MATH/COMP61-03 Spring 2014 Notes: January 30th

Andrew Winslow

1 A Nice Conjecture

Last lecture someone in the audience gave the following conjecture:

Conjecture. *Let A and B be sets. If $A - B = B - A$, then $A = B$.*

I sort of danced around it, some people seemed to have an intuition that it was true. I would not expect people to necessarily be able to come up with a proof of this conjecture on a homework or test, but here is a proof for fun, starting with a preliminary theorem we call a *lemma*[1]:

Lemma. *Let A and B be sets. If $A - B = B - A$, then $A - B = B - A = \{\}$.*

Proof. *Let A and B be sets with $A - B = B - A$. Since every element in $B - A$ is an element of B, $B - A \subseteq B$. So $A - B = B - A \subseteq B$. Since $A - B \subseteq B$, every element $x \in A - B$ is also in B. But by definition of set difference, every element $x \in A - B$ is not in B. So there must be no elements in $A - B$, and $A - B = B - A = \{\}$.* □

The lemma is kind of interesting on its own. Now we prove the conjecture, recalling the lemma in the proof:

Theorem. *Let A and B be sets. If $A - B = B - A$, then $A = B$.*

Proof. *Let A and B be sets with $A - B = B - A$. Then by the previous lemma, $A - B = B - A = \{\}$. Let $x \in A$. Since $A - B = \{\}$, x must also be in B. So $x \in A \Rightarrow x \in B$ and so $A \subseteq B$. Now let $x \in B$. Since $B - A = \{\}$, x must also be in A. So $x \in B \Rightarrow x \in B$ and so $B \subseteq A$. So $A = B$.* □

A nice ~~conjecture~~ theorem.

2 Cartesian Product

In the last lecture we introduced *lists* or *k-tuples*, ordered collections of elements (allowing repeats). We now introduce an idea combining lists and sets:

[1] A *lemma* is just a helpful theorem. Calling a statement a *lemma* rather than a *theorem* is just a literary device to communicate that it will be used later.

Definition. *The* Cartesian product *of two sets A and B, written $A \times B$, is* $\{(x, y) : x \in A, y \in B\}$

Notice that the Cartesian product of two sets is another set, but with elements that are ordered pairs of objects in A and B. This makes the Cartesian product different than other set operators like union, intersection, etc. Moreover, the Cartesian product does not obey basic rules like commutativity and associativity found in some other set operators.

The Cartesian product will come in later lectures, but we observe here that if each set denotes options for a choice, then the Cartesian product is the set of all sequences of choices. In other words, the Multiplication Rule for $k = 2$ sets can be proved using the following theorem on Cartesian products:

Theorem. *Let A and B be two finite sets. Then $|A \times B| = |A| \times |B|$.*

3 Relations

Today we consider *relations*, which are meant to be an generalization of relationships between objects, such as $=$, $\geq$, $\leq$, and $\subseteq$. Relations describe relationships between elements of a single set, e.g. $\geq$ is defined on $\mathbb{Z}$, but can also be describe relationships between elements of two different sets, e.g. "has absolute value" is defined on $\mathbb{Z}$ and $\mathbb{N}$.

Let's consider the case of a single set first, as it is more common. Relations are defined by a set of pairs (lists of length 2) that specify which pairs of elements are related. For instance, $\geq$ can be described as a relation on the set $\mathbb{Z}$ containing the pair $(4, 0)$ (since $4 \geq 0$) but not $(2, 3)$ (since $2 \not\geq 3$). Formally, a relation on a set A is just a subset of the Cartesian product of A:

Definition. *A* relation *on a set A is a set $R \subseteq A \times A$.*

Similarly, a relation between sets A and B is a subset of $A \times B$, i.e. a set of pairs (a, b), where $a \in A$ and $b \in B$. If two elements $a \in A$ and $b \in B$ are related by a relation R, we write aRb, even though R is actually a set of ordered pairs. We also define the *inverse* of a relation R, the set of ordered pairs obtained by swapping the elements in the ordered pairs of R:

Definition. *The* inverse *of a relation R on a set A, written R^{-1}, is* $\{(b, a) \in A \times A : (a, b) \in R\}$.

This comes up with related relations, like $\geq$ and $\leq$, that are sometimes inverses of each other. In the study of relations, there are several properties that relations can have that are useful to name. This gives us some options to talk about how different relations are similar. Here are some good ones:

1. A relation R on a set A is *reflexive* provided $\forall a \in A, (a, a) \in R$.
2. A relation R on a set A is *irreflexive* provided $\forall a \in A \Rightarrow (a, a) \notin R$.

3. A relation R on a set A is *symmetric* provided $\forall a, b \in A, (a, b) \wedge a \neq b \Rightarrow (b, a) \in R$.

4. A relation R on a set A is *antisymmetric* provided $\forall a, b \in A, (a, b) \in R \wedge a \neq b \Rightarrow (b, a) \notin R$.

5. A relation R on a set A is *transitive* provided $\forall a, b, c \in A, (a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$.

Some of these properties you've seen before. The operator $=$ for pretty much any set you can think of is reflexive (wouldn't it be weird of $x \neq x$?) A relation R is symmetric if swapping the elements on both sides preserves the relationship (aRb iff bRa), not found in $\geq$, $\leq$, or other operators that suggest an ordering on the elements of the set. Transitivity is found in many common algebraic operators, but not in relations like "have difference at most 5", since $|5 - 0| \leq 5$ and $|-5 - 0| \leq 5$, but $|5 - -5| \not\leq 5$. Antisymmetry is found in $\leq$, $<$, and other operators that suggest an ordering.

But be careful! A relation can be neither reflexive nor irreflexive, and can also be both symmetric and antisymmetric. The relation $R = \{(1, 1), (2, 2)\}$ on the set $A = \{1, 2, 3\}$ is not reflexive ($(3, 3) \notin R$), not irreflexive ($(1, 1) \in R$), symmetric (vacuously true since no $(a, b) \in R$ with $a \neq b$ exists), and antisymmetric (also vacuously true). The takeaway is just that the properties aren't really opposites, even though they sound complementary in English.

Let's do an example for determining whether some rando relation on a set has any or all of these five properties. Let $R = \{(1, 1), (1, 2), (2, 1), (3, 4), (4, 3)\}$ be a relation on the set $A = \{1, 2, 3, 4, 5\}$. Now check the various properties:

1. R is not reflexive, since $(2, 2) \notin R$.

2. R is symmetric, since $(1, 2)$ and $(2, 1)$ are in R, as are $(3, 4)$ and $(4, 3)$. (Why does the definition not require $a \neq b$?)

3. R is not transitive, since $(3, 4)$ and $(4, 3)$ are in R, but $(3, 3)$ is not.

4. R is not antisymmetric, since $(1, 2)$ and $(2, 1)$ are in R, and $1 \neq 2$.

5. R is not irreflexive, since $(1, 1) \in R$.

Ok, not so bad, just needs some care. As an aside, the book defines *antisymmetry* as $(a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$. Why is this equivalent to the definition here? Consider the following theorem (about Boolean algebra!):

Theorem. $(p \wedge q) \rightarrow r = (p \wedge \neg r) \rightarrow \neg q$

Proof. *We give the proof as a series of equalities:*

$$
\begin{aligned}
(p \wedge q) \to r &= (\neg(p \wedge q)) \vee r && \text{by previous notes} \\
&= (\neg p \vee \neg q) \vee r && \text{by DeMorgan's} \\
&= \neg p \vee (\neg q \vee r) && \text{by associativity} \\
&= \neg p \vee (r \vee \neg q) && \text{by commutativity} \\
&= (\neg p \vee r) \vee \neg q && \text{by associativity} \\
&= \neg(p \wedge \neg r) \vee \neg q && \text{by DeMorgan's} \\
&= (p \wedge \neg r) \to \neg q && \text{by previous notes}
\end{aligned}
$$

So the two expressions are equal by the transitivity of equality. □

Now notice that if $A =$ "$(a, b) \in R$", $B =$ "$(b, a) \in R$", and $C =$ "$a = b$", then the book's definition is $A \wedge B \Rightarrow C$ and our definition is $A \wedge \neg C \Rightarrow \neg B$. Then by the previous theorem, these definitions are equal.

4 Equivalence Relations

In some cases, people look for a relation on weird objects that behaves like a familar relation on more standard object. The most common situation is trying to define a relation that behaves like $=$. What relation properties does $=$ on, say, $\mathbb{Z}$ have? The relation $=$ is reflexive, since $a = a$ for all $a \in \mathbb{Z}$, symmetric, since $a = b \Rightarrow b = a$ for any $a, b \in \mathbb{Z}$, and transitive, since $a = b \wedge b = c \Rightarrow a = c$ for any $a, b, c \in \mathbb{Z}$. On the other hand, $=$ is not irreflexive or antisymmetric.

If you consider other objects on which $=$ is defined (other types of numbers, sets, matrices, lists, etc.), they are all reflexive, symmetric, and transitive. Any relation with this trio of properties really behaves a lot like $=$ does, and we call any such relation an *equivalence relation*:

Definition. *A relation R on a set A is an* equivalence relation *provided R is reflexive, symmetric, and transitive.*

Consider evenness on the integers, e.g. 2 and 6 have the same evenness (they are even), as do 3 and 5 (they are not even), while 2 and 7 do not (one is even and the other is not). Evenness is clearly reflexive (any number has the same evenness as itself), symmetric (a has the same evenness as b implies b has the same evenness as a), and transitive (a has the same evenness as b and b has the same evenness as c implies a and c has the same evenness). Evenness then works like equality, but rather than integers where each $a \in \mathbb{Z}$ is on its own (no two are equal), evenness puts all the integers in two piles: integers that are even and integers that are not. These piles split up or partition the integers, and we'll talk about these tiles later. For right now, the takeaway is that equivalence relations look like equality, but possibly permitting many objects in the set to be *equivalent* to each other.

A very common example of an equivalence relation with applications across math and computer science is congruence mod n, where n is some natural number:

Definition. *For any $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ are* congruent mod n*, written $a \equiv b \bmod n$, provided $n | a - b$.*

It is uncommon to see the situations $n = 0$ or $n = 1$ (Why?) On the other hand, congruence mod 2 should look familar – it is evenness! Congruence mod n is an equivalence relation for any $n \geq 1$. Let's prove this:

Theorem. *For any $n \in \mathbb{N}$, congruence mod n is an an equivalence relation on $\mathbb{Z}$.*

Proof. *Let $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \bmod n\}$. For any $a \in \mathbb{Z}$, $a - a = 0 = 0 \times n$, so $n \mid a - a$. So $(a, a) \in R$ and so R is reflexive.*

For any $(a, b) \in R$ with $a \neq b$, $n \mid a - b$. So there exists a $c \in \mathbb{Z}$ such that $cn = a - b$. So $-cn = b - a$. So $n \mid b - a$ and $(b, a) \in R$. So $(a, b) \in R \Rightarrow (b, a) \in R$. So R is symmetric.

Now let $(a, b) \in R$ and $(b, c) \in R$. So $n \mid a - b$ and $n \mid b - c$. So there exists $c, d \in \mathbb{Z}$ such that $cn = a - b$ and $dn = b - c$. So $(c + d)n = cn + dn = a - b + b - c = a - c$. So $n \mid a - c$ and so $(a, c) \in R$. So $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$. So R is transitive.

In conclusion, R is reflexive, symmetric, and transitive. So R is an equivalence relation. □

5 Partial Orders: A Use for Relations

In lecture, I challenged someone to give a definition of $\geq$ that wasn't based on relations to give some motivation for defining and studying relations. As a response, I got a very nice one using subtraction and sets, and so lost my motivation for why we care about general relations and their properties. I mean, $\geq$ and $>$ are both antisymmetric and $=$ and congruence mod n are both reflexive, but how much can be done with knowing this?

Imagine you had a whole bunch of teams (sports? or could be something else), and these teams have various levels of skill. Then an interesting relation would be "has won against" on the set of teams. So the pair $(\text{Team } 7, \text{Team } 4)$ showing up in the relation means "Team 7 has won against Team 4."

Some properties are easy to determine, like reflexiveness (no), irreflexiveness (yes). Symmetry is possible, but only teams always trade wins when they play. Antisymmetry is also possible if the teams are consistent and always either win or lose when they play the same team. But something in the middle is more likely (some teams dominate others, some trade wins).

And transitivity? Suppose all teams are forced to play each other. Then if Team 1 beats Team 2, Team 2 beats Team 3, and Team 3 beats Team 1 every time they play then no transitivity ($(\text{Team } 1, \text{Team } 2)$ and $(\text{Team } 2, \text{Team } 3)$, but no $(\text{Team } 1, \text{Team } 3)$). But if teams all play each other and can be ranked, and win against all lower-ranked teams and lose against higher-ranked teams, then transitivity comes back.

Imagine I don't tell you exactly what teams played each other or won/lost, but only that "has won against" is transitive. Then it turns out there's always a way to assign team rankings such that any game between two teams has the high-ranked team winning. This assignment is called a *(strict) partial order* and is guaranteed to exist only from knowing "has won against" is transitive (and irreflexive). Kind of nice (go team transitivity).

6 Partitions

We finish by considering a side effect of equivalence relations: they separate elements of the set into groups (called *partitions*) that are all related to each other.

Definition. *A* partition *of a set A is a set of pairwise-disjoint non-empty subsets of A whose union equals A.*

The set $A = \{1, 2, 3, 4, 5\}$ has a partition $\{\{1, 5\}, \{2\}, \{3, 4\}\}$, a partition $\{\{1, 2, 3, 4\}, \{5\}\}$, a partition $\{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$, etc. (How many are there? Not an easy question.) A partition is just a way to split A into parts, with each element of A going into exactly one part. Partitions of a set A and equivalence relations on A share a special connection.

Recall that for the equivalence relation congruence mod n on the set $\mathbb{Z}$, each integer in $\mathbb{Z}$ belonged to a group of equivalent integers. For $n = 2$, these groups were the even and odd integers, while for $n = 3$ they are the number equivalent to $0 \bmod 3$, $1 \bmod 3$, and $2 \bmod 3$. We call these groups *equivalence classes*:

Definition. *An* equivalence class *of an equivalence relation R on a set A is the set of all elements of A equivalent to each other under R.*

Hold up; how do we even know these tidy classes exist where all the elements are equivalent to each other? If we have $a, b \in A$ such that $(a, b) \in R$, what's to say that there isn't some $c \in A$ such that $(a, c) \in R$ but $(b, c) \notin R$? Well, the symmetry and transitivity of R gives us this, since if $(a, b) \in R$, then $(b, a) \in R$, and since $(b, a) \in R$ and $(a, c) \in R$, then $(b, c) \in R$. Moreover, each element $a \in A$ goes in some class, since $a = a$, so it goes in the class containing itself. Suffice to say, the following is true:

Theorem. *Let A be a set. For every partition of A there exists a equivalence relation on A and vice versa.*

We'll see later how partitions are useful to solve some counting problems. As a teaser, consider the number of permutations of a set of elements, some of which are *not* distinct, e.g. the permutations of the objects $1, 1, 2, 2$. Let me "mark" the objects to differentiate the equivalent ones: $1, 1', 2, 2'$. Counting permutations, $(1, 1', 2, 2')$ is different than $(1, 2, 1', 2')$, but the same as $(1', 1, 2', 2)$, since 1 and $1'$ don't count as different in the permutation.

To count these, we treat repeated elements as equivalent with their own order just among themselves, e.g. $1'$ then 1 in the permutation $(1', 2, 2', 1)$. Then the total number of permutations of k things is $k!$ divided by the number of ways to reorder the equivalent objects. The example here has $\frac{4!}{2!2!}$ permutations, since there are 4 objects with 2 equivalence classes (1 and 2), each of size 2. For the set $1, 1', 1'', 2, 2''$, there would be $\frac{5!}{3!2!}$ permutations, since the equivalence class 1 now has 3 items. We'll go into more detail and example later, so don't worry if you don't quite follow this brief intro.