9/19

Nested quantifiers §1.6

Consider a statement like:

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

We can represent this statement symbolically using nested quantifiers:

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

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.

With the previous example we saw that using nested quantifiers we can mix existential + universal statements. But we can also represent something like

"The sum of two positive real numbers is positive"

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

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

Here we used two universal quantifiers.

When we do mix $\forall$ and $\exists$, it is very important to make sure the order of quantifiers is right.

for instance, $\forall x \, \exists y \;\; y > x$ is TRUE: it expresses the idea that there is no biggest real number. But: $\exists y \, \forall x \;\; y > x$ is FALSE: this would be saying that 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 with "$\exists y \forall x\ ((x+y)=0)$" which is FALSE: there is not a real number that sums to zero with every real number.

But: Is $\exists y \forall x\ (x+y=x)$ true?
Yes: take $y=0$ so $x+y = x+0 = x\ \forall x$.

Q: What does "$\exists x \exists y\ (x>1) \wedge (y>1) \wedge (xy=6)$", where the domain of discourse is $D = \mathbb{Z} \times \mathbb{Z}$ (pairs of integers) mean?

A: It means there are two integers x and y strictly bigger than 1 whose product is 6.
This is TRUE because we can take $x=2$ and $y=3$.
But for instance the proposition
"$\exists x \exists y\ (x>1) \wedge (y>1) \wedge (xy=7)$"
(w/ $D = \mathbb{Z} \times \mathbb{Z}$) would be FALSE: there are not two integers strictly bigger than 1 whose product is 7, precisely because 7 is prime.

We see how most mathematical properties can be expressed by nested quantifiers.

9/21 Proofs (Chapter 2 of text)

We are finally moving past 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. These systems are made up of axioms, definitions, and undefined terms.

For example, the theory of "planar Euclidean geometry" is a math. 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 "point" and "line" are undefined terms: their meaning is inferred from the axioms.

An example of a definition in Euclidean geometry would be:

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

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

Even with axioms + definitions, to really make a math. system worthwhile we need theorems: results that can be proved 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 used to prove a big theorem.

Another important type of proposition in a math. system is a conjecture: something you suspect is true but don't know how to prove.

E.g. Another math. system is the "theory of the real numbers."
An axiom for the real numbers is

- If x and y are real numbers, then $x \cdot y = y \cdot x$.

Multiplication of real numbers is implicitly defined by this and the other axioms it appears in. We similarly define the positive numbers by order axioms, etc.
A theorem for the real numbers might be:

- For any real number x, $x^2 \geq 0$.

See the book for more examples...

Our goal is not to develop a big complicated mathematical system, but rather to see in some simple examples what proving theorems looks like. Therefore, we will mostly stick to the theory of the integers or the theory of sets, where we assume familiarity with basic 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. 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 as $n = 2k+1$ for some integer k.

Let's use these definitions to prove the following:

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

Pf: What we want to show is that:

"For all integers n_1, 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. Assume the hypothesis of the "if... then": that n_1 is even and n_2 is odd. This means that $n_1 = 2k_1$ for some integer k_1, and $n_2 = 2k_2+1$ for some integer k_2. Hence,
$n_1 + n_2 = 2k_1 + 2k_2 + 1 = 2(k_1 + k_2) + 1$,
which shows $n_1 + n_2$ is odd b.c. $k_1 + k_2$ is an integer. $\boxtimes$

9/23 — 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 two sets are equal, we need to show they have the same elements. Thus, we must show

(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:

$x \in X$ and ($x \in Y$ or $x \in Z$). There are two possibilities: if $x \in Y$ then $x \in X \cap Y$ (since $x \in X$ and $x \in Y$) and thus $x \in (X \cap Y) \cup (X \cap Z)$ as required,

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 thus $x \in (X \cap Y) \cup (X \cap Z)$.

We see that no matter what, $x \in (X \cap Y) \cup (X \cap Z)$, so we have shown what we needed to show.

The proof of (b) is very similar and we leave it to you as an exercise. ☒

This kind of proof, where we assume the hypotheses of the theorem we are trying to prove and use them to deduce the conclusion is called a direct proof: we "directly" prove what we want to prove.

We will discuss 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 propositional formula is false.

Counterexamples can disprove proposed conjectures.

<u>E.g.</u> Find a counterexample to the conjecture
"for all nonnegative integers n, 2^n+1 is prime."

For $n=0,1,2,3,\ldots$ get $2,3,5,9,\ldots$
and $9=3\times 3$ is not prime, so $n=3$ is counterexample.

<u>E.g.</u> Find counterexample to "For all $n\geq 0$, $2^{2^n}+1$ is prime."
for $n=0,1,2,3,4$ get $3,5,17,257,65537$
which are prime but $n=5$ w/ $4294967297 = 641\times 6700417$
so $n=5$ is counterexample (conjectured by Fermat!).

<u>E.g.</u> If the statement "$(A\cap B)\cup C = A\cap(B\cup C)$" is true then prove it; otherwise find a counterexample.

Let's start by trying to prove it. We need to show that
$\forall x\in(A\cap B)\cup C$ have $x\in A\cap(B\cup C)$ and conversely.

So let $x\in(A\cap B)\cup C$. Thus (x is in A and x is in B)
or (x is in C)
and we want to show that (x is in A) and (x is in B or in C).

If x is in A and B, everything looks okay.
But the other possibility is that x is in C. Then
we would need to show that x is also in A.
But does such an x have to be in A? Doesn't seem like it...

So now we think there might be a <u>counterexample</u>,
where C has some elements not in A.

Let's try $A=\{1,2\}$, $B=\{2,3\}$ and $C=\{4\}$
Thus, $(A\cap B)\cup C = (\{1,2\}\cap\{2,3\})\cup\{4\} = \{2\}\cup\{4\} = \{2,4\}$
but $A\cap(B\cup C) = \{1,2\}\cap(\{2,3\}\cup\{4\}) = \{1,2\}\cap\{2,3,4\} = \{2\}$,
a <u>counterexample</u> to the statement! //

9/26

More methods of proof §2.2

We have so far focused on the most common kind of proof: a direct proof of a universal statement $\forall x\, P(x)$. But now we will discuss some other kinds of proofs.

Existence proofs.

Sometimes theorems are of the form $\exists x\, P(x)$. To prove a statement like this, we just need to find an x for which $P(x)$ 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 $x = -\sqrt{2}$). ∎

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

You may notice that existence proofs have a similar form to counterexamples: this is no coincidence because by De Morgan's Law $\neg \forall x\, P(x) \equiv \exists x\, \neg P(x)$.

E.g. Sometimes existence theorems also involve more quantifiers inside the existential quantifier.

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

Pf: We can take $A = \emptyset$, the empty set. To see that this works we need to prove that $\emptyset \cup B = B$ for all sets B. The containment $B \subseteq \emptyset \cup B$ is clear. To see $\emptyset \cup B \subseteq B$, let $x \in \emptyset \cup B$. Since $x \notin \emptyset$ for any x, this means that $x \in B$, proving the desired inclusion. ∎