Pólya's enumeration theorem

Luka Opravš

March 22, 2025

Abstract

The goal of this project is to formalize the `Pólya's enumeration theorem`, implement a fast algorithm for its usage, and formalize some of its applications in Lean 4 with 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 $X^g = \{x \in X : g \cdot x = x\}$.
- **Stabilizer:** The *stabilizer* of $x \in X$ is $G_x = \{g \in G : g \cdot x = x\}$.

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 $S_X = \{\pi : X \to X \mid \pi \text{ is bijective}\}$. 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: $c(g) = |X/\sim_g|$.
The *number of elements in* G *with exactly* i *cycles* is: $|\{g \in G \mid c(g) = i\}|$.

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. It is stated as:

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

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 the 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 *Pólya's enumeration theorem*. Since division of natural numbers in Lean is defined as an operation $-/- : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ that rounds downwards (and returns 0 when dividing by 0), we first prove a version of the theorem without division to preserve the fact that $\sum_{g\in G} |Y|^{c(g)}$ is divisible by $|G|$.

Theorem 7. (Pólya's enumeration theorem) *The number of distinct colorings of X with colors in Y under the group action of G on X is:*

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

A version of the theorem that preserves the fact that $\sum_{g\in G} |Y|^{c(g)}$ is divisible by $|G|$ is also provided:

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

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

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

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

We also formalize a version of the theorem where the sum ranges over the possible numbers of cycles. We denote $[n] = \{0, \dots, n-1\}$.

Theorem 8.

$$|Y^X/G| \cdot |G| = \sum_{i\in[|X|+1]} |\{g \in G \mid c(g) = i\}| \cdot |Y|^i.$$

Proof. For any $g \in G$ we have $0 \le c(g) \le |X|$. Then:

$$|Y^X/G| \cdot |G| = \sum_{g\in G} |Y|^{c(g)} = \sum_{i\in[|X|+1]} \sum_{g'\in\{g\in G|c(g)=i\}} |Y|^i = \sum_{i\in[|X|+1]} |\{g \in G \mid c(g) = i\}| \cdot |Y|^i.$$

□

4 Computation

To enable efficient usage of *Pólya's enumeration theorem*, we construct a function that quickly computes the number of cycles of any permutation of the set $[n]$. By renaming the elements of X with an arbitrary bijection $X \to [n]$, we can compute the numbers of cycles of elements of the group using this function.

We define the number of cycles of a permutation as follows:

Definition 9. Given a permutation $\pi \in S_X$, the set of *cycles of* π is defined as $X/\sim_\pi$, where $\sim_\pi$ is the equivalence relation of being in the same cycle of π:

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

The *number of cycles of* π is:

$$c(\pi) = |X/\sim_\pi|.$$

Since working with cardinalities of quotients can be somewhat abstract, we show that the number of cycles is equal to the cardinality of any set that contains exactly one representative from each cycle of the permutation.

Proposition 10. *For a permutation $\pi \in S_X$ and a set S containing exactly one element from each cycle of π, we have $c(\pi) = |S|$.*

Proof. We construct a bijection $\varphi : X/\sim_\pi \to S$ defined by:

$$\begin{aligned}\varphi([x]) &= \text{the unique element in } S \text{ that lies in the same cycle as } x,\\ \varphi^{-1}(x) &= [x].\end{aligned}$$

Since φ is a bijection, we conclude that $c(\pi) = |S|$. □

We establish some auxiliary results about powers of permutations, which are needed for proving the correctness of our algorithm.

Proposition 11. *Let π be a permutation on a finite set X, and $x \in X$. Then there exists some $n \in \mathbb{N}$ such that:*

$$\pi^{n+1}(x) = x.$$

Proof. Since X is finite, the cycle containing x has finite length. We set n to be the length of this cycle minus 1. □

Proposition 12. *Let π be a permutation such that $\pi^n(x) = x$ for some $n \in \mathbb{N}$. Then for any $m, r \in \mathbb{N}$, we have:*

$$\pi^{m\cdot n+r}(x) = \pi^r(x).$$

Proof. We prove this by induction on m.
If $m = 0$, the equation follows immediately.
If $m > 0$, then

$$\pi^{(m+1)\cdot n+r}(x) = \pi^{m\cdot n+r}(\pi^n(x)) = \pi^{m\cdot n+r}(x),$$

and we can use the inductive hypothesis. □

Proposition 13. *Let π be a permutation such that $\pi^{n+1}(x) = x$ for some $n \in \mathbb{N}$. Then for any $k \in \mathbb{Z}$ there exists an $m \in [n+1]$ such that:*

$$\pi^k(x) = \pi^m(x).$$

Proof. We use $m = k \bmod (n+1)$. We will apply Proposition 12, which requires natural numbers, so we split the proof into cases based on whether $k \geq 0$.
If $k \geq 0$, we have:

$$\pi^k(x) = \pi^{\lfloor \frac{k}{n+1} \rfloor \cdot (n+1) + (k \bmod (n+1))}(x) = \pi^m(x).$$

If $k < 0$, we have:

$$\pi^k(x) = (\pi^{-1})^{-k}(x) = (\pi^{-1})^{\lfloor \frac{-k}{n+1} \rfloor \cdot (n+1) + (-k \bmod (n+1))}(x) = (\pi^{-1})^{-k \bmod (n+1)}(x) = \pi^{-(-k \bmod (n+1))}(x).$$

If $k \bmod (n+1) = 0$, this is equal to $\pi^m(x)$.
Otherwise, we use $\pi^{n+1}(x) = x$ to increment the power by $n+1$, making the expression equal to:

$$\pi^{n+1-(n+1-(k \bmod (n+1)))}(x) = \pi^m(x).$$

□

For an array v, we denote with $v[x] = \top$ the array that is identical to v except that it is set to $\top$ at index x. We also denote $S_n = S_{[n]}$.

We define a function that sets a boolean array indexed by $[n]$ at indices that are in the same cycle of a permutation $\pi \in S_n$ as $x \in [n]$ to $\top$ and prove that it works correctly.

Definition 14. Let $n \in \mathbb{N}$, $\pi \in S_n$, $x, y \in [n]$ and v be a boolean array indexed by $[n]$.
The function *visitCycleAux* takes v and a proof of $\exists m \in \mathbb{N}, \pi^{m+1}(x) = y$. It returns an array that is identical to v except that it is set to $\top$ at all indices in $\{x, \pi(x), \pi^2(x), \dots, \pi^{-1}(y)\}$. The function works by recursively calling itself with $v := (v[x] = \top), x := \pi(x)$ until it reaches $\pi(x) = y$, then it returns $v[x] = \top$. The proof ensures termination by guaranteeing that $\pi(x) = y$ will eventually hold.
The function *visitCycle* takes π, x, v, and returns an array identical to v except that it is set to $\top$ at all indices that are in the same cycle of π as x. It uses *visitCycleAux* with $y = x$ and a proof of $\exists m, \pi^{m+1}(x) = x$ from Proposition 11.

Proposition 15. *The function* visitCycleAux *given* $v, (\exists m \in \mathbb{N}, \pi^{m+1}(x) = y)$ *returns an array that is set to* $\top$ *at all entries where* v *is set to* $\top$.

Proof. We prove this by induction on m.
If $m = 0$, then $\pi(x) = y$ is reached immediately and the function returns $v[x] = \top$.
Otherwise the function recursively calls itself with $v' := (v[x] = \top), x := \pi(x)$. Since m satisfies $\pi^m(\pi(x)) = y$, the recursive call will result in an array that is set to $\top$ at all entires where v' is set to $\top$ by inductive hypothesis. Thus the returned array is set to $\top$ at all entries where v is set to $\top$. □

Proposition 16. *Let* $m \in \mathbb{N}$ *be the smallest number satisfying* $\pi^{m+1}(x) = y$. *Then* visitCycleAux *given* $v, (\exists k \in \mathbb{N}, \pi^{k+1}(x) = y)$ *returns an array that:*

- *is identical to* v *at all indices not in the same cycle as* x,
- *is set to* $\top$ *at all indices in* $\{x, \pi(x), \pi^2(x), \dots, \pi^m(x)\}$,
- *has the same size as* v.

Proof. This is proven by induction on m.
If $m = 0$ then $\pi(x) = y$ is reached immediately and the function returns $v[x] = \top$.
Otherwise the function recursively calls itself with $v' := (v[x] = \top), x := \pi(x)$. Since m is the smallest number satisfying $\pi^m(\pi(x)) = y$, the recursive call will result in an array that:

- is identical to the input array at all indices not in the same cycle as $\pi(x)$ (and therefore also at all indices not in the same cycle as x),
- is set to $\top$ at $\{\pi(x), \pi^2(x), \dots, \pi^m(x)\}$,
- has the same size as v' (and therefore also as v).

Since v' is set to $\top$ at x and the function can never change any entry in the array from $\top$ to $\bot$ by Proposition 15, the resulting array is still set to $\top$ at x. Thus it is set to $\top$ at all indices in $\{x, \pi(x), \pi^2(x), \dots, \pi^m(x)\}$. □

Proposition 17. *The function* visitCycle *given* π, x, v *returns an array identical to* v, *except that it is set to* $\top$ *at all indices that are in the same cycle of* π *as* x.

Proof. Let $m \in \mathbb{N}$ be the smallest number satisfying $\pi^{m+1}(x) = x$.
visitCycle calls *visitCycleAux* to return an array that is:

- identical to the input array at all indices not in the same cycle as x,
- set to $\top$ at all indices in $\{x, \pi(x), \pi^2(x), \dots, \pi^m(x)\}$,
- of the same size as the input array.

By Proposition 13, all elements that are in the same cycle as x satisfy $y = \pi^l(x)$ for some $0 \leq l < m + 1$. Thus the set $\{x, \pi(x), \pi^2(x), \dots, \pi^m(x)\}$ contains exactly all the elements that are in the same cycle of π as x. □

We define a function that computes the number of cycles of any permutation on $[n]$ and prove that it works correctly.

Definition 18. Let $n, i, c \in \mathbb{N}$, $\pi \in S_n$ and v be some boolean array indexed by $[n]$.
The function *computeNumCyclesOfPermAux* takes π, v, c and a proof that $i \leq n$. It iterates over $j \in [i-1, \dots, 0]$ and if $v[j] = \bot$ it increments c by 1 and sets v to $\top$ at all indices that are in the same cycle as j with the *visitCycle* function. Then it returns updated c.
The function *computeNumCyclesOfPerm* takes π and returns its number of cycles. It uses *computeNumCyclesOfPermAux* with $i = n, v =$ constant $\bot$ array of length n, $c = 0$.

Proposition 19. *Let $\pi \in S_n$, v be a boolean array that is set to $\top$ at exactly those indices that are in the same cycle of π as some element in $\{i, \dots, n-1\}$ and c be the cardinality of some set S of representatives of those cycles of π that contain some element in $\{i, \dots, n-1\}$.*
Then computeNumCyclesOfPermAux *given π, v, c returns the cardinality of some set of cycle representatives of π.*

Proof. This is proven by induction on i.
If $i = 0$ then the function returns c, which is already the cardinality of some set of representatives of cycles of π by assumption.
Otherwise the function checks whether $v[i-1] = \top$.

- If $v[i-1] = \top$, then $i-1$ must be in the same cycle as one of the elements in $\{i, \dots, n-1\}$. So v is already set to $\top$ at exactly those indices that are in the same cycle of π as some element in $\{i-1, \dots, n-1\}$ and c is already equal to the cardinality of some set of representatives of those cycles of π that contain some element in $\{i-1, \dots, n-1\}$. Therefore we can use inductive hypothesis to conclude that the function returns the cardinality of some set of representatives of cycles of π.
- If $v[i-1] = \bot$, then $i-1$ must be in some cycle whose elements do not appear in $\{i, \dots, n-1\}$. The function increments c by 1 and sets v at indices that are in the same cycle as $i-1$ to $\top$. Now v is set to $\top$ at exactly those indices that are in the same cycle of π as some element in $\{i-1, \dots, n-1\}$ and c is now equal to the cardinality of $S \cup \{i-1\}$ which is the set or representatives of those cycles of π that contain some element in $\{i-1, \dots, n-1\}$. We can therefore use the inductive hypothesis to conclude that the function returns the cardinality of some set of representatives of cycles of π.

□

Proposition 20. *The function* computeNumCyclesOfPerm *given π computes the cardinality of some set of representatives of cycles of π - that is a set that contains exactly one element from every cycle of π.*

Proof. The function *computeNumCyclesOfPerm* given π returns the result of *computeNumCyclesOfPermAux* given

$$i = n, \quad v = \text{constant } \bot \text{ array of length } n, \quad c = 0.$$

The result follows from Proposition 19 with $S = \emptyset$. □

Proposition 21. *The function* computeNumCyclesOfPerm *given π computes the number of cycles of π.*

Proof. By Proposition 20, *computeNumCyclesOfPerm* returns the cardinality of some set of representatives of cycles of π. By Proposition 10 this cardinality is equal to the number of cycles of π. □

Renaming the elements of X using a bijection $\phi : X \to [|X|]$ does not change the number of distinct colorings.

Proposition 22. *Given a group action of G on X, we can define an induced group action of G on $[|X|]$ with:*

$$g \cdot i = \phi(g \cdot \phi^{-1}(i)).$$

Proof.

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

□

Proposition 23. *The number of distinct colorings of X with colors in Y under the group action of G on X is equal to the number of distinct colorings of $[|X|]$ with colors in Y under the induced group action of G on $[|X|]$.*

Proof. We define the bijection:

$$\varphi : Y^X/G \to Y^{[|X|]}/G, \quad [f] \mapsto [f \circ \phi^{-1}]$$

with inverse

$$\varphi^{-1} : Y^{[|X|]}/G \to Y^X/G, \quad [f] \mapsto [f \circ \phi].$$

These are well-defined, since for any $f, h \in Y^X$ with $f = g \cdot h$, we have:

$$\begin{aligned}
(f \circ \phi^{-1}) &= (g \cdot h) \circ \phi^{-1} \\
&= (x \mapsto h(g^{-1} \cdot x)) \circ \phi^{-1} \\
&= i \mapsto h(g^{-1} \cdot \phi^{-1}(i)) \\
&= i \mapsto h(\phi^{-1}(\phi(g^{-1} \cdot \phi^{-1}(i)))) \\
&= i \mapsto ((h \circ \phi^{-1})(g^{-1} \cdot i)) \\
&= g \cdot (h \circ \phi^{-1}).
\end{aligned}$$

and similarly for any $f, h \in Y^{[|X|]}$ such that $f = g \cdot h$, we have:

$$f \circ \phi = g \cdot (h \circ \phi).$$

Since φ and φ^{-1} are mutual inverses, it follows that

$$|Y^X/G| = |Y^{[|X|]}/G|.$$

□

We now define a function that computes the number of distinct colorings using *Pólya's enumeration theorem* and prove its correctness.

Proposition 24. *The function* computeNumDistinctColorings *computes the number of distinct colorings of X with colors in Y under the group action of G. It uses* Pólya's enumeration theorem *and the function* computeNumCyclesOfPerm *to count cycles of permutations:*

$$|Y^X/G| = \frac{1}{|G|} \sum_{g \in G} |Y|^{computeNumCyclesOfPerm(\phi \circ \pi_g \circ \phi^{-1})}.$$

Proof. By Proposition 23, we rewrite $|Y^X/G| = |Y^{[|X|]}/G|$. The result then follows from *Pólya's enumeration theorem* (Proposition 7) and the correctness of *computeNumCyclesOfPerm* (Proposition 21). □

5 Numbers of distinct colorings for some concrete examples

5.1 Trivial group

The trivial group is a group that contains only a unit. Its group action is defined by $1 \cdot x = x$. Since for any $f \in Y^X$, we have $1 \cdot f = f$, each coloring is only equivalent to itself. Thus, the number of distinct colorings is:

Proposition 25.

$$|Y^X/\{1\}| = |Y|^{|X|}.$$

Proof. We define a bijection $\varphi : Y^X/\{1\} \to Y^X$ by:

$$\varphi([f]) = f, \quad \varphi^{-1}(f) = [f].$$

This is well-defined since:

$$[f] = [h] \implies f = 1 \cdot h = h.$$

It follows that:

$$|Y^X/\{1\}| = |Y^X| = |Y|^{|X|}.$$

Alternatively, we can derive the result using *Pólya's enumeration theorem*:

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

We used the fact that 1 has $|X|$ cycles. □

5.2 Necklaces

For $n \geq 1$ we interpret the elements of the group $\mathbb{Z}_n$ as n beads of a necklace, where $x \in \mathbb{Z}_n$ is connected with $x+1$ and $x-1$ (computed in $\mathbb{Z}_n$). Necklaces can be rotated, but not reflected. The elements of the group $\mathbb{Z}_n$ are also interpreted as rotations of the necklace, where $i \in \mathbb{Z}_n$ rotates the necklace by $\frac{2\pi i}{n}$. This defines a group action of $\mathbb{Z}_n$ on itself with $i \cdot x = i + x$ (computed in $\mathbb{Z}_n$).

Definition 26. For $n \geq 1$, the *number of distinct colorings of a necklace with n beads and m colors* is given by:

$$|[m]^{\mathbb{Z}_n}/\mathbb{Z}_n|.$$

For $n = 0$, we define that there is a single coloring of a necklace with 0 beads. This is defined separately since we do not have a finite group $\mathbb{Z}_0$. This definition is inspired by the fact that $Y^\emptyset$ contains exactly one function.

Proposition 27. *The number of distinct colorings of a necklace can be computed using the* computeNumDistinctColorings *function.*

Proof. By Proposition 24. □

5.3 Bracelets

For $n \geq 1$, we interpret the elements of the group $\mathbb{Z}_n$ as n beads of a bracelet, where $x \in \mathbb{Z}_n$ is connected with $x + 1$ and $x - 1$ (computed in $\mathbb{Z}_n$). Bracelets can be rotated and reflected. The dihedral group D_{2n} contains two types of elements:

- r_i for $i \in \mathbb{Z}_n$, interpreted as a rotation of the bracelet by $\frac{2\pi i}{n}$,
- sr_i for $i \in \mathbb{Z}_n$, interpreted as a rotation of the bracelet by $\frac{2\pi i}{n}$ followed by a reflection.

This defines the following group action:

Definition 28. The dihedral group D_{2n} acts on $\mathbb{Z}_n$ with:

$$r_i \cdot x = i + x,$$
$$sr_i \cdot x = n - 1 - (i + x),$$

computed in $\mathbb{Z}_n$.

Definition 29. For $n \geq 1$, the *number of distinct colorings of a bracelet with n beads and m colors* is given by:

$$|[m]^{\mathbb{Z}_n}/D_{2n}|.$$

For $n = 0$, we define that there is a single coloring of a bracelet with 0 beads. This is defined separately since we do not have a group $D_{2\cdot 0}$. This definition is inspired by the fact that $Y^\emptyset$ contains exactly one function.

Proposition 30. *The number of distinct colorings of a bracelet can be computed using the* computeNumDistinctColorings *function.*

Proof. By Proposition 24. □

5.4 Cube

We interpret the elements of [6] as 6 faces of the cube as follows:

- 0 is the face at the front,
- 1 is the face at the right,
- 2 is the face at the back,

- 3 is the face at the left,
- 4 is the face at the top,
- 5 is the face at the bottom.

Definition 31. We define two fundamental rotations of the cube:

- $r = (0\ 1\ 2\ 3)$: A rotation of the cube by $\frac{\pi}{2}$ around the vertical axis passing through the centers of the top and bottom faces. The front face moves to the position of the right face.
- $s = (1\ 4\ 3\ 5)$: A rotation of the cube by $\frac{\pi}{2}$ around the horizontal axis passing through the centers of the front and back faces. The right face moves to the position of the top face.

The set of rotational symmetries of the cube is given by:

$$S = \{r^i \cdot s^j \mid i, j \in [4]\} \cup \{s^{2i+1} \cdot r \cdot s^j \mid i \in [2], j \in [4]\}.$$

The reasoning is as follows:

- First, we apply s at most three times to set the position of face 1.
- Then, we move face 0 to any other position using appropriate rotations. To move 0 to one of the faces in $\{0, 1, 2, 3\}$, we apply r the necessary number of times. To move 0 to 4 or 5, we first apply r once to move 0 to 1, then apply s either once or three times.

Since we can move 0 to any position and 1 to any position adjacent to the new position of 0 (by applying s an appropriate amount of times in the beginning), this results in $6 \times 4 = 24$ distinct rotational symmetries. Because the entire cube configuration is determined by the new positions of faces 0 and 1, we have all rotational symmetries of the cube.

We need to prove that S is a subgroup of S_6. While this can be proven with the *decide* tactic via brute force, Lean takes a long time to check such a proof. Therefore, we construct a more systematic proof.

Proposition 32. *Let M be a monoid. If $m \in M$ satisfies $m^n = 1$, then for any $i, j \in [n]$, we have:*

$$m^{(i+j) \bmod n} = m^{i+j}.$$

Proof. If $i + j < n$, the result follows immediately. Otherwise, since $n \leq i + j < 2n$, we have:

$$m^{i+j} = m^{i+j-n} \cdot m^n = m^{(i+j) \bmod n}.$$

□

Proposition 33. *For all $x \in S$, we have:*

$$r \cdot x \in S, \quad s \cdot x \in S.$$

Proof. For each $x \in S$, we verify that the result remains in S. □

Proposition 34. *For all $x \in S$ and $n, m, k \in \mathbb{N}$, we have:*

$$s^n \cdot r^m \cdot s^k \cdot x \in S.$$

Proof. By induction on k. If $k = 0$, we perform another induction on m. If also $m = 0$, we perform another induction on n. If also $n = 0$, then $1 \cdot 1 \cdot 1 \cdot x \in S$.
All inductive steps are proven in the same manner, using Proposition 33 to reduce an exponent by 1 and applying the inductive hypothesis. □

Proposition 35. *S is a subgroup of S_6.*

Proof.
- $x_1, x_2 \in S \implies x_1 \cdot x_2 = s^n \cdot r^m \cdot s^k \cdot x_1 \in S$
- $1 = r^0 \cdot s^0 \in S$
- $x \in S \implies x^{-1} = (s^n \cdot r^m \cdot s^k)^{-1} = (s^{-1})^k \cdot (r^{-1})^m \cdot (s^{-1})^n = s^{3k} \cdot r^{3m} \cdot s^{3n} \in S$

□

Definition 36. The *number of distinct colorings of a cube with m colors* is given by:

$$|[m]^{[6]}/S|.$$

Proposition 37. *The number of distinct colorings of a cube can be computed using the* computeNumDistinctColorings *function.*

Proof. By Proposition 24. □

5.5 Permutations

We interpret the elements of $[n]$ as n unordered, indistinguishable objects. The group S_n, consisting of all permutations of $[n]$, acts on $[n]$. Its elements permute our objects. Since we can permute the objects in any way and still get an equivalent configuration, two colorings are equivalent if and only if they color the same number of objects with each color. Thus, the number of distinct colorings of n unordered, indistinguishable objects with m colors is equal to the number of ways to separate n objects into m ordered sets (i.e., the number of weak compositions of n into m parts).

Definition 38. The number of distinct colorings of n *unordered, indistinguishable objects with m colors* is

$$|[m]^{[n]}/S_n|.$$

Definition 39. The number of weak compositions of n into m parts is:

$$\begin{cases} 1 & \text{if } n = m = 0, \\ 0 & \text{if } m = 0 \text{ and } n > 0, \\ \binom{n+m-1}{m-1} & \text{if } m > 0. \end{cases}$$

This is the number of ways to separate n objects into m ordered sets.

We now prove that the number of distinct colorings of n unordered, indistinguishable objects with m colors is equal to the number of weak compositions of n into m parts.

Definition 40. We define functions that contract and expand the domain and codomain of colorings:

- *contractCodomain*: Given a coloring $f : [n] \to [m + 1]$ and a proof that f does not map any element to m, this function returns f with codomain contracted to $[m]$.

- *expandCodomain*: Given a coloring $f : [n] \to [m]$, this function returns f with codomain expanded to $[m+1]$.
- *contractDomain*: Given a coloring $f : [n+1] \to [m]$, this function returns f with domain contracted to $[n]$.
- *expandDomain*: Given a coloring $f : [n] \to [m+1]$, this function returns f with domain expanded to $[n+1]$, where $f(n) = m$.

Proposition 41. *Let $\pi \in S_n$ such that $\pi(i) = n$ for some $i < n$. Then $\pi(\pi(i)) < n$.*

Proof. Assume, for a contradiction, that $\pi(\pi(i)) \geq n$. Then

$$\pi(\pi(i)) = n = \pi(i) \implies \pi(i) = i \implies i = n < n,$$

which is a contradiction. □

Definition 42. We define functions that contract and expand permutations:

- *permContract*: Contracts $\pi \in S_{n+1}$ by removing n from the domain and remapping $\pi^{-1}(n) \mapsto \pi(n)$, if $\pi^{-1}(n) \neq n$. The result is a permutation in S_n, whose inverse can be constructed by using the same procedure on π^{-1}.
- *permExpand*: Expands a permutation $\pi \in S_n$ by adding n to the domain and defining $\pi(n) = n$. The result is a permutation in S_{n+1}, whose inverse can be constructed by using the same procedure on π^{-1}.

Proposition 43. *A recurrence formula for the number of distinct colorings of $n+1$ unordered, indistinguishable objects with $m+1$ colors:*

$$|[m+1]^{[n+1]}/S_{n+1}| = |[m]^{[n+1]}/S_{n+1}| + |[m+1]^{[n]}/S_n|.$$

Proof. We construct a bijection

$$\varphi : \left([m]^{[n+1]}/S_{n+1}\right) \cup \left([m+1]^{[n]}/S_n\right) \to [m+1]^{[n+1]}/S_{n+1}.$$

The function φ is defined as follows:

- For $[f] \in [m]^{[n+1]}/S_{n+1}$, we set

  $$\varphi([f]) = [\mathit{expandCodomain}(f)].$$

  This is well-defined since if $f_1 = g \cdot f_2$, then

  $$\mathit{expandCodomain}(f_1) = g \cdot (\mathit{expandCodomain}(f_2)).$$

- For $[f] \in [m+1]^{[n]}/S_n$, we set

  $$\varphi([f]) = [\mathit{expandDomain}(f)].$$

  This is well-defined since if $f_1 = g \cdot f_2$, then

  $$\mathit{expandDomain}(f_1) = (\mathit{permExpand}(g)) \cdot (\mathit{expandDomain}(f_2)).$$

We now prove that φ is a bijection.
Injectivity: Suppose $\varphi([f_1]) = \varphi([f_2])$. Then either:

- no function in $\varphi([f_1]) = \varphi([f_2])$ maps to m, which implies

$$[f_1], [f_2] \in [m]^{[n+1]}/S_{n+1}.$$

In this case, we have

$$[expandCodomain(f_1)] = [expandCodomain(f_2)]$$

so

$$expandCodomain(f_1) = g \cdot (expandCodomain(f_2)).$$

This implies $f_1 = g \cdot f_2$, so $[f_1] = [f_2]$.

- some function in $\varphi([f_1]) = \varphi([f_2])$ maps to m, which implies

$$[f_1], [f_2] \in [m+1]^{[n]}/S_n.$$

In this case, we have

$$[expandDomain(f_1)] = [expandDomain(f_2)],$$

so

$$expandDomain(f_1) = g \cdot (expandDomain(f_2)).$$

This implies that

$$f_1(x) = ((permContract(g)) \cdot f_2)(x)$$

for all $x \in [n] \setminus \{g \cdot n\}$.
If $g \cdot n \neq n$, then we have

$$\begin{aligned} f_1(g \cdot n) &= expandDomain(f_1)(g \cdot n) \\ &= expandDomain(f_2)(n) \\ &= m \\ &= expandDomain(f_1)(n) \\ &= expandDomain(f_2)(g^{-1} \cdot n) \\ &= f_2(g^{-1} \cdot n) \\ &= ((permContract(g)) \cdot f_2)(g \cdot n). \end{aligned}$$

Thus, $[f_1] = [f_2]$.

Surjectivity: Take any $[f] \in [m+1]^{[n+1]}/S_{n+1}$. If f does not map any element to m, then

$$\varphi([contractCodomain(f)]) = [f].$$

Otherwise, there exists some i such that $f(i) = m$. Define

$$h = (i\ n) \cdot f,$$

where $(i\ n)$ is the transposition swapping i and n. Since $h(n) = m$, we have

$$\varphi([contractDomain(h)]) = [h] = [f].$$

□

Proposition 44. *The number of distinct colorings of n unordered, indistinguishable objects with m colors is equal to the number of weak compositions of n with m parts.*

Proof. We use induction on $m + n$.
If $m + n = 0$, then $n = m = 0$, and we have $|\emptyset^{\emptyset}/S_0| = 1$.
Otherwise we first check cases when $n = 0$ or $m = 0$ and see that the result holds.
If $n > 0$ and $m > 0$, applying Proposition 43 and the inductive hypothesis, we obtain

$$|[m]^{[n]}/S_n| = |[m-1]^{[n]}/S_n| + |[m]^{[n-1]}/S_n| = \binom{n+m-2}{m-2} + \binom{n+m-2}{m-1} = \binom{n+m-1}{m-1}.$$

□

6 Sum of Stirling numbers of the first kind

Definition 45. The `Stirling numbers of the first kind` count the number of permutations of a set of size n with exactly k cycles:

$$s(n,k) = |\{\pi \in S_n \mid c(\pi) = k\}|,$$

where $c(\pi)$ denotes the number of cycles in the permutation π.

We now derive a summation formula for Stirling numbers of the first kind using our previous results.

Proposition 46. *For any $n, m \in \mathbb{N}$ with $m > 0$, we have*

$$\sum_{k=0}^{n} s(n,k)m^k = n!\binom{n+m-1}{m-1}.$$

Additionally:

- *If $n = m = 0$, the sum evaluates to 1 in Lean, since $0^0 = 1$.*
- *If $n > 0$ and $m = 0$, the sum evaluates to 0.*

Proof. We apply *Pólya's enumeration theorem* (Proposition 8) and Proposition 44:

$$\sum_{k=0}^{n} s(n,k)m^k = |[m]^{[n]}/S_n| \cdot |S_n| = n!\binom{n+m-1}{m-1}.$$

□