Finish Set Theory
Nested Quantifiers

Margaret M. Fleck

18 February 2009

This lecture does a final couple examples of set theory proofs. It then fills in material on quantifiers, especially nested ones, from sections 1.3 and 1.4.

1 Announcements

Return first quiz.

First midterm is a week from Wednesday (25 February) in class. We've posted a skills list and the midterm from last fall. Please tell me ASAP about any conflicts.

There will not be a homework due the Friday after the midterm. (Yeah!)

Schedule preview:

- today: finish set theory, nested quantifiers
- Fri and next Monday: functions (Rosen 2.3)
- discussions next week: exam review

2 Another set theory proof

Last Friday, we saw several proofs of identities from set theory. The key step in many of these proofs involved showing that a set A was a subset of a set B by picking a random element from A and showing that it must be in B.

Here's another claim of the same type. This property is called "transitivity," just like similar properties for (say) $\leq$ on the real numbers.

Claim 1 *For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

> Proof: Let A, B, and C be sets and suppose that if $A \subseteq B$ and $B \subseteq C$.

Our ultimate goal is to show that $A \subseteq C$. This is an if/then statement: for any x, if $x \in A$, then $x \in C$. So we need to pick a representative x and assume the hypothesis is true, then show the conclusion. So our proof continues:

> Let x be an element of A. Since $A \subseteq B$ and $x \in A$, then $x \in B$ (definition of subset). Similarly, since $x \in B$ and $B \subseteq C$, $x \in C$. So for any x, if $x \in A$, then $x \in C$. So $A \subseteq C$ (definition of subset again). $\square$

3 A proof using power sets

The claim we just proved can be used to prove a useful fact about powersets.

Claim 2 *For all sets A and B, $A \subseteq B$ if and only if $\mathbb{P}(A) \subseteq \mathbb{P}(B)$.*

Our claim is an if-and-only-if statement. The normal way to prove such a statement is by proving the two directions of the implication separately. Although it's occasionally possible to do the two directions together, this doesn't always work and is often confusing to the reader.

> Proof ($\rightarrow$): Suppose that A and B are sets and $A \subseteq B$. Suppose that S is an element of $\mathbb{P}(A)$. By the definition of power set, S must be a subset of A. Since $S \subseteq A$ and $A \subseteq B$, we must have that $S \subseteq B$ (by the claim we proved above). Since $S \subseteq B$, the definition of power set implies that $S \in \mathbb{P}(B)$. Since we've shown that any element of $\mathbb{P}(A)$ is also an element of $\mathbb{P}(B)$, we have that $\mathbb{P}(A) \subseteq \mathbb{P}(B)$.

A really common mistake is to stop at this point, thinking you are done. But we've only done half the job. We need to show that the implication works in the other direction:

> Proof ($\leftarrow$): Suppose that A and B are sets and $\mathbb{P}(A) \subseteq \mathbb{P}(B)$. By the definition of power set, $A \in \mathbb{P}(A)$. Since $A \in \mathbb{P}(A)$ and $\mathbb{P}(A) \subseteq \mathbb{P}(B)$, we know that $A \in \mathbb{P}(B)$ (definition of subset). So, by the definition of power set, $A \subseteq B$. $\square$

4 Another example with products

Here's another fact about Cartesian products of sets:

Claim 3 *For any sets A, B, and C, if $A \times B \subseteq A \times C$ and $A \neq \emptyset$, then $B \subseteq C$.*

Notice that this is like dividing both sides of an algebraic equation by a non-zero number: if $xy = xz$ and $x \neq 0$ then $y = z$. The empty set is playing the role of zero in these set theory identities.

A general property of proofs is that the proof should use all the information in the hypothesis of the claim. If that's not the case, either the proof has a bug (e.g. on a CS 173 homework) or the claim could be revised to make it more interesting (e.g. when doing a research problem, or a buggy homework problem). Either way, there's an important issue to deal with. So, in this case, we need to make sure that our proof does use the fact that $A \neq \emptyset$.

Here's a draft proof:

> Proof draft 1: Suppose that A, B, C, and D are sets and suppose that $A \times B \subseteq A \times C$ and $A \neq \emptyset$. We need to show that $B \subseteq C$.
>
> So let's choose some $x \in B$. ...

The main fact we've been given is that $A \times B \subseteq A \times C$. To use it, we need an element of $A \times B$. Right now, we only have an element of B. We need to find an element of A to pair it with. To do this, we reach blindly into A, pull out some random element, and give it a name. But we have to be careful here: what if A does contain any elements? So we have to use the assumption that $A \neq \emptyset$.

> Proof draft 1: Suppose that A, B, C, and D are sets and suppose that $A \times B \subseteq A \times C$ and $A \neq \emptyset$. We need to show that $B \subseteq C$.
>
> So let's choose some $x \in B$. Since $A \neq \emptyset$, we can choose an element t from A. Then $(t, x) \in A \times B$ by the definition of Cartesian product.
>
> Since $(t, x) \in A \times B$ and $A \times B \subseteq A \times C$, we must have that $(t, x) \in A \times C$ (by the definition of subset). But then (again by the definition of Cartesian product) $x \in C$.
>
> So we've shown that if $x \in B$, then $x \in C$. So $B \subseteq C$, which is what we needed to show.

5 Quantifier scope

Before we move onto functions, we need to digress a bit and fill in some facts about quantifiers.

As an example, I claim that $\mathbb{P}(A \cup B)$ is not (always) equal to $\mathbb{P}(A) \cup \mathbb{P}(B)$. We can disprove this claim with a concrete counter-example. Suppose that $A = \{x, y\}$ and $B = \{y, z\}$. Then $\{x, y, z\}$ is in $\mathbb{P}(A \cup B) = \mathbb{P}(\{x, y, z\})$. But it's not in $\mathbb{P}(A) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$, nor in $\mathbb{P}(B) = \{\emptyset, \{z\}, \{y\}, \{z, y\}\}$.

Let's look at this using quantifiers. Suppose that X is some set. $X \in \mathbb{P}(A)$ if $X \subseteq A$ i.e. $\forall x \in X, x \in A$. So $X \in \mathbb{P}(A) \cup \mathbb{P}(B)$ if

$$(\forall x \in X, x \in A) \vee (\forall y \in X, y \in B)$$

A quantifier is said to *bind* its variable. And the *scope* of that binding is the portion of equations and/or text during which that binding is supposed to be in force. Normally, the scope extends to the end of the sentence, unless the variable is redefined by a new quantifier. In this example, the scope of the binding of x is the whole statement. Or, you could say the scope is just the first half of the statement, since x is never used in the second half.[1] The scope of the binding of y is the second half.

A more sloppy or distracted author might write this with two copies of the variable x.

$$(\forall x \in X, x \in A) \vee (\forall x \in X, x \in B)$$

This actually means the same thing. There's two different bindings for x, once of which lasts ("has scope") for the first half of the statement and one of which has scope over the second half. Sometimes you have to look carefully at parentheses to figure out how long the author intended a variable binding to last.

Now, let's look at $X \in \mathbb{P}(A \cup B)$. This is the case if

$$\forall x \in X, x \in A \vee x \in B$$

This time, there's only one variable binding, extending for the whole sentence.

The two versions don't mean the same thing. The statement $\forall x \in X, x \in A \vee x \in B$ requires that every x belong to one of the two sets. The statement $(\forall x \in X, x \in A) \vee (\forall y \in X, y \in B)$ requires that either all the values satisfy a more restrictive condition (belonging to A) or that all the values satisfy a second more restrictive condition (belonging to B).

[1] It doesn't really matter which way you want to think about such cases.

6 Nested quantifiers

The more interesting cases arise when we set up two quantified variables and then use a predicate that refers to both variables at once. These are called *nested quantifiers*. For example,

> For every person p in the Fleck family, there is a toothbrush t such that p brushes their teeth with t.

This sentence asks you to consider some random Fleck. Then, given that choice, it asserts that they have a toothbrush. The toothbrush is chosen after we've picked the person, so the choice of toothbrush can depend on the choice of person. This doesn't absolutely force everyone to pick their own toothbrush. (For a brief period, two of my sons were using the same one because they got confused.) However, at least this statement is consistent with each person having their own toothbrush.

Suppose now that we swap the order of the quantifiers, to get

> There is a toothbrush t, such that for every person p in the Fleck family, p brushes their teeth with t.

In this case, we're asked to choose a toothbrush t first. Then we're asserting that every Fleck uses this one fixed toothbrush t. Eeeuw!

We'd want the quantifiers in this order when there's actually a single object that's shared among the various people, as in:

> There is a stove s, such that for every person p in the Fleck family, p cooks his food on s.

When you try to understand or prove a statement with nested quantifiers, think of making a sequence of choices for the values, one after another.

Notice that a statement with multiple quantifiers is only difficult to understand when it contains a mixture of existential and universal quantifiers. If all the quantifiers are existential, or if all the quantifiers are universal, the order doesn't matter and the meaning is usually what you'd think.

7 Nested quantifiers in mathmatics

Suppose that S is a set of real numbers, then a real number x is called an *upper bound* for S if

$$\forall y \in S, y \leq x$$

For example, 2.5 is an upper bound for the set $A = \{-3, 1.5, 2\}$. So is 2. So is 3.14159.

S is *bounded above* if there is some upper bound for S, i.e.

$$\exists x \in \mathbb{R}, \forall y \in S, y \leq x$$

For example, our set A is bounded above. But the set of even integers is not.

Notice that the existential quantifier came first, so we are requiring one choice of x (the upper bound) to work for all elements of S. This is the shared stove case.

What if we reverse the order of the quantifiers, to get:

$$\forall y \in S, \exists x \in \mathbb{R}, y \leq x$$

This is the personal toothbrush case. For each element of x, we're claiming that there is a larger real number. That's obviously true, because we could just pick $x + 1$. So this weaker condition is true for any set of real numbers, even ones that stretch off to infinity like the even integers.