**CS 2800: Discrete Math** Oct. 12, 2011?

# Lecture

*Lecturer: John Hopcroft* *Scribe: Yipu, Eunsol & June*

## Proof Style

Correct ideas do not guarantee solid proofs. Part of math and cs is learning how to communicate and structure arguments. To show why picking up these skills is important, consider the following problem from Assignment 6:

*If for a given $a$ there exists $x$ such that $ax \equiv 1 \pmod{m}$, are $a$ and $m$ necessarily relatively prime? Prove why or why not.*

Here is a poorly written proof:
Yes, the condition implies $a$ and $m$ are relatively prime.

*Proof.*

$$\begin{aligned} a^{-1}a \equiv a^{-1}bc &\equiv 1 \pmod{m} \\ \implies a^{-1}bc &= ebd + 1 \\ \implies b(a^{-1}c - ed) &= 1 \end{aligned}$$

□

The proof contains most of right ideas for a proof, but is completely unreadable for the following reasons:

- Variables are introduced with little rhyme or reason. It's not clear what $b$, $c$, $d$, $e$ are. The presence of a equals sign suggests that they are numbers, but what kind of numbers they are is still left in doubt. Whenever you use variables that are not specified in the problem itself, you have to clearly define them.
- Transition from one equation to another should be obvious. If it is not obvious, there should be explanations. Here equations do not clearly follow from previous equations. In particular, it's unclear how the second line follows from the first.
- It's not clear why the last equation proves that $a$ and $m$ are relatively prime.

Solution readers are not mind readers or codebreakers. All variables should be clearly defined and all steps should be justified. The following proof is closer to what we are looking for:

*Proof.* The proof is by contradiction. Assume that $a$ and $m$ are not relatively prime. Let $b = \gcd(a, m) > 1$. Then there exist $c, d \in \mathbb{N}$ such that $a = bc$ and $m = bd$. Hence $a^{-1}bc \equiv a^{-1}a \equiv 1 \pmod{m}$, so we can write $a^{-1}bc = em + 1$ for some $e \in \mathbb{N}$. Thus

$$\begin{aligned} a^{-1}bc &= ebd + 1 \\ \implies b(a^{-1}c - ed) &= 1 \end{aligned}$$

The left hand side of the above equation is divisible by $b$, but the right hand side is not, since $b > 1$. This is our desired contradiction, thus $a$ and $m$ must be relatively prime. □

# Balls and Buckets

Suppose we have $n$ balls and $k$ buckets. How many ways can be put the balls into the buckets?

The answer depends on whether or not the *balls* or *buckets* are distinguishable. For example, suppose $k = 2$, $n = 3$. When the buckets are distinguishable, then putting 3 balls in the first bucket is different from putting 3 balls in the second bucket. When balls are distinguishable, putting 1st ball in the first bucket is different from putting 2nd ball in the first bucket. You have decide whether balls are distinguishable, and whether buckets are distinguishable before start solving problems.

## Distinguishable balls and buckets

Each of the $k$ balls has $n$ different buckets in which it can be put. Thus there are $n^k$ ways to put the balls in the buckets.

## Indistinguishable balls and distinguishable buckets

(For clarity in the next section, refer to your notes for pictures.)

If we place the balls in a line, then we can count the number of ways of putting the balls into the buckets by counting the number of ways of inserting $n - 1$ partitions in the line and then putting the balls between the $(i - 1)$th and $i$th partition in the $i$th bucket. Note that we can choose a position for a partition twice: this just corresponds to a bucket not getting any balls. There are

$$\underbrace{n}_{\#\text{ of balls}} + \underbrace{k-1}_{\#\text{ of partitions}}$$

places to put the partitions, so the number of ways to insert the partitions is

$$\binom{n+k-1}{k-1} = \binom{n+k-1}{n}$$

## Indistinguishable buckets

Whether or not the balls are distinguishable, the calculations for this case involve Pólya's enumeration theorem, which is beyond the scope of this course.

# Tic-tac-toe

We'd like to count the number of possible tic-tac-toe boards. For simplicity, first consider the case where only the first move has been made, so that there is a single × on the board. As there are nine possible places, one may conclude that there are 9 possible positions for this first move. However, by symmetry, there are only 3 positions that are not equivalent: one in a corner, on an edge, or in the center. This is because when the board is rotated, corner spaces stay in the corner, so all corner spaces are equivalent move.

From the preceding discussion, we know that there are 3 possible tic-tac-toe boards that contain a single ×. In other words, the boards with one × come in 3 equivalence classes. Now lift the restriction that the boards must contain a single × and nothing else. How many equivalence classes are there?

*Finding the number of Symmetries*

We saw earlier that equivalence classes have multiple elements because of symmetry, so let's first find all of the symmetries of the tic-tac-toe board. Each symmetry is a permutation of the set of all possible boards. Symmetries consist of rotations and flips. The set of rotations is

$$\{I, r, r^2, r^3\}$$

where $r^i$ is a $90 \cdot i°$ counterclockwise rotation. We don't include $r^i$ for $i > 3$ because $r^4 = I$. Flips can be about the horizontal axis, the diagonal connecting the top right and lower left corners, the vertical axis, or the diagonal connecting the top left and lower right corners. If we denote these flips by $f_0$, $f_1$, $f_2$, and $f_3$, then the set of all symmetries is

$$D := \{I, r, r^2, r^3, f_0, f_1, f_2, f_3\}$$

Alternatively, each flip is the same as a horizontal reflection combined with a rotation, so if we call a horizontal reflection $f$, then the set of all symmetries can be written as

$$D = \{I, r, r^2, r^3, f, fr, fr^2, fr^3\}$$

You have to be careful to include identity when counting symmetries.

## Groups

**Definition 1** (Group)**.** *Consider a set $G$, and let $\cdot : G \times G \to G$ be a binary operation on $G$. By definition, a group $(G, \cdot)$ has the following properties, known as the group axioms:*

1. *(Closure) If $a, b \in G$, then $a \cdot b \in G$.*
2. *(Associativity) For all $a, b, c \in G$,*
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
3. *(Identity element) There exists an element $e \in S$ such that for all $a \in S$,*
$$a \cdot e = e \cdot a = a$$
4. *(Inverse element) For all $a \in S$, there exists $a^{-1} \in S$ such that*
$$a^{-1} \cdot a = e$$

You can check that the set $D$ of all symmetries of a tic-tac-toe board satisfies the four group axioms if for $a, b \in D$ we define $a \cdot b := a \circ b$ to be the composition of the symmetries $a$ and $b$. Thus $D$ is a group. In fact, this group has a name: it's called the dihedral group $D_8$.

In general, the group operation $\cdot$ need not be commutative. For example, you can check that $f \cdot r \neq r \cdot f$.

## Burnside's Theorem

**Theorem 2** (Burnside's lemma, Burnside's counting theorem, Cauchy-Frobenius theorem, orbit-counting theorem)**.** *The number of equivalence classes into which a set $S$ is partitioned by the equivalence relation, induced by a permutation group $G$, is given by*

$$\frac{1}{|G|} \sum_{\pi \in G} \phi(\pi),$$

*where $\phi(\pi)$ is the number of elements of $S$ that are left invariant by the permutation $\pi$.*

*Example* For an example of what these variables represent, consider the $2x2$ board filled with $X$'s and $O$'s. If we consider boards to only be equivalent under rotation, then $G = \{I, r, r^2, r^3\}$ and $|G| = 4$. Now, let us consider $\pi = r$, how many boards are invariant under rotation? By invariant, we mean that after rotating the board it looks exactly the same. The only invariant boards are:

| X | X |
|---|---|
| X | X |

| O | O |
|---|---|
| O | O |

.

Hence, $\phi(\pi) = 2$. A trick to realizing there are only 2, is to figure out, if you have an X in a certain spot, which other spots on the board must also have an X in order to be invariant.

Similarly, the boards invariant under $\pi = r^2$ are:

$$\begin{array}{c|c} \text{X} & \text{X} \\ \hline \text{X} & \text{X} \end{array} \qquad \begin{array}{c|c} \text{X} & \text{O} \\ \hline \text{O} & \text{X} \end{array} \qquad \begin{array}{c|c} \text{O} & \text{X} \\ \hline \text{X} & \text{O} \end{array} \qquad \begin{array}{c|c} \text{O} & \text{O} \\ \hline \text{O} & \text{O} \end{array}.$$

Similarly, the boards invariant under $\pi = r^3$ are:

$$\begin{array}{c|c} \text{X} & \text{X} \\ \hline \text{X} & \text{X} \end{array} \qquad\qquad \begin{array}{c|c} \text{O} & \text{O} \\ \hline \text{O} & \text{O} \end{array}.$$

To finish off the example, the number of equivalence classes is:

$$\begin{aligned} &= \frac{1}{4}(2^4 + 2 + 4 + 2) \\ &= 6 \end{aligned}$$

Now let $S$ be the set of all possible tic-tac-toe boards. Since every symmetry is a permutation on $S$, the set of symmetries $D$ is a permutation group. Thus we can let $G$ be the set of symmetries of the tic-tac-toe board and apply the above theorem to find the number of equivalence classes of tic-tac-toe boards.