# Lecture 2

Ben Rosenberg

June 8, 2021

## Mathematical background (cont.)

Previously: *predicates* (template for making propositions); propositional function. Takes some argument from some domain, and transforms it into a proposition. In order to define a predicate, we need to know the domain that its arguments come from and the way it transforms the argument into a proposition.

For the time being, our domain will be the set of natural numbers, $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

### Variables

Suppose that we have a predicate which squares an argument, adds one, and checks whether it is $> 18$.

One value that would make this predicate `true` is $10$, and one that would make it `false` is $0$.

Another example: consider the proposition in which we multiply some number by 2, add the square of a different number, and check whether that is greater than 3 times the last number minus 2. In other words:

$$2\blacksquare + \square^2 > 3\square - 2$$

This is difficult to understand and so we introduce variables to represent arbitrary equivalent values in a predicate function. For instance, in the above example, it is better to write:

$$2x + y^2 > 3y - 2$$

*"A predicate is a named box"*

We can write the entire predicate as $Q(x, y) = 2x + y^2 > 3y - 2$. $Q$ is the propositional function, with arguments $x$ and $y$. We can calculate the truth value of $Q(a, b)$ by plugging $a$ and $b$ in for $x$ and $y$ respectively within $Q$. For example, $Q(1, 2) = 2 \cdot 1 + 2^2 > 3 \cdot 2 - 2 \implies$ `false`.

### Universal Quantifiers

Recall the example from last time in which we wanted to fail every student.

Consider predicate $P(x)$. Then, $(\forall x)(P(x))$ is pronounced "for all $x$, $P(x)$", and is a proposition that is `true` exactly when (if and only if) $P(x)$ is `true` for every value of $x$ in the domain of $P$. This is, in essence, a generalized conjunction operator:

$$(\forall x)(P(x)) = P(0) \wedge P(1) \wedge P(2) \wedge P(3) \wedge \cdots$$

We need this generalized conjunction operator in order to be rid of the "and so on" idea. Consider the sequence that begins $s_0 = 0, s_1 = 1, s_2 = 2, s_3 = 3$, "and so on". The logical continuation is $s_4 = 4$,

as the sequence appears to be an enumeration of the natural numbers. However, it could also have been $s_m := m(m-1)(m-2)(m-3)+m$, which would mean that $s_4 = 28$. We need a way to describe concretely the behaviour of infinite sequences outside of "and so on", so that we can be sure as to its values at any given place.

And so we define $\forall$ as the "for all" operator, the universal quantifier, as the generalized infinite conjunction of propositions.

For example, consider $(\forall x)(x > 3) : x \in \mathbb{N}$. This is a `false` statement – we can enumerate the conjunctions as $0 > 3 \wedge 1 > 3 \wedge 2 > 3 \wedge 3 > 3 \wedge \ldots$ and we can clearly see that the entire proposition is `false`.

## Existential quantifier

$(\exists x)(P(x))$ is a proposition which is `true` exactly when $P(x)$ is `true` for at least one value of $x$ in the domain. This is the generalized disjunction: $P(1) \vee P(2) \vee P(3) \vee \ldots$.

Now consider our previous example but with the existential quantifier: $(\exists x)(x > 3)$. This is `true` because there is at least one example (e.g., $x = 4$) for which $x > 3$ in the domain.

Both of these quantifiers allow us to make generalized statements about the domain without discussing individuals.

Consider $G(x) \Leftrightarrow$ student $x$ fails. Then, to return to our original motivating problem, we would say that every student fails with the proposition $(\forall x)(G(x))$.

## Free and bound variables

Consider the predicate $R(x)$. We cannot say anything about the truth value of $R(x)$ other than that its value depends on $x$. Similarly, $R(x) = R(y)$ depends on both $x$ and $y$ – in general, it is `false` unless we know that $x = y$.

Now consider $(\forall x)(R(x)) = (\forall y)(R(y))$. This is `true`, because neither of these propositions truly depend on $x$ or $y$, as they relate to every value in the domain. (We assume that $x$ and $y$ have the same domain.) To intuitively grasp this we can harken back to our notion of boxes, and realize that $x$ and $y$ are simply different boxes which can take any value in the domain.

Consider $R(x)$ for *free variable* x. We say that $x$ must receive a value to turn this into a proposition – $R(x)$ depends on $x$. A **free variable** is a variable on which an expression depends.

Now consider $(\forall x)(R(x))$. Here, $x$ is a **bound variable**, because this expression does not depend on $x$ – by definition, this expression requires that every possible value be plugged into $x$, and then the infinite conjunction be taken. There is no freedom to use arbitary values.

Consider the expression $(\exists x)(x > y)$. This is a predicate in $y$, because while $x$ is bound, $y$ is free. Let this equal $T(y)$.

$T(1)$ is $(\exists x)(x > 1)$ which is `true`; $T(17)$ is $(\exists x)(x > 17)$ which is `true`. We know that for all $y$, $T(y)$ is `true` – that is, $(\forall y)(T(y))$. Plugging in our original $T(y)$ we can say that $(\forall y)(\exists x)(x > y)$.

We can rename $x$ to $w$ without consequence because $x$ is bound, which results in the (still true) statement that $(\forall y)(\exists w)(w > y)$. This can be repeated so long as the names aren't identical to a previously defined variable (that is, the new names cannot occur in the scope of renaming). In fact, this issue of scope is the one which causes conflicts in the renaming of variables to predefined names in programming languages.

## Multiple quantifiers

Ex. $(\forall x)(\forall y)(x > y)$. This is clearly `false` because $x$ and $y$ take all possible pairs of values, from which infinitely many `false` propositions emerge.

Ex. $(\exists x)(\exists y)(x > y)$. This is clearly `true` because $x$ and $y$ can take all possible pairs of values, from which at least one `true` proposition emerges.

#### Alternating quantifiers

Some examples:

- $(\forall x)(\exists y)(y \geq x)$: `true`
- $(\exists y)(\forall x)(y \geq x)$: `false`
- $(\forall y)(\exists x)(y \geq x)$: `true`
- $(\exists x)(\forall y)(y \geq x)$: `true`

The second and third of these were difficult for the class. The third one should be written out in terms of the infinite conjunction supplied by the $\forall$ operator as $\exists x : 0 \geq x \wedge \exists x : 1 \geq x \wedge \exists x : 2 \geq x \wedge \ldots$. Since there is one of these (namely, $0$) we can reason that each of these will be `true` for $x = 0$. (More formally, we could prove by induction that this is the case for all $y$ but that level of rigor is currently unnecessary.)

The way given in class to think about this is as though the "adversary has chosen $y$", as though proving the truth value of the proposition were a game theory problem: we are helpless as to the values of $y$, as it is beyond our control. We as the evaluators of the proposition are the choosers of $x$. The existential quantifiers are our choices, the universal quantifiers are the adversary's choices, and the order in which they are written is the order in which the choices are made.

The second one of these examples is similar to the previously-covered one, in which the adversary can always choose a number one higher than ours. It is `false` because the natural numbers $\mathbb{N}$ are infinite.

When the claim is `false`, we can prove the negation. Applying DeMorgan's laws to the universal quantifier is possible as follows:

$$\neg(\quad \wedge \quad) = (\neg \quad) \vee (\neg \quad)$$

$$\neg(\exists x)(\quad) = (\forall x)(\neg \quad)$$

$$\neg(\forall x)(\quad) = (\exists x)(\neg \quad)$$

We know that the negation of the second example is therefore $(\forall y)(\exists x)(y < x)$, which we can prove to be `false` by choosing $x = y + 1$ for all of our adversary's choices.

Example game theory quantifier alternation:

$$(\forall x)(\exists y)(\forall q)(\exists v)(\forall t)(\exists s)(xy + t - w < s + v)$$

This is `true`, which we can prove with our game theory method easily. As this was done in class it is left as an exercise to those reviewing the notes.

## Sets

Consider the expression $x \in S$. This is a predicate in two variables, $x$ and $S$, and is pronounced "$x$ is an element of $S$", or "$x$ is in $S$". Let's say that we fix $S$. Then, we propose that $P_s(x)$ is equivalent to $x \in S$.

$P_s(x)$ splits the natural numbers into two parts – the `false` part and the `true` part. In fact, every predicate does this, splitting the universe into the parts that make it `true` and `false`.

Sets allow us to explore the notion of collections of elements of the domain which make a predicate `true` or `false`, grouping individuals rather than simply classifying them.

The grading book predicate, for example, splits the domain of students into those who pass and those who fail. If we want to perform some kind of operation on all the students who passed, we would need to employ the notion of a set.

We can write a set $S = \{x|P_s(x)\}$. Note that $x$ is bound – $P_s(x)$ is defining $x$ here; we could write $S = \{y|P_s(y)\}$ to the same effect. We can read this as "$S$ is the set of all $x$ such that $P_s(x)$".

More notation: $x \notin S \Leftrightarrow \neg(x \in S)$, read as "$x$ is not in $S$".

We can also specify a set elementwise: $A = \{1, 2, 3, 4\}$. The predicate in this case is defined implicitly, as $A = \{x|x = 1 \vee x = 2 \vee x = 3 \vee x = 4\}$.

Definition: Proper subset. $A \subset B \Leftrightarrow A \subseteq B \wedge A \neq B$

$A \subset B \Leftrightarrow A \subseteq B \wedge B \nsubseteq A$

$A$ is a proper subset of $B$ if $A$ is a subset of $B$ but not equal to $B$.

**Set operations**

Definitions:

- $A \subseteq B \Leftrightarrow (\forall x)(x \in A \implies x \in B)$: subset
- $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$: "two-way inclusion" (set equality)
- $A \cup B = \{x|x \in A \vee x \in B\}$: union
- $A \cap B = \{x|x \in A \wedge x \in B\}$: intersection

Theorem: $A \cup B = B \cup A$

Proof:

$$\begin{aligned} A \cup B &= \{x|x \in A \vee x \in B\} \\ &= \{x|x \in B \vee x \in A\} (\vee \text{ is commutative}) \\ &= B \cup A (\text{definition of union}) \end{aligned}$$

The proof is the same for the theorem of $A \cap B = B \cap A$, as $\wedge$ is commutative.

Definition: $A \backslash B = \{x|x \in A \wedge x \notin B\}$ (set difference – *not* commutative)

If all sets are known to belong to a certain set $E$ as subsets, then we can write $\overline{A} = E \backslash A$, pronounced "$A$ complement" or "the complement of $A$". Note that we need to specify the universe set $E$ before we specify complement implicitly.

Theorem: $A \subseteq A$

Proof:

$(\forall x)(x \in A \implies x \in A)$ (`true` by definition of implication – `true` implies `true`, and `false` implies `false`)

So, $A \subseteq A$ by the definition of subset.

□

Definition: The empty set is $\emptyset = \{\} = \{x|x \neq x\}$. The predicate for this set is always `false`, so nothing belongs to the empty set – it has zero elements. Thus, the predicate that $x \in \emptyset$ is `false` for all $x$.

Theorem: The empty subset is a subset of every set: $\emptyset \subseteq A$.

Proof:

$$\begin{aligned} \emptyset \subseteq A &\Leftrightarrow (\forall x)(x \in \emptyset \implies x \in A) \ \text{(definition of subset)} \\ &\Leftrightarrow (\forall x)(\texttt{true}) \ \text{(definition of implication)} \end{aligned}$$

□

Theorem: The empty set is unique: if $\emptyset_1$ and $\emptyset_2$ are empty sets, then $\emptyset_1 = \emptyset_2$.

Proof:

$$\begin{aligned} &\emptyset_1 \subseteq \emptyset_2 \ \text{(previous theorem –}\emptyset_1\text{ is empty)} \\ &\emptyset_2 \subseteq \emptyset_1 \ \text{(previous theorem –}\emptyset_2\text{ is empty)} \\ &\emptyset_1 = \emptyset_2 \end{aligned}$$

□

Theorem: $\{a, a\} = \{a\}$: Each set contains no duplicate elements.

Proof:

$$\begin{aligned} \{a, a\} &= \{x | x = a \vee x = a\} \ \text{(definition of this notation)} \\ &= \{x | x = a\} \ \text{(truth table for } p \vee p \Leftrightarrow p) \\ &= \{a\} \ \text{(notation for curly braces again)} \end{aligned}$$

□

Theorem: $\{a, b\} = \{b, a\}$: Sets are unordered.

Proof:

$$\begin{aligned} \{a, b\} &= \{x | x = a \vee x = b\} \ \text{(definition of this notation)} \\ &= \{x | x = b \vee x = a\} \ \text{(commutativity of } \vee) \\ &= \{b, a\} \ \text{(notation for curly braces again)} \end{aligned}$$

□

Theorem: $A \cup \emptyset = A$

Proof: $A \cup \emptyset = \{x | x \in A \vee x \in \emptyset\} = \{x | x \in A \vee x \in \emptyset\}$ because $p \vee \ \texttt{false} \ = p$

Other interesting corollaries:

- $\overline{A} \cup A = E$
- $\overline{E} = \emptyset$
- $\overline{\emptyset} = E$

## Ordered pairs

An ordered pair $(x, y)$ is a set $\{\{a, b\}, \{b\}\}$ containing the set $\{a, b\}$ and the singleton set $\{b\}$.

Theorem: $(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$: Ordered pairs are equal if and only if they are equal componentwise.

Note: when proving a theorem that contains an `iff`, we need to prove both directions.

Proof:

$(\Leftarrow)$: Need to prove that if $a = c \wedge b = d$ then $(a, b) = (c, d)$.

This is evident; we can simply substitute.

$(\Rightarrow)$: Need to prove that if $(a, b) = (c, d)$ then $a = c \wedge b = d$.

Indeed:

$(a, b) = (c, d) \implies \{\{a, b\}, \{b\}\} = \{\{c, d\}, \{d\}\}$

Now we need to use set equality ($A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$).

Case 1: $b = d, a = c$. This works.

Case 2: We have a two-element set equal to a one-element set. This is possible only if $a = b = d = c$. In this case, it still holds that $a = c$ and $b = d$.

Thus, ordered pairs are equal if any only if they are componentwise equal.

## Set product (Cartesian product)

Definition: Given sets $A$ and $B$, the set product $A \times B$ of $A$ and $B$ is equal to the following set of ordered pairs:

$$A \times B = \{(x, y) | x \in A \wedge y \in B\}$$

To improve our intuition of the operation, we might wholly embrace the "Cartesian" element of the Cartesian product and illustrate the operation on a graph. With two axes, one for the elements of $A$ and one for the elements of $B$, and note that each point on the plane in the upper right-hand quadrant will correspond to one of the ordered pairs in the set.

Define the **cardinality** or **size** (number of elements) of a set $A$ as $|A|$. Then, the cardinality of the set product of two sets $A$ and $B$ is $|A| \cdot |B|$.

Other relevant fact: $A \times \emptyset = \emptyset$ (note that using our above definition of size, $|A \times \emptyset| = 0 \ \forall A$).

Definition: The set of subsets of a given set $S$ is called the power set $\mathcal{P}(S) = \{x | x \subseteq S\}$. (The "preferred name" according to Professor Obrenić is simply "the set of all subsets" but everyone calls it the power set.)

Ex. $A = \{1, 2, 3\}$

Then:

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Theorem: If $|S| = m$, then $|\mathcal{P}(S)| = 2^m$. (This is where the name "power set" comes from.)

We will continue with the proof of this next time. (Hint: we must choose whether or not each of the elements is to be included, which is two choices for each element in the set.)