Finish Set Theory
Nested Quantifiers

Margaret M. Fleck

17 February 2010

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

Schedule preview:

- today: finish set theory, nested quantifiers
- Fri and next Monday: functions (Rosen 2.3)
- discussions next week: exam review
- midterm next Wednesday (30 September) **7-9pm, 141 Wohlers**. lecture is optional exam question/answer.
- No homework due a week from Friday (2 October)

2 Recap

Last lecture, 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. We also saw that you can prove two sets A and B to be equal by showing that $A \subseteq B$ and $B \subseteq A$.

In particular, remember that we proved the following:

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

Let's also recall that the powerset of A ($\mathbb{P}(A)$) is the set containing all subsets of A. For example

$$\mathbb{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$$

3 A proof using power sets

Now, we can prove a claim about power sets:

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 transitivity). 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 $\mathbb{P}(A) \subseteq \mathbb{P}(B)$. Notice that $A \subseteq A$. By the definition of power set, this implies that $A \in \mathbb{P}(A)$. 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 A proof using sets and contradiction

Here's a claim about sets that's less than obvious:

Claim 3 *For any sets A and B, if $(A-B)\cup(B-A) = A\cup B$ then $A\cap B = \emptyset$.*

Notice that the conclusion $A \cap B = \emptyset$ claims that something does not exist (i.e. an object that's in both A and B). So this is a good place to apply proof by contradiction.

> Proof: Suppose not. That is, suppose that A and B are sets, $(A - B) \cup (B - A) = A \cup B$ but $A \cap B \neq \emptyset$.
>
> Since $A \cap B \neq \emptyset$, we can choose an element from $A \cap B$. Let's call it x.
>
> Since x is in $A \cap B$, x is in both A and B. So x is in $A \cup B$.
>
> However, since x is in B, x is not in $A - B$. Similarly, since x is in A, x is not in $B - A$. So x is not a member of $(A - B) \cup (B - A)$. This means that $(A - B) \cup (B - A)$ and $A \cup B$ cannot be equal, because x is in one but not the other. This contradicts our assumption at the start of the proof.
>
> Therefore $A \cap B$ must be empty. $\square$.

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).

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

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

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.