Math 300 Class 4

Friday 11th January 2019

Recall from your pre-class reading:

Definition 1
A **predicate** is a symbol p together with a specified list of **free variables** $x_1, x_2, \ldots, x_n$ and, for each free variable x_i, a specification of a **domain of discourse** of x_i. We will typically write $p(x_1, x_2, \ldots, x_n)$ in order to make the variables explicit.

Definition 2
A **logical formula** is an expression that is built from predicates using logical operators and quantifiers; it may have both free and bound variables.

The two most important quantifiers are the **universal quantifier** $\forall$ and the **existential quantifier** $\exists$:

- The expression '$\forall x \in X, \ldots$' denotes 'for all $x \in X, \ldots$';
- The expression '$\exists x \in X, \ldots$' denotes 'there exists $x \in X$ such that $\ldots$'.

Proving universally quantified logical formulae

When X is finite, we can prove that a property $p(x)$ is true of all the elements $x \in X$ just by checking them one by one. But what if X is infinite?

Example 3
Prove that the square of every odd integer is odd.

Let n be an odd integer.

Then $n = 2k+1$ for some $k \in \mathbb{Z}$

$$\Rightarrow \quad n^2 = (2k+1)^2 = 4k^2 + 4k + 1$$
$$= 2\underbrace{(2k^2 + 2k)}_{\in \mathbb{Z}} + 1$$

So n^2 leaves a remainder of 1 when divided by 2. So n^2 is odd, as required. $\square$

The key to Example 3 was introducing a new variable n that refers to an odd integer and, without assuming anything about n other than that it is an odd integer, proving that n^2 is even. We say that n is an *arbitrary* odd integer.

A proof of $\forall x \in X,\ p(x)$ typically looks a bit like this:

- Introduce a variable x, which refers to an element of X.
- Prove $p(x)$, assuming nothing about x except that it is an element of X.

Useful phrases for introducing an arbitrary variable include 'fix $x \in X$' or 'let $x \in X$' or 'take $x \in X$'.

Example 4
Prove that every integer is rational.

Fix $n \in \mathbb{Z}$.

Then $n = \dfrac{n}{1} = \dfrac{\text{integer}}{\text{nonzero integer}} \Rightarrow n \in \mathbb{Q}$ as required. $\square$

Example 5
Prove that, for all irrational numbers x and y, the numbers $x+y$ and $x-y$ are not both rational.

Let x and y be arbitrary rational numbers.

Towards a contradiction, assume $x+y \in \mathbb{Q}$ and $x-y \in \mathbb{Q}$.

Then $x+y = \frac{a}{b}$ and $x-y = \frac{c}{d}$ for some $a,b,c,d \in \mathbb{Z}$ with $b, d \neq 0$.

So $\frac{a}{b} + \frac{c}{d} = (x+y)+(x-y) = 2x$

$\Rightarrow x = \frac{1}{2}\left(\frac{a}{b} + \frac{c}{d}\right) = \frac{ad+bc}{2bd}$

Since $ad+bc \in \mathbb{Z}$ and $2bd \in \mathbb{Z}$, with $2bd \neq 0$, it follows that $x \in \mathbb{Q}$. Contradiction! So $x+y$ and $x-y$ are not both rational. $\square$

Proving existentially quantified logical formulae

In order to prove that an element of a set X satisfying a property $p(x)$ exists, all we need to do is find one! (Well, and prove that $p(x)$ truly does hold of that element.)

Example 6
Prove that there is a natural number that is a perfect square and is one more than a perfect cube.

Define $n = 9$. Then

- n is a perfect square $\because$ $n = 3^2$
- n is one more than a perfect cube $\because$ $n-1 = 8 = 2^3$

So n is as required. $\square$

The following exercise involves both a universal and an existential quantifier.

Example 7
Prove that, for all $x, y \in \mathbb{Q}$, if $x < y$ then there is some $z \in \mathbb{Q}$ with $x < z < y$. $\Big\}$ $\forall x, y \in \mathbb{Q}, [x < y \Rightarrow \exists z \in \mathbb{Q}, x < z < y]$

Let $x, y \in \mathbb{Q}$. (Then $x = \frac{a}{b}$ and $y = \frac{c}{d}$ for some $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$.)

Assume $x < y$.

Define $z = \frac{x+y}{2}$. Then

- $z \in \mathbb{Q}$, since $z = \dfrac{\frac{a}{b} + \frac{c}{d}}{2} = \dfrac{ad+bc}{2bd}$
- $x = \frac{x}{2} + \frac{x}{2} < \underbrace{\frac{x}{2} + \frac{y}{2}}_{=z} < \frac{y}{2} + \frac{y}{2} = y$

So z is a rational number with $x < z < y$, as required. $\square$

Uniqueness

Sometimes we want to know not just that an object with a certain property *exists*, but that there is *exactly one* of them. This property is called *uniqueness*. We write $\exists! x \in X,\, p(x)$ to mean that there is exactly one $x \in X$ making $p(x)$ true.

Proving that there is one and only one element x of a set X making a property true is typically done in two stages:

- **(Existence)** Prove that *at least* one $x \in X$ makes $p(x)$ true:

$$\exists x \in X,\, p(x)$$

- **(Uniqueness)** Prove that *at most* one $x \in X$ makes $p(x)$ true:

$$\forall a, b \in X,\, [p(a) \wedge p(b) \Rightarrow a = b] \qquad \text{or} \qquad \underbrace{\forall a \in X,\, [p(a) \Rightarrow a = x]}_{\text{relative to the } x \text{ we proved } \textit{exists}}$$

Example 8
Prove that for all $a \in \mathbb{R}$, there is a unique $x \in \mathbb{R}$ such that $x^2 + 2ax + a^2 = 0$.

Let $a \in \mathbb{R}$. We prove $\exists! x \in \mathbb{R},\, x^2 + 2ax + a^2 = 0$

($\exists$) Define $x = -a$. Then

$$x^2 + 2ax + a^2 = (-a)^2 - 2a^2 + a^2 = a^2 - 2a^2 + a^2 = 0$$

as required.

(!) Let $y \in \mathbb{R}$ and assume $y^2 + 2ay + a^2 = 0$.

Then $(y+a)^2 = 0$, so $y + a = 0$, and hence $y = -a$

$\Rightarrow y = x$, as required. $\square$

Pre-class assignment for Class 5 (Mon, Jan 14)

Read §1.3 *Logical equivalence* up to and including Example 1.3.3, and then answer the questions on Canvas (go to Assignments $\to$ Class 5).

Strategies for proving statements involving quantifiers

Strategy (Proving universally quantified statements)
To prove a proposition of the form $\forall x \in X,\ p(x)$, it suffices to prove $p(x)$ for an **arbitrary** element $x \in X$—in other words, prove $p(x)$ whilst assuming nothing about the variable x other than that it is an element of X. $\triangleleft$

Strategy (Proving existentially quantified statements)
To prove a proposition of the form $\exists x \in X,\ p(x)$, it suffices to prove $p(a)$ for some **specific** element $a \in X$, which should be explicitly defined. $\triangleleft$

Strategy (Proving unique-existentially quantified statements)
A proof of a statement of the form $\exists! x \in X,\ p(x)$, consists of two parts:

- **Existence** — prove that $\exists x \in X,\ p(x)$ is true;
- **Uniqueness** — let $a, b \in X$, assume that $p(a)$ and $p(b)$ are true, and derive $a = b$.

Alternatively, prove existence to obtain a fixed $a \in X$ such that $p(a)$ is true, and then prove $\forall x \in X,\ [p(x) \Rightarrow x = a]$. $\triangleleft$

Strategies for using statements involving quantifiers as assumptions

Strategy (Assuming universally quantified statements)
If an assumption in a proof has the form $\forall x \in X,\ p(x)$, then we may assume that $p(a)$ is true whenever a is an element of X. $\triangleleft$

Strategy (Assuming existentially quantified statements)
If an assumption in the proof has the form $\exists x \in X,\ p(x)$, then we may introduce a new variable $a \in X$ and assume that $p(a)$ is true. $\triangleleft$