2/6 Nested quantifiers §1.6

Consider a statement like:

"For every real number x, there is a real number y that is strictly greater than x."

We can represent this statement using nested quantifiers:

$$\forall x \, \exists y \; P(x,y) \qquad \text{where } P(x,y) = \text{"} y > x \text{"}$$

Here $P(x,y)$ is a propositional formula involving two variables x and y. Its domain of discourse is the set $\mathbb{R} \times \mathbb{R}$ of pairs (x,y) of real numbers.

The previous example mixed existential & universal quantifiers. We can also use multiple of the same kind of quantifier with a statement like

"The sum of two positive real numbers is positive"

which can be written symbolically as:

$$\forall x \; \forall y \quad (x > 0) \wedge (y > 0) \rightarrow (x + y > 0)$$

where the domain of discourse is again $\mathbb{R} \times \mathbb{R}$.

WARNING: when we do mix $\forall$ and $\exists$ it is very important to make sure the order of quantifiers is correct.

E.g. $\forall x \, \exists y \;\; y > x$ is TRUE: it expresses the idea that there is no biggest real number.

But... $\exists y \, \forall x \;\; y > x$ is FALSE: that would be saying there is a real number bigger than every real number.

Q: What does "$\forall x \, \exists y \, (x + y = 0)$" mean? ($D = \mathbb{R} \times \mathbb{R}$ again)

A: For every real number x, there is a real number y such that $x + y = 0$. This is true because we can take $y = -x$ and then $x + (-x) = 0$.

Compare the previous example w/ "$\exists y \, \forall x \, (x+y)=0$"
which is FALSE: there is not a single real number y that sums to 0 with every real number x.

Key difference between $\forall x \, \exists y \, P(x,y)$ and $\exists y \, \forall x \, P(x,y)$:
with $\forall x \exists y \, P(x,y)$: the y is allowed to depend on x,
but with $\exists y \, \forall x \, P(x,y)$: the y cannot depend on x.
((Can also think in terms of "adverserial game": see book).

Q: Is $\exists y \, \forall x \, (x+y=x)$ true?
A: Yes, take $y=0$ so that $x+y=x+0=x \;\; \forall x$.

We can also use (nested) quantifiers to define properties.
Consider the propositional formula $P(n)$ where
$P(n) =$ "$\exists m \in \mathbb{Z} \; \exists p \in \mathbb{Z} \;\; (m>1) \wedge (p>1) \wedge (mp=n)$."

For example, for $P(6)$ we have "$\exists m,p \in \mathbb{Z}^2 \; (m>1) \wedge (p>1) \wedge (mp=6)$"
and this statement is true since we can take $m=2$ and $p=3$ so that $mp=6$. But on the other hand $P(7)$ is false since we cannot write 7 as a product of two integers that are strictly greater than 1.
We can see that for an integer $n \geq 2$,
$P(n)$ express the property "n is composite",
i.e., "n is not a prime number."

Many important properties of mathematical objects are expressed like this using nested quantifiers.

2/8

Proofs (Chapter 2 of textbook)

We are finally moving beyond the 1st chapter of the book. In Chapter 2, we will use the logical language we have developed to talk about mathematical proofs, and learn several different kinds of proof techniques.

Mathematical systems and direct proofs §2.1

Proofs occur within mathematical systems, which are made up of axioms, definitions, and undefined terms.

For example, the theory of "planar Euclidean geometry" is a mathematical system. One of its axioms is:

- Given two distinct points, there is exactly one line that contains both of them.

Axioms are the basic laws from which other results are deduced. Here the terms "point" and "line" are undefined terms: their meaning is inferred from axioms.

An example of a definition in Euclidean geometry is:

- A triangle is equilateral if all its sides are the same length.

(Of course, "triangle," "side," etc. would also need to be defined...)

Even with axioms & definitions, to really make a math. system worthwhile we also need theorems: results that can be deduced from the basic axioms.

A theorem in Euclidean geometry is:

- If a triangle is equilateral then it is equiangular.

Sometimes we give special names to certain kinds of theorems: a corollary is deduced from a bigger theorem, while a lemma is a helper result to prove a big theorem.

Another math. system is the "theory of the real numbers."
An axiom of the real numbers is:

- For any two real numbers $x, y \in \mathbb{R}$, $x \cdot y = y \cdot x$.

Multiplication of real numbers is implicitly defined by this (commutativity) and other axioms (associativity, etc.) it appears in.
We similarly define positivity for real numbers by order axioms...
A theorem of the real numbers could be:

- For any real number $x \in \mathbb{R}$, $x^2 \geq 0$.

See the book for more examples...

Our goal is not to develop a big complicated mathematical system, but to see in some simple examples what proving theorems looks like. Therefore, we will stick to two simple math. systems:
the theory of the integers and the theory of sets
where we will assume some basic familiarity with the axioms & definitions.

In practice most theorems are of the form:
$\forall x_1, x_2, \ldots, x_n$ if $P(x_1, \ldots, x_n)$ then $Q(x_1, \ldots, x_n)$.
To prove this theorem we need to show that if $P(x_1, \ldots, x_n)$ is true then $Q(x_1, \ldots, x_n)$ is true for all $x_1, \ldots, x_n$ in the domain of discourse.

E.g. Let's prove a theorem about integers, specifically about evenness/oddness of integers.
Of course, we all know what even & odd integers are, but let's establish a formal definition:

Def'n An integer n is even if it can be written as $n = 2k$ for some integer k. An integer n is odd if it can be written $n = 2k+1$ for some integer k.

Theorem The sum of an even integer and an odd integer is odd.

Proof: What we want to show is that:

"For all integers n_1 and n_2, if n_1 is even and n_2 is odd then $n_1 + n_2$ is odd."

So let n_1 and n_2 be integers, and assume the hypothesis of the "if... then...": that n_1 is even and n_2 is odd. This means $n_1 = 2k_1$ for some integer k_1 and $n_2 = 2k_2 + 1$ for some integer k_2. Therefore, $n_1 + n_2 = 2k_1 + 2k_2 + 1 = 2(k_1 + k_2) + 1$, which shows $n_1 + n_2$ is odd because $k_1 + k_2$ is an integer. ☒

2/10 — Let's prove another theorem, this time about sets:

Theorem For any sets X, Y, and Z, $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.

Pf: To prove that $A = B$ for two sets A and B, we need to show that they have the same elements. That is, that:

(a) if $x \in A$ then $x \in B$ (this is the same as $A \subseteq B$),

and (b) if $x \in B$ then $x \in A$ (this is the same as $B \subseteq A$).

So to prove this theorem we must show that

(a) if $x \in X \cap (Y \cup Z)$ then $x \in (X \cap Y) \cup (X \cap Z)$,

and (b) if $x \in (X \cap Y) \cup (X \cap Z)$ then $x \in X \cap (Y \cup Z)$.

First let's prove (a). So assume that $x \in X \cap (Y \cup Z)$. By definition of intersection, this means that: $x \in X$ and $x \in Y \cup Z$. By definition of union, this means that: $x \in X$ and ($x \in Y$ or $x \in Z$).

There are two possibilities to consider:

(1) If $x \in Y$, then $x \in X \cap Y$ (since $x \in X$ and $x \in Y$), so that $x \in (X \cap Y) \cup (X \cap Z)$ as required.

(2) If $x \notin Y$, then since ($x \in Y$ or $x \in Z$) we must have $x \in Z$, so $x \in X \cap Z$ and therefore $x \in (X \cap Y) \cup (X \cap Z)$.

We see that no matter the case, $x \in (X \cap Y) \cup (X \cap Z)$, and so we have proved (a) like we wanted to.

The proof of (b) is very similar and is left as an exercise. ☒

2/13 This kind of proof, where we assume the hypotheses of theorem and use them (together with axioms, definitions, and rules of logic) to deduce the conclusion of the theorem, is called a direct proof. We will discuss several other methods of proof soon...

First let us recall that a counterexample to a universally quantified statement is an element of the domain of discourse for which the prop. formula is false. Counterexamples can disprove proposed conjectures (= statements you think might be true).

E.g. Find a counterexample to the conjecture:

"For all nonnegative integers n, $2^n + 1$ is prime."

For $n = 0, 1, 2, 3, \ldots$ get $2^n + 1 = 2, 3, 5, 9, \ldots$

And $9 = 3 \times 3$ is not prime, so $n = 3$ is a counterexample.

E.g. The smallest counterexample to

"For all $n \geq 0$, $2^{2^n} + 1$ is prime"

is $n = 5$ with $2^{2^5} + 1 = 4294967297 = 641 \times 6700417$.

So sometimes it can be hard to find a counterexample!

Often we don't know ahead of time if a statement is true:

E.g.: If the statement "For all sets A, B, C, we have $(A \cap B) \cup C = A \cap (B \cup C)$" is true, prove it. Otherwise, find a counterexample!

Let's start by trying to prove the statement. So we'd need to show $\forall x \in (A \cap B) \cup C$ have $x \in A \cap (B \cup C)$ and conversely. Thus, let $x \in (A \cap B) \cup C$. This means that:

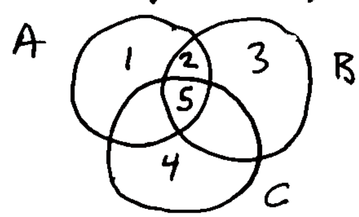
(x is in A and x is in B) or (x is in C).

We want to show: $x \in A \cap (B \cup C)$, that is:

(x is in A) and (x is in B or x is in C).

If x is in A and B, everything looks okay. But what if x is in C? Then we need to show that x is also in A. But does x have to be in A? Doesn't seem like it does... We are stuck in our attempted proof, so now we might try to make a counterexample.

We got stuck in the proof when there was an element in the set C that was not in A. This suggests a counter example might look like:



$A = \{1, 2, 5\}$
$B = \{2, 3, 5\}$
$C = \{4, 5\}$

Indeed, we can check that $(A \cap B) \cup C = \{2,5\} \cup \{4,5\} = \{2,4,5\}$ but $A \cap (B \cup C) = \{1,2,5\} \cap \{2,3,4,5\} = \{2,5\}$. $\neq$

Since $(A \cap B) \cup C \neq A \cap (B \cup C)$, these A, B, C give a counterexample which disproves the statement!

2/15

More methods of proof § 2.2

We have so far discussed the most common kind of proof: a direct proof of a universal statement $\forall x \; P(x)$. Now will we discuss some other kinds of proof...

Existence proofs: Sometimes theorems are of the form $\exists x \; P(x)$. To prove, just find x s.t. $P(x)$ is true:

E.g. Prove "There is a real number x for which $x^2 = 2$".

Pf: We can just take $x = \sqrt{2}$ (or $x = -\sqrt{2}$). $\boxtimes$

Of course, this is not much of a theorem...

You may notice existence proofs have similar form to counterexamples: By DeMorgan's Law we have that $\neg \forall x \; P(x) \equiv \exists x \; \neg P(x)$, so the relationship is clear.

Sometimes existence theorems also involve universal quantifiers nested inside of the existential quantifier:

E.g. Thm There exists a set A such that $A \cup B = B$ for all sets B.

Pf: We take $A = \emptyset$, the empty set. To prove that this works we need to prove that $\emptyset \cup B = B \;\; \forall B$.

The containment $B \subseteq \emptyset \cup B$ follows from:

Exercise: $\forall$ sets A, B have $B \subseteq A \cup B$.

To see that $\emptyset \cup B \subseteq B$, let $x \in \emptyset \cup B$.

We know that $x \notin \emptyset$ for any x, which means that $x \in B$, proving the desired inclusion.

$\boxtimes$