Lecture 11: Burnside's Lemma, Fixed Point Set, Number Theory

Summary:
We examine fixed point sets and prove Burnside's lemma, applying it to count distinct colorings of objects under symmetries. We then introduce fundamental concepts of divisibility, including greatest common divisors and least common multiples, establishing the linear combination lemma for integers.

Topics Covered: Burnside's lemma, common divisor, common multiple, fixed point lemma for permutation action, fixed point set, greatest common divisor, least common multiple, linear combination lemma for integers

Fixed point set:

Let G be a group action on X and $g \in G$. Then, we have

$$X^g = \{x \in X.\ g(x) = x\}$$

X^g is just the set of all fixed points of g.

Burnside's Lemma:

Let G act on X with G and X finite. Then, we have

$$\text{number of orbits} = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Consider the collection of functions $f : X \to Y$ from X to some set of colors Y. We have a group action of G on this collection by

$$(gf)(x) = (f \circ g^{-1})(x)$$

Lemma:

Let G act on X, and Y is any other set with G, X, Y finite. Let $g \in G$. Let $c(g)$ be the number of cycles of G. Then, we have

$$|(Y^X)^g| = |Y|^{c(g)}$$

- Y^X is the set of functions $X \to Y$
- $(Y^X)^g$ is the set of functions fixed by g
- $c(g)$ is the number of disjoint cycles required to represent g as a product of disjoint cycles. Note that $g : X \to X$ is a bijective, so it is a permutation. $g \in \text{Sym}(X)$.

> The key insights here is that g can be expressed as a product of disjoint cycles. So,

G acts on Y^X naturally. We have

$$(gf)(x) = f(g^{-1}(x))$$

Above, we have

- $g : X \to X$
- $f : X \to Y$

We define it in the above way because, otherwise, the composition wouldn't work as desired in a group action.

Example:

Suppose we are interested in counting the number of necklaces with four beads up to rotation, where each bead is black or white. Number the beads 1, 2, 3, 4. We can think of ordered colorings of the beads as functions

$$f : [4] \to \{B, W\}^4$$

The group $G = \langle (1, 2, 3, 4) \rangle$ acts in the obvious way on $X = [4]$, so it also acts on the set of functions $f : [4] \to \{B, W\}^4$

Distinct colorings (up to rotation) correspond precisely to orbits of $\{B, W\}^4$ under this group action.

Thus, the number of distinct necklaces (up to rotation) is computed by Burnside's lemma:

$$\text{number of orbits} = \frac{1}{|G|} \sum_{g \in G} |(Y^X)^g|$$

$$\langle (1,2,3,4) \rangle = \{(1)(2)(3)(4), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$$

Compute the following quantities

g	$c(g)$	$\|(Y^X)^g\| = \|Y\|^{c(g)}$
$(1)(2)(3)(4)$	4	2^4
$(1,2,3,4)$	1	2^1
$(1,3)(2,4)$	2	2^2
$(1,4,3,2)$	1	2^1

For a permutation g with $c(g)$ cycles, there are $2^{c(g)}$ fixed points. This is because $|Y| = 2$.

Therefore, the number of orbits is

$$\text{number of orbits} = \frac{1}{4}(2^4 + 2^1 + 2^2 + 2^1) = 6$$

The orbits are

- `BBBB`
- `BBBW`
- `BBWW`
- `BWBW`
- `BWWW`
- `WWWW`

and their rotations.

Example:

Suppose we want to color the faces of a cube from a set of r colors. It has ^ faces, label them

- 1 - top
- 2 - front
- 3 - right
- 4 - back
- 5 - left
- 6 - bottom

Let us say colors of the faces are equivalent if they can be achieved by rotation. There are three types of rotations:

- About an axis perpendicular to opposite faces, with an angle of rotation in $\{0, 90, 180, 270\}$
- About an axis perpendicular to opposite edges, with angle of rotation in $\{0, 180\}$
- About an axis passing through opposite vertices, with an angle of rotation in $\{0, 120, 240\}$

Now, we want to know how many cycles are in each of these rotations. They are as follows:

Type of rotation	# of such elements in G	Example $g \in G$	$c(g)$	$\|(Y^X)^g\|$
Identity	1	$(1)(2)(3)(4)(5)(6)$	6	r^6

Type of rotation	# of such elements in G	Example $g \in G$	$c(g)$	$\|(Y^X)^g\|$
Face rotation $\pm$ 90	$3 \cdot 2$	$(1)(6)(2,3,4,5)$	3	r^3
Face rotation $\pm$ 180	$3 \cdot 1$	$(1)(6)(2,4)(3,5)$	4	r^4
Edge rotation $\pm$ 180	$6 \cdot 1$	$(1,4)(2,6)(3,5)$	3	r^3
Vertex rotation $\pm$ 120	$4 \cdot 2$	$(1,2,5)(3,6,4)$	2	r^2

By Burnside's lemma, we have
{

$$\text{number of distinct colorings} = \frac{1}{4}(r^6 + 6r^3 + 3r^4 + 6r^3 + 8r^2) = \frac{r^6 + 3r^4 + 12r^3 + 8r^2}{24}$$

Cryptography and number theory

Definition 5:

Let $a, b \in \mathbb{Z}$. Then, we have

1. If $c \mid a$ and $c \mid b$, then we say that c is a common divisor of a and b. Among all the common divisors of a, b, there is a largest one. We call this the greatest common divisor, and denote it $\gcd(a, b)$.
2. If $a \mid c$ and $b \mid c$, then we say that c is a common multiple of a and b. Among all the common multiples of a and b, there is a smallest one. We call this the least common multiple and denote it $\operatorname{lcm}(a, b)$.

Lemma:

Suppose that $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then

$$c \mid xa + yb$$

for any $x, y \in \mathbb{Z}$.

In particular,

$$\forall x, y \in \mathbb{Z}.\ \ \gcd(a, b) \mid xa + yb$$

Proof:

We have

$$c \mid a \implies a = qc, q \in \mathbb{Z}$$
$$c \mid b \implies b = q', c, q' \in \mathbb{Z}$$

Thus,

$$xa + yb = xqc + yq'c = c(xq + yq')$$

So, $c \mid xa + yb$ as claimed. Take $c = \gcd(a, b)$ to get the final claim.

$$\text{QED}$$