Pólya's enumeration theorem

Luka Opravš

December 3, 2024

Abstract

The goal of this project is to formalize the `Pólya's enumeration theorem` and some of its applications in Lean 4 using Mathlib.

1 The number of distinct colorings

Given a set of objects X and a set of colors Y, we interpret functions in $Y^X = \{f : X \to Y\}$ as *colorings* of X with colors in Y. In a coloring f, an object $x \in X$ is colored with $f(x)$.

Let G be a group. A (left) *group action* of G on a set X is a function $- \cdot - : G \times X \to X$ that satisfies:

$$\begin{aligned} 1 \cdot x = x \quad & \forall x \in X, \\ g \cdot (h \cdot x) = (gh) \cdot x \quad & \forall g, h \in G, \forall x \in X. \end{aligned}$$

For any group action, we define the following:

- **Orbits:** A group action induces an equivalence relation on X defined by $x \sim y \iff \exists g \in G : g \cdot x = y$. The quotient set X/G is the set of equivalence classes under this relation. The equivalence class of an element $x \in X$ is called the *orbit of* x and is denoted as $Gx = \{g \cdot x : g \in G\}$.
- **Fixed points:** The set of *fixed points* of $g \in G$ is $X^g = \{x \in X : g \cdot x = x\}$.

Given a group G acting on a set X, we interpret the elements of G as transformations that permute the elements of X into an equivalent configuration. If we color the elements of X using a function $f : X \to Y$ and then permute X with an element $g \in G$, we obtain an equivalent configuration with a new coloring defined by $x \mapsto f(g^{-1} \cdot x)$. The inverse g^{-1} appears in the definition of the new coloring because the color of the element x in the new permuted configuration must match the color of its preimage $g^{-1} \cdot x$ in the original configuration. Thus, for any $g \in G$, we consider the colorings f and $x \mapsto f(g^{-1} \cdot x)$ to be equivalent.

Any action of G on X induces an action of G on the set of functions $X \to Y$, mapping colorings to equivalent colorings. We will denote both group actions using $- \cdot -$, because we can always determine which action is intended from the type of the second argument.

Proposition 1. *Given a group action of G on X, we can define an induced group action of G on Y^X by:*

$$g \cdot f = (x \mapsto f(g^{-1} \cdot x)).$$

Proof.

$$(1 \cdot f)(x) = f(1^{-1} \cdot x) = f(1 \cdot x) = f(x),$$
$$(g \cdot (h \cdot f))(x) = f(h^{-1} \cdot (g^{-1} \cdot x)) = f((h^{-1}g^{-1}) \cdot x) = f((gh)^{-1} \cdot x) = ((gh) \cdot f)(x).$$

□

The orbits of this group action correspond to sets of equivalent colorings. When X and Y are finite, the set of orbits Y^X/G is also finite. The number of distinct colorings is exactly the number of orbits. From this point onward, we will assume that both X and Y are finite.

Definition 2. The *number of distinct colorings* is defined as $|Y^X/G|$.

2 Cycles of elements in a group

A group action of G on X associates each element $g \in G$ with a permutation in $S_X = \{f : X \to X \mid f \text{ is bijective}\}$. Specifically, each $g \in G$ is mapped to a permutation π_g defined by $\pi_g(x) = g \cdot x$. The mapping $\phi : G \to S_X$, given by $\phi(g) = \pi_g$, is a group homomorphism.

Using this correspondence, we define the *cycles of* g as the cycles of the permutation π_g. The number of cycles of g is denoted by $c(g)$.

In Mathlib, the function ϕ is implemented as *MulAction.toPerm*. Cycles and the decomposition of permutations into disjoint cycles are included as well. However, in our case, they are tedious to work with because cycles of length 1 are not recognized as proper cycles and are excluded from the factorizations. For this reason, we define our own version of cycles that also includes cycles of length 1.

Definition 3. Given $g \in G$, the set of *cycles of* g is defined as $X/\sim_g$, where $\sim_g$ is the equivalence relation of being in the same cycle of g:

$$x_1 \sim_g x_2 \iff \exists k \in \mathbb{Z} : \pi_g^k(x_1) = x_2.$$

The *number of cycles of* g is: $c(g) = |X/\sim_g|$.

Colorings of the cycles of $g \in G$ are then defined as functions in $Y^{X/\sim_g}$.

3 Proof of Pólya's enumeration theorem

Mathlib already includes an important result known as *Burnside's lemma*, which states that for any finite group G acting on a set X, the number of orbits is equal to the average number of fixed points:

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

This result is available as *MulAction.sum_card_fixedBy_eq_card_orbits_mul_card_group* in Mathlib.

First, we prove that for any $g \in G$, a coloring f is a fixed point of g if and only if f maps all elements in the same cycle of g to the same color.

Proposition 4. *For any* $g \in G$*:*

$$f \in (Y^X)^g \iff \forall x_1, x_2 \in X : (x_1 \sim_g x_2 \implies f(x_1) = f(x_2)).$$

Proof.

$$
\begin{aligned}
f \in (Y^X)^g &\iff g \cdot f = f, && (1)\\
&\iff \forall x \in X : (g \cdot f)(x) = f(x), && (2)\\
&\iff \forall x \in X : f(g^{-1} \cdot x) = f(x), && (3)\\
&\iff \forall x \in X, \forall k \in \mathbb{Z} : f(g^k \cdot x) = f(x), && (4)\\
&\iff (\forall x_1, x_2 \in X : (x_1 \sim_g x_2 \implies f(x_1) = f(x_2))). && (5)
\end{aligned}
$$

The (3) $\implies$ (4) implication is proven inductively.
If $k = 0$ then $f(1 \cdot x) = f(x)$ by first property of group action.
If $k \geq 1$ then we use (3) on $g^k \cdot x$ to get $f(g^{k-1} \cdot x) = f(g^k \cdot x)$ and then use the induction hypothesis $f(g^{k-1} \cdot x) = f(x)$ to conclude $f(g^k \cdot x) = f(x)$.
If $k \leq -1$ then we use (3) on $g^{k+1} \cdot x$ to get $f(g^k \cdot x) = f(g^{k+1} \cdot x)$ and then use the induction hypothesis $f(g^{k+1} \cdot x) = f(x)$ to conclude $f(g^k \cdot x) = f(x)$.

To prove that (4) $\iff$ (5) we use the fact that $x_1 \sim_g x_2 \iff \exists k \in \mathbb{Z} : g^k \cdot x_1 = x_2$.
The (4) $\implies$ (5) implication follows by using (4) with $x = x_1$ and k from $\exists k \in \mathbb{Z} : g^k \cdot x_1 = x_2$.
The (5) $\implies$ (4) implication follows by using (5) with $x_1 = g^k \cdot x$ and $x_2 = x$. □

We will only use the left-to-right implication of this result. However, the right-to-left direction is also proven, as it requires only a small amount of additional work and it nicely encapsulates the idea that the set of colorings fixed by g is the same as the set of colorings that map all elements in the same cycle of g to the same color.

Since we can interpret elements of $Y^{X/\sim_g}$ as functions that map all elements in the same cycle of g to the same color, we can conclude that $|(Y^X)^g| = |Y^{X/\sim_g}|$. However, in Lean, $(Y^X)^g$ is a set of functions that map from X, while $Y^{X/\sim_g}$ is a type of functions that map from $X/\sim_g$. Therefore, we cannot formally talk about equality of sets. To formalize our argument, we construct a bijection between $(Y^X)^g$ and $Y^{X/\sim_g}$.

Proposition 5. *Let $[x]$ denote the equivalence class of x in $X/\sim_g$.*
Let $\varphi : (Y^X)^g \to Y^{X/\sim_g}$ be defined by $\varphi(f) = [x] \mapsto f(x)$, where x is some element of $[x]$.
Let $\varphi^{-1} : Y^{X/\sim_g} \to (Y^X)^g$ be defined by $\varphi^{-1}(f) = x \mapsto f([x])$.
Then φ and φ^{-1} are well-defined and inverses of each other. Therefore we have a bijection between $(Y^X)^g$ and $Y^{X/\sim_g}$.

Proof. φ is well-defined because by Proposition 4 $f \in (Y^X)^g$ and $x_1 \sim_g x_2$ imply $f(x_1) = f(x_2)$.
φ^{-1} is well-defined because it maps to $(Y^X)^g$:

$$\forall f \in Y^{X/\sim_g}, \forall x \in X : (g \cdot \varphi^{-1}(f))(x) = f([g^{-1} \cdot x]) = f([x]) = (\varphi^{-1}(f))(x).$$

$\varphi^{-1}(\varphi(f))(x) = f(x')$, where x' is some representative of $[x]$. Therefore we have $x \sim_g x'$ and since $f \in (Y^X)^g$ by Proposition 4: $f(x) = f(x')$.
$\varphi(\varphi^{-1}(f))([x]) = f([x'])$ where x' is some representative of $[x]$. Therefore $[x] = [x']$ and then $f([x]) = f([x'])$. □

Proposition 6.

$$\forall g \in G : |(Y^X)^g| = |Y|^{c(g)}$$

Proof. The equality $|(Y^X)^g| = |Y^{X/\sim_g}|$ follows from the bijection in Proposition 5. The number of functions in $Y^{X/\sim_g}$ is $|Y|^{|X/\sim_g|}$. By definition, $c(g) = |X/\sim_g|$, which completes the proof. □

We use *Burnside's Lemma* to prove the *Pólya's enumeration theorem*.

Proposition 7. *The number of distinct colorings of X with colors in Y under the group action of G on X is:*

$$|Y^X/G| = \frac{1}{|G|}\sum_{g\in G}|Y|^{c(g)}.$$

Proof. We use *Burnside's lemma* on colorings to get:

$$|Y^X/G| = \frac{1}{|G|}\sum_{g\in G}|(Y^X)^g|.$$

Using Proposition 6, we substitute $|(Y^X)^g|$ with $|Y|^{c(g)}$. □

4 Applications

- Trivial group
- S_n
- Necklaces
- Bracelets
- Cube