical purposes—can be ignored. Aside from that, we can easily verify this is indeed a group, since the identity exists (the move that does nothing), and for any sequence of moves, performing the reverse of those moves in reverse order gives the inverse.

Alone, know very little about $\mathcal{R}$ other than the fact that each generator has order 4. We discover more information about $\mathcal{R}$ when we allow it to act on some set (say, the stickers of a Rubik's cube of certain size), and analyze how elements of $\mathcal{R}$ permute the set (see Aside 3.8).

Let X be the set of all 54 stickers on a $3 \times 3 \times 3$ Rubik's cube, and let $\mathcal{R}$ act on X in the way we would imagine. For this group action, imagine we fix the cube in space (so that the 'front' face is always facing us, the 'up' face is always facing up, etc.) and perform rotations on the faces. Is this action transitive, and are there any derangements?

We claim there are no derangements. To show this, take any *center sticker* (one of six stickers at the center of a face), and realize that its position cannot be affected by any rotations of faces. Thus, no element of $\mathcal{R}$ will change the position of the center stickers, showing that there cannot be derangements in this group action.

Example 3.6. A more interesting example arises if we let $\mathcal{R}$ act on just the 48 *non-center stickers* of a $3 \times 3 \times 3$ Rubik's cube. Let us denote this set as Y. Now, any sticker in Y is "movable" by some move in $\mathcal{R}$. Is there a derangement? That is, is there a move that changes the location of every sticker in Y?

It turns out there are many such moves. For example, $RL^{-1}FB^{-1}UD^{-1}RL^{-1}$ is a derangement.

However, we note that this group action is *not* transitive. This follows from recognizing that the set of stickers has a very rigid structure, as stickers are partitioned into a subset of *corner stickers* and a subset of *edge stickers.*

corner	edge	corner
edge	center	edge
corner	edge	corner

No matter what moves we perform, a corner sticker can only ever reside in a corner position, and similarly for edge stickers. Thus, the orbit of a corner sticker cannot contain any edge stickers, showing that this group action cannot have just a single orbit. This gives a nice example demonstrating why the converse of Theorem 2.2 is false.

Example 3.7. Let $\mathcal{R}$ act on the set of all 24 stickers on a $2 \times 2 \times 2$ Rubik's cube. Denote this set as Z. Equivalently, Z can also be viewed as the set of all corner stickers of a $3 \times 3 \times 3$ Rubik's cube, and so Z is a subset of Y. It then follows that this group action has derangements as well.

However, this case is interesting since now every element of the set is a corner sticker. One can show (by working moves out on a Rubik's cube) that there is always a sequence of moves to move one corner sticker to any other corner position. Thus, this group action is transitive as well.

To summarize, we have shown that $\mathcal{R}$ acting on

(i) all 54 stickers of a $3 \times 3 \times 3$ cube has no derangements (and thus is not transitive)

(ii) the 48 non-center stickers of a $3 \times 3 \times 3$ cube has derangements but is not transitive

(iii) all 24 stickers of a $2 \times 2 \times 2$ cube (equivalently, the 24 corner stickers of a $3 \times 3 \times 3$ cube) has derangements and is transitive.

Aside 3.8. When we let $\mathcal{R}$ act on some set of stickers X, there is a homomorphism $\varphi : \mathcal{R} \to S_{|X|}$. From here, we can better understand elements in $\mathcal{R}$ by analyzing their order as permutations in the image of φ. Essentially, looking at how moves permute the stickers gives insight into the structure of the group of moves itself.

Let us take the case when X is all 54 stickers in on a $3 \times 3 \times 3$ cube. We don't know much about the order of the "sexy move" $RUR^{-1}U^{-1}$, but as a permutation in S_{54}, $\varphi(RUR^{-1}U^{-1})$ has order 6 (which one can verify by starting on a fully solved Rubik's cube and continually iterating the moves $RUR^{-1}U^{-1}$, counting the number of iterations until the cube returns to its original solved state). Some seemingly simple sequences of moves have surprisingly large order, while some long sequences of moves have small order. For example $\varphi(RU)$ has order 105, while $\varphi(RUR^{-1}U^{-1}R^{-1}FR^2U^{-1}R^{-1}U^{-1}RUR^{-1}F^{-1})$ has order 2.

When we let $\mathcal{R}$ act on the stickers of a $2 \times 2 \times 2$ cube, the orders of the moves may differ from the $3 \times 3 \times 3$ case. Let $\psi : \mathcal{R} \to S_{24}$ be the homomorphism obtained when $\mathcal{R}$ acts on the set of stickers of a $2 \times 2 \times 2$ cube. One can verify that $\psi(RUR^{-1}U^{-1})$ still has order 6 and $\varphi(RUR^{-1}U^{-1}R^{-1}FR^2U^{-1}R^{-1}U^{-1}RUR^{-1}F^{-1})$ still has order 2, but in fact $\psi(RU)$ has order 15 (not 105).

References

[1] Richard E Borcherds. *Group theory 10: Burnside's lemma.* YouTube. 2020. URL: https://www.youtube.com/watch?v=jhfFfYfmMpc.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra.* 3rd ed. Hoboken, NJ: John Wiley & Sons, 2004. ISBN: 0-471-43334-9.

[3] Charlotte Sweeney. *Of Groups and Cubes.* Medium. 2022. URL: https://charlotte-sweeney.medium.com/of-groups-and-cubes-b2fdb3e825ce.