Math 155 (Lecture 9)

September 21, 2011

In the last few lectures, we have discussed Joyal's theory of species. This is a convenient language for analyzing *labelled* counting problems: that is, for answering questions of the following form:

Proto-Question 1. In how many ways can we endow the set $\{1, \ldots, n\}$ with a particular structure?

A more specific example, which we have already discussed, is the following:

Question 2. How many graphs are there with vertex set $\{1, \ldots, n\}$?

The answer is $2^{\binom{n}{2}}$. A related, but much trickier question, is the following:

Question 3. Up to isomorphism, how many graphs are there with n vertices?

Questions 2 and 3 are related but have very different answers. To analyze Question 3, we can begin by thinking about the set S of all graphs with vertex set $\{1, \ldots, n\}$. This set is acted on by the symmetric group Σ_n consisting of all permutations of the set $\{1, \ldots, n\}$. Question 2 asks for the number of elements of S, while Question 3 asks for the number of elements in the quotient $G \backslash S$. This is an instance of the following more general sort of problem:

Proto-Question 4. Let X be a finite set and let G be a finite group acting on X. How many elements does the quotient set $G \backslash X$ have?

Before attempting to say something about this problem, let's briefly review some definitions. If G is a group and X is a set, then a (left) action of G on X is a map

$$G \times X \to X$$

$$(g, x) \mapsto gx$$

satisfying the identities

$$ex = x \qquad (gh)x = g(hx)$$

where e denotes the identity element of G. Given an action of G on X, we say that two elements $x, y \in X$ *lie in the same orbit* if $x = gy$ for some $g \in G$. This is an equivalence relation:

- Reflexivity: for each $x \in X$, we have $ex = x$, so that x is in the same orbit as itself.

- Symmetry: if x is in the same orbit as y, then $x = gy$, so that

$$g^{-1}x = g^{-1}(gy) = (g^{-1}g)y = ey = y$$

  shows that y is in the same orbit as x.

- Transitivity: assume that x is in the same orbit as y an that y is in the same orbit as z. Then $x = gy$ and $y = hz$ for some $g, h \in G$. Then $x = gy = g(hz) = (gh)z$, so that x and z lie in the same orbit.

We refer to the equivalence classes of X (under this equivalence relation) as the *orbits* of X, and denote the set of orbits by $G \backslash X$.

Definition 5. Let G be a group, let X be a G-set, and let $g \in G$ be an element. We will say that an element $x \in X$ is *fixed by* g if $gx = x$. We let $X^g = \{x \in X : gx = x\}$ denote the set of elements of X which are fixed by g. If x is fixed by g, we will also say that g *stabilizes* x. We let $\text{Stab}(x) = \{g \in G : gx = x\}$ denote the set of elements of G which stabilize x. This is a subgroup of G, called the *stabilizer* of x.

Definition 6. Let G be a group. A *G-set* is a set X equipped with a left action of G. We say that a G-set is *transitive* if it has exactly one orbit: that is, if the quotient $G \backslash X$ has a single element.

Example 7. Let G be a group and let $H \subseteq G$ be a subgroup. Let G/H denote the set of right cosets for H in G (equivalently, G/H is the set of orbits for the *right* action of H on G via right multiplication). Then G/H is equipped with a left action of G, given

$$g(g'H) = (gg')H.$$

In particular, every coset gH can be obtained by acting on the identity coset $eH = H$ by the element $g \in G$. It follows that G/H is a transitive G-set.

Example 7 has a converse. To see this, let X be an arbitrary transitive G-set. Choose an element $x \in X$ and let $H = \text{Stab}(x)$. We define a map

$$\rho : G \to X$$

by the formula $g \mapsto gx$. Note that if $h \in H$, then $hx = x$ so that

$$(gh)x = g(hx) = gx.$$

It follows that $\rho(g)$ depends only on the right coset gH to which g belongs, so that ρ factors as a composition

$$G \to G/H \xrightarrow{\rho'} X.$$

The map ρ' is given by $\rho'(gH) = gx$. Since X has only one orbit, every element of X has the form gx for some $g \in G$. This shows that ρ' is surjective. To prove injectivity, we note that if $gx = g'x$ for $g, g' \in G$, then

$$x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}(g'x) = (g^{-1}g')x$$

so that $g^{-1}g' \in H$ and therefore $gH = g'H$. We have proven:

Proposition 8. *Every transitive G-set X is isomorphic to G/H, for some subgroup $H \subseteq G$.*

Warning 9. The subgroup H appearing in Proposition 8 is not unique: it depends on a choice of element $x \in X$. Choosing a different element $y \in X$ gives an isomorphism $X \simeq G/H'$, where H' is the stabilizer of y. Since X is a transitive G-set, we can write $y = gx$ for some $g \in G$. Then $g'y = y$ if and only if $g'gx = gx$ if and only if $g^{-1}g'gx = x$. It follows that $H = g^{-1}H'g$.

We can summarize the situation as follows: there is a one-to-one correspondence between isomorphism classes of transitive G-sets and conjugacy classes of subgroups of G.

Proposition 8 gives a clear picture of the structure of any G-set X. We can always write X as a disjoint union of orbits, each of which looks like a set of right cosets of G. We therefore obtain the following:

Corollary 10. *Let G be a group and let X be a G-set. Then there exists a collection of subgroups $\{H_i\}_{i \in I}$, indexed by the set of orbits $I = G \backslash X$, and a bijection of G-sets*

$$X \simeq \coprod_{i \in I} G/H_i.$$

Let's now return to Proto-Question 4. We have the following basic identity:

Theorem 11 (Burnside's Formula)**.** *Let G be a finite group and let X be a finite G-set. Then*

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

Example 12. If X is a G-set, we say that the action of G is *free* if $\operatorname{Stab}(x) = \{e\}$ for each $x \in X$. In this case, the fixed sets X^g are empty unless $g = e$, in which case $X^g = x$. Burnside's formula therefore reduces to

$$|G\backslash X| = \frac{|X|}{|G|}.$$

Example 13. Let G act trivially on a set X: that is, so that $gx = x$ for all $g \in G$, $x \in X$. Then $X^g = X$ for all $g \in G$, so that $\sum_{g \in G} |X^g| = |G| \, |X|$. Burnside's formula then reads

$$|G\backslash X| = \frac{1}{|G|} |G| \, |X| = |X|.$$

Let us now prove Burnside's formula. Using Proposition 8, we can reduce to the case where X has the form G/H, for some subgroup G/H. For each $g \in G$, we have

$$X^g = \{g'H \in G/H : gg'H = g'H\} = \{g'H \in G/H : g'^{-1}gg' \in H\}.$$

We therefore have

$$|X^g| = \frac{|\{g' \in G : g'^{-1}gg' \in H\}|}{|H|}.$$

It follows that $\sum_{g \in G} |X^g|$ is given by

$$\frac{1}{|H|} |\{(g, g') \in G^2 : g'^{-1}gg' \in H\}| \quad = \quad \frac{1}{|H|} |\{(g, g') \in G^2 : g \in g'Hg'^{-1}\}|$$

$$= \quad \frac{1}{|H|} \sum_{g' \in G} |g'Hg'^{-1}|.$$

Each of the sets $g'Hg'^{-1}$ has cardinality $|H|$, and we are adding up $|G|$ of them. It follows that $\sum_{g \in G} |X^g| = \frac{1}{|H|} |G| \, |H| = |G|$ so that

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

as desired.

Remark 14. Though the proof of Burnside's formula is not difficult, it can be surprisingly useful. We should emphasize that the left hand side and the right hand side have very different natures: one measures the size of $G\backslash X$, which is a *quotient* of the set X, and the other involves the sizes of the sets X^g, which are *subsets* of X. It is often the case that the latter sets are much easier to count than the former.

Let us now give a classic application of Burnside's formula.

Question 15. Let G be a finite group acting on a set X, and let T be a finite set. How many G-orbits are there on the set T^X? In other words, how many ways can we color the set X using a set of colors T, up to symmetry (where the symmetries are given by G)?

Let's apply Burnside's formula to this problem. We have

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

Fix an element $g \in G$. We will say that two elements $x, y \in X$ *lie in the same g-orbit* if $x = g^k y$ for some $k \in \mathbf{Z}$. Note that coloring $X \to T$ is fixed by the element g if and only if is constant on each g-orbit. If we let $t = |T|$ and $o(g)$ denote the number of g-orbits on X, then the number of such colorings is given by $t^{o(g)}$. We have proven:

Theorem 16 (Polya's Enumeration Theorem). *Let G be a finite group acting on a set X, let T be a finite set with t elements. Then*

$$|G\backslash T^X| = \frac{1}{|G|} \sum_{g \in G} t^{o(g)}.$$

In particular, the left hand side is a polynomial function of t, having degree $\leq |X|$.