Lecture 5: Generating Functions and Group Actions

Combinatorial Methods (Winter 2023)
University of Toronto
Swastik Kopparty
Scribes: Augustine Bugler, Akira Takaki, Enrique Nunez Lon-wo

1 Generating Functions

What's a generating function? An example is the Fibonacci generating function. The Fibonacci numbers are defined as:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \end{aligned}$$

The idea of a generating function: Instead of studying specific elements of a sequence, study them all at once.

$$\left.\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \end{aligned}\right\} \longrightarrow f = \sum_{i=0}^{\infty} F_i x^i$$

A sequence, and a formal power series in $[[x]]$

You can think of it as a clothesline where you "hang" series.

$$f(x) = 0 \cdot x^0 + 1 \cdot x^1 + F_2 \cdot x^2 + \dots$$

The Fibonacci generating function.

How do you solve this? Look at the same series, but shifted:

$$\begin{aligned} F(x) &= 0x^0 + 1x^1 + F_2x^2 + \dots \\ xF(x) &= \quad 0x^1 + \quad 1x^2 + F_2x^3 + \dots \\ x^2F(x) &= \quad\quad\quad 0x^2 + \quad 1x^3 + F_2x^4 + \dots \end{aligned}$$

$$\begin{aligned} F(x) - x &= xF(x) + x^2F(x) \\ F(x)[1 - x - x^2] &= x \\ F(x) &= \frac{x}{1 - x - x^2} \end{aligned}$$

So what's the point of having done this? Recall that

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots$$

We can use partial fraction decomposition on $\frac{x}{1-x-x^2}$ to get

$$\frac{A}{\dots} + \frac{B}{\dots}$$

where A, B are the roots of $1 - x - x^2$.

After you get here, you can find the closed form of the sequence. This is an OGF (ordinary generating function). You can also get an exponential generating function:

$$\sum_k \frac{a_k}{k!}x^k$$

Take any set, then match it with a polynomial (like a generating function).

1.1 Weights

Suppose you have a weight function,

$$\text{wt} : S \to \mathbb{C}[[x]]$$

then we define

$$f_S(x) = \sum_{s \in S} \text{wt}(s)(x)$$

This works well with set operations. If $S \cap T = \emptyset$, $f_{S \sqcup T} = f_S + f_T$.

If wt functions are defined properly, we can also define multiplication, like

$$f_{S\times T} = f_S \cdot f_T \quad \text{and} \quad \mathrm{wt}(x,y) = \mathrm{wt}(x)\cdot \mathrm{wt}(y)$$

In combinatorics, we want to turn clever tricks into full blown theories and generalize into other problems. We will use this theory of weights to prove the binomial theorem.

Recall that the binomial theorem is:

$$\sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n$$

The traditional way of looking at the right side is

$$(1+x)\cdots(1+x)$$

Coefficient of x^k in the above is the number of ways of choosing k xs from here. This is the usual combinatorial proof of the equality.

Let $S = P([n])$. Define for $T \in S$, $\mathrm{wt}(T) = x^{|T|}$.

Then,

$$f_S = \sum_{k=0}^{n} \binom{n}{k} x^k$$

as there are $\binom{n}{k}$ such Ts of size k. Notice that $S \cong \{(1^{\varepsilon_1}, 2^{\varepsilon_2}, \ldots, n^{\varepsilon_n}) : \varepsilon_i \in \{0,1\}\} = V$. Here we use $\cong$ to mean there is a naturally defined bijection.

Define $\mathrm{wt}(1^{\varepsilon_1}, 2^{\varepsilon_2}, \ldots, n^{\varepsilon_n}) = x^{\sum \varepsilon_i}$. Note that this makes the natural bijection also a weight-preserving one, so $f_S = f_V$.

Note that $V = (1^0 \sqcup 1^1) \times (2^0 \sqcup 2^1) \times \cdots \times (n^0 \sqcup n^1)$. By the above properties, we see that

$$f_V = \prod_{i=1}^{n} f_{(i^0 \sqcup i^1)} = (1+x)^n$$

This proves the binomial theorem.

2 Towards Burnside's Lemma

Recall a group is a pair $(S, *)$, where

- $(a * b) * c = a * (b * c)$

- $a * e = e * a$
- $a * a^{-1} = e$

Examples:

- $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$
- $(\mathbb{Q} \setminus \{0\}, *)$
- $(\mathbb{Z}_n, +)$
- $(\mathbb{Z}_p \setminus \{0\}, *)$

We wish to prove the following.

Theorem 1. *(Lagrange's) For finite groups G, if $H \leq G$, then $|H| \mid |G|$.*

We will show that cosets partition G, and this will be enough. Recall that gH is a coset for $g \in G$. Look at $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Note $\{0, 2\} \leq \mathbb{Z}_4$. The cosets are

- $0 + \{0, 2\} = \{0, 2\}$
- $1 + \{0, 2\} = \{1, 3\}$
- $2 + \{0, 2\} = \{0, 2\}$
- $3 + \{0, 2\} = \{1, 3\}$

Now we can get into the proof.

Proof. Show cosets partition G. We do this by the following three observations.

1. $|gH| = |H|$
2. $gH \cap g'H = \emptyset \implies g \neq g'$

For (1), $gh = gh' \implies h = h'$. For (2),

$$\begin{aligned} x &\in gH \cap g'H \\ x &= gh_1 \\ &= g'h_2 \\ (g')^{-1}g &= h_2(h_1^{-1}) \in H \end{aligned}$$

Notice that $hH = H$ by closure for subgroups. Examples:

- $0 + \{0, 2\} = \{0, 2\}$
- $2 + \{0, 2\} = \{0, 2\}$

3. $gH = H \iff g \in H$

From here, since we have a partition that covers G, with each element of the cover having size H, it must be that $|H| \mid |G|$. □

Corollary 2. $gH = g'H \iff (g')^{-1}g \in H$.

3 Group Actions, Orbits, and Stabilizers

In this section we defined group actions, orbits and stabilizers, and considered various related theorems and applications.

Definition 3. *Let G be a group and X be a set. Then we define a group action to be a mapping $\phi : g \to \varphi_g$ that satisfies:*

$$e \to id_X \tag{1}$$

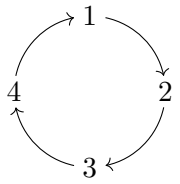
$$(gh) \to \varphi_g \circ \varphi_h = \varphi_{gh} \tag{2}$$

In this case, we say that "G acts on X", denoted $G \curvearrowright X$.

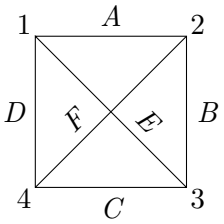
Definition 4. *The symmetric group of a finite set X is the set $S_X = \{f : X \to X\}$, where f is a bijection.*

Definition 5. *Let X be a set. The orbit of an element $x \in X$ is the set $O_x = \{g \cdot x : g \in G\}$, which corresponds to the set of rotations of x, or alternatively the set of elements which x can be mapped to by some element in G.*

Example 6. *Consider the set $X = \langle(1234)\rangle = \{(1)(2)(3)(4), (1234), (13)(24), (1432)\}$, which is a subset of S_4. Since S_4 acts on vertices, it acts on both the necklace $N = (1234)$ and the complete graph K_4, illustrated below.*



S_4 acts on the vertices of $N = (1234)$



For the graph K_4, we have that S_4 acts on the vertices as above. So (1234) *takes the edges to* $(ABCD)(EF)$.

This idea can be used to count graphs up to isomorphism. This is useful as it can be applied in areas such as enumeration theory.

Claim 7. *Suppose $G \curvearrowright O_x$. For any $a, b \in O_x$, we can get from a to b via the group action.*

Proof. Let $g, g', x \in G$ such that $g \cdot x = a$, $g' \cdot x = b$, where $\cdot$ is a group action.

$$\begin{aligned} & g \cdot x = a \\ \Rightarrow \quad & x = g^{-1} \cdot a \\ \Rightarrow \quad & b = g' \cdot (g^{-1} \cdot a) = (g' \cdot g^{-1}) \cdot a \\ \Rightarrow \quad & a = (g \cdot g'^{-1}) \cdot b \end{aligned}$$

Therefore there is an element of the form $(g \cdot g'^{-1})$ that maps a to b. □

Claim 8. *Let $X = \bigsqcup O_x$, over all $x \in X$. If $z \in O_x \cap O_y$, then $O_x = O_y$.*

Proof. Suppose $z \in O_x \cap O_y$.

$$\begin{aligned} z = g \cdot x = g' \cdot y \\ \Rightarrow x = (\ g^{-1} \cdot g')\ \cdot y \end{aligned}$$

So $O_x \subseteq O_y$ and similarly, $O_y \subseteq O_x$ □

Definition 9. *The stabilizer of a group element x (denoted $stab_x$ or G_x) is the set $G_x = \{g \in G : g \cdot x = x\}$. This is the set of elements in G under which x is invariant. Note that $\cdot$ denotes the group action.*

Claim 10. *The stabilizer $G_x \subseteq G$ is a subgroup.*

Theorem 11 (Orbit-Stabilizer)**.** *For any group G, we have that $|G_x| \cdot |O_x| = |G|$.*

Proof. By Legrange, $\frac{|G|}{|O_x|}$ is the number of cosets of G. So it is sufficient to find a bijection $G_X \to O_X$.

Claim: $gG_X \to g \cdot x$ is such a bijection.

We must check that it is well defined:

$$\begin{aligned} & gG_x = hG_x \\ \Leftrightarrow \quad & h^{-1}g \in G_x \\ \Leftrightarrow \quad & (h^{-1}g) \cdot x = x \\ \Leftrightarrow \quad & g \cdot x = h \cdot x \end{aligned}$$

Thus, our bijection is well defined and we have also shown invertibility. □

Definition 12. *Define the set $X^g = \{x \in X : g \cdot x = x\}$. This is the subset of X which is invariant under g.*

Theorem 13. *For any group G, we have that $\sum_{x \in X} |G_x| = \sum_{g \in G} |X^g|$.*

Proof. Suppose $|G| = m$ and $|X| = n$. Construct a matrix $A_{m \times n}$ with entries $a_{ij} = 1$ if $g_i \cdot x_j = x_j$ and 0 otherwise.

$$A_{m \times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Then, summing over the entries in the i^{th} row, we get the number of elements $x \in X$ such that $g_i \cdot x = x$, which is $|X^{g_i}|$. So summing again over each row, we get $\sum_{g \in G} |X^g|$.

Similarly, the summing over the entries in the j^{th} column, we get the number of elements $g \in G$ such that $g \cdot x_j = x_j$, which is equal to $|G_x|$. The sum over all columns will be $\sum_{x \in X} |G_x|$.

Each of these summations is equal to the sum over all elements in A_{ij}. Therefore, we conclude that $\sum_{x \in X} |G_x| = \sum_{g \in G} |X^g|$. □

Theorem 14. *Suppose $\mathbb{Z}_p \curvearrowright X$. Then $|X^g| \equiv |X| \mod p$.*

Proof. First, note that the orbits form a partition of X, so $|X| = \sum_{O_x \subseteq X} |O_x|$.

Since $|O_x| \mid |\mathbb{Z}_p|$, we see that $|O_x| = 1, p$. □

Lemma 15 (Bernside's)**.** *Suppose G is a group and X is a set such that $G \curvearrowright X$. Then # orbits $= \frac{1}{|G|} \sum_{g \in G} |X^g|$.*

Proof. Let G be a group, X a set such that $G \curvearrowright X$

$$\begin{aligned} \#\text{ orbits } &= \sum_{x \in X} \frac{1}{|O_x|} \\ &= \sum_{x \in X} \frac{|G_x|}{|G|} \\ &= \frac{1}{|G|} \sum_{x \in X} |G_x| \\ &= \frac{1}{|G|} \sum_{g \in G} |X^g| \end{aligned}$$

□

Note that since all necklaces under rotation considered equal, Bernside's lemma allows us to count necklaces.

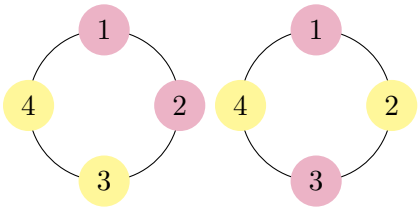
Lemma 16. *The group action $G \curvearrowright X$ induces $G \curvearrowright \{f : X \to Y\} = H$.*

Proof. Let $C(g)$ denote the number of cycles of g. Suppose $F \in H^g$ (ie. F is a fixed point). This is equivalent to F being constant on cycles.

$$\begin{aligned} \Rightarrow \quad (gF)(x) &= F(g^{-1}x) \\ &= F(x) \\ \Rightarrow \quad F(O_x) &= O_x \\ \Rightarrow \quad |H^g| &= |Y|^{C(g)} \end{aligned}$$

□

How can we count the number of necklaces with colouring up to rotation?



These necklaces are the same under the normal group action, but are not equivalent if we consider colouring

Instead of using $G \curvearrowright X$, we can use the induced action $G \curvearrowright \{F : G \to Y\}$, where $F : G \to$ maps each element to a colour in Y.

So to count the necklaces on $N = (1234)$ with colouring, we do the following:

$$\begin{aligned}\text{Number of orbits} &= \frac{1}{4}\sum_{g\in G}|X^g| \\ &= \frac{1}{4}\sum_{g\in G}|2^{C(g)}| \\ &= \frac{1}{4}(2^4 + 2^2 + 2 + 2) \\ &= 16\end{aligned}$$

Theorem 17 (Fermat's Little Theorem)**.** *If p is prime, $a^p \equiv a \mod p$.*

Proof. Choose $X = [p]$, $Y = [a]$ and define $H = \{f : X \to Y\}$. Since $\mathbb{Z}_p \curvearrowright X$, we know $\mathbb{Z}_p \curvearrowright H$.

$$\begin{aligned}\Rightarrow |H| &= a^p \\ &= |H| \\ &\equiv |H^g| \mod p \\ &\equiv |Y|^{C_g} \mod p \\ &\equiv a \mod p\end{aligned}$$

□

4 Wilson's Theorem

Wilson's Theorem is a theorem of number theory which says

Theorem 18. *If p is a positive prime then*

$$(p-1)! \equiv -1 \mod p$$

The first proof consists of a slick number theoretic argument involving polynomials and their roots.

Proof. Suppose that $a \in \{1, ..., p-1\}$ then $\gcd(a, p) = 1$ therefore by Fermat's little theorem $a^p \equiv a \mod p$. Since a is co-prime to p there exists an inverse mod p, therefore Fermat's little theorem becomes $a^{p-1} \equiv 1 \mod p$. The above tells us that a is a root of the polynomial $f(x) = x^{p-1} - 1 \in \mathbf{F}_p[x]$. Since $\mathbf{F}_p$ is a field we can use the division algorithm to show that $x - a | f(x)$. Thus

$$f(x) = \prod_{a \in \mathbf{F}_p / \{0\}} (x - a)$$

by a degree argument and the fact that $f(x)$ is monic. Setting $x = 0$ we find that $-1 \equiv (p-1)! \mod p$. □

Now we prove the same result using combinatorics.

Proof. We begin with the group of permutations on n letters S_n. We then act on S_n by the action $\sigma \cdot \phi = \sigma\phi\sigma^{-1}$. The following lemma helps us understand the action of conjugation on S_n.

Lemma 19. *(Basis Change) Suppose $\rho \in S_n$ such that $\rho = (ijk \dots n)$ then*

$$\sigma\rho\sigma^{-1} = (\sigma(i)\sigma(j)\sigma(k) \dots \sigma(n)).$$

Now let X be p-cycles in S_p and we have $G =< (123 \dots p) >$ acting on X. By the lemma (#?) above we find

$$|X| \equiv |X^g| \mod p$$

for all $g \in G$. We know that $|X| = p!/p$ since we can construct X by looking at $Y = \{f : [p] \to [p] | \text{f is an iso}\}$ which can be seen as orderings of $[p]$ and which has size $p!$. If we act G on Y in the natural way then we see that that two orderings give the same cycle if they are in the same orbit, but each orbit has size p. Now we look at the size of X^g, let $g \in G$ be a non-identity element then by the basis change lemma we see that the only elements of X which are stabilized by g are elements of $G \cap X = G - \{e\}$. Therefore, $|X^g| = p - 1$ which proves Wilson's Theorem. □

5 Pólya-Redfield Counting

Suppose that G acts on the set X and $|X| = n$ and that $g \in G$ then we define

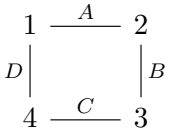
Definition 20. $z_g \in \mathbf{C}[[t_1, ..., t_n]]$ *as*

$$z_{g,X}(t_1, ..., t_n) = \prod_{j=1}^{n} t_j^{c_j(g)}$$

where $c_j(g)$ is the number of j-cycles in g relative to the action of G on X. We then define $z_{G,X} \in \mathbf{C}[[t_1, ..., t_n]]$ as

$$z_{G,X}(t_1, ..., t_n) = \sum_{g \in G} z_g(t_1, ..., t_n).$$

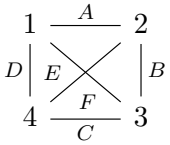
Example 21. *Let* $G =< (1234) >= \{e, (1234), (13)(24), (1432)\}$ *and we act on the following graph* X *in the natural way*



If we denote $\alpha = (1234)$ *then we find the elements of* G *have the following cycles* $e = (A)(B)(C)(D)$, $\alpha = (ABCD)$, $\alpha^2 = (AC)(BD)$ *and* $\alpha^3 = (ADCB)$. *This gives us the following polynomial*

$$Z_{G,X}(t_1, t_2, t_3, t_4) = t_1^4 + t_2^2 + 2t_4.$$

Suppose we instead acted on the graph X' *given by*



where $E = \{13\}$ *and* $F = \{24\}$. *We get the following cycles* $e = (A)(B)(C)(D)(E)(F)$, $\alpha = (ABCD)(EF)$, $\alpha^2 = (AC)(BD)(E)(F)$ *and* $\alpha^3 = (ADCB)(EF)$. *Thus we get the following polynomial*

$$Z_{G,X}(t_1, t_2, t_3, t_4) = t_1^6 + t_2^2 t_1^2 + 2t_4 t_2.$$

We want to use the polynomials we have defined to help us count the number isomorphism classes of graphs with n vertices. We can conceptualize graphs as subsets of $\binom{[n]}{2}$, so we bring our attention to the more general case. Suppose we had a group G acting on X then given $k \leq |X|$ we can produce an action on $\binom{X}{k}$ by defining $g \cdot \{x_1, x_2, \ldots, x_k\} = \{g \cdot x_1, g \cdot x_2, \ldots, g \cdot x_k\}$.

Lemma 22. *Suppose* $s \in \binom{X}{k}$ *and* $g \in G$ *with an action like above, then* $s \in \binom{X}{k}^g$ *if and only if* s *is the union of cycles of* g *as an action on* X.

Theorem 23. *Suppose that* S_n *acts on* $Y = \binom{[n]}{2}$ *as above. If* f_k *is the number of non-isomorphic graphs with* n *vertices and* k *edges then*

$$F_n(x) = \sum_{k=0}^{\binom{n}{2}} f_k x^k = \frac{1}{|G|} Z_{S_n,Y}(1 + x, 1 + x^2, \ldots, 1 + x^n)$$

Example 24. *Let us use this to count the number of non-isomorphic graphs with three vertices. We know* $\binom{[3]}{2} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$, *we'll call* $A = \{1, 2\}$ $B = \{1, 3\}$ *and* $C = \{2, 3\}$. *We find:*

$$\begin{aligned} e &= (A)(B)(C) & (12) &= (A)(BC) \\ (13) &= (B)(AC) & (23) &= (C)(AB) \\ (123) &= (ACB) & (132) &= (ABC). \end{aligned}$$

Therefore we have

$$Z_{S_3,Y}(t_1, t_2, t_3) = t_1^3 + 3t_1 t_2 + 2t_3$$

plugging in the monic polynomials in the theorem we get

$$\begin{aligned} Z_{S_3,Y}(1+x, 1+x^2, 1+x^3) &= (1+x)^3 + 3(1+x)(1+x^2) + 2(1+x^3) \\ &= x^3 + 3x^2 + 3x + 1 + 3(x^3 + x^2 + x + 1) + 2(x^3 + 1) \\ &= 6x^3 + 6x^2 + 6x + 6 \end{aligned}$$

and so $F_3(x) = x^3+x^2+x+1$. *Therefore the number of edges totally determines which isomorphism class you are in.*