Proofs Involving Quantifiers

For a given universe U:

Theorem $(\forall x)\, P(x)$

Proof Let x be an arbitrary member of U. Call it $x = a$, say. (*You can continue to call it x if you like; switching to a name like "a" just makes the psychological point that its no longer a variable but a particular object chosen from U. That "a is arbitrary" means just that you know nothing special about a beyond the fact that it's a member of U.*)

Prove that $P(a)$ is true.

Theorem $(\exists x)\, P(x)$

Proof Somehow show that there is a value of x, say $x = a$, from U that makes $P(a)$ true. (*You can "announce" a and verify that it works, construct an a that must work, or argue that you theoretical reasons there must be such a value $x = a$ even though the proof doesn't explicitly say how to find the value $x = a$.*)

<u>Sometimes these theorems can be proved by contradiction</u>

Theorem $(\forall x)\, P(x)$

Proof Assume $\sim (\forall x)\, P(x)$, or equivalently, that $(\exists x) \sim P(x)$. Choose such an x : call it $x = a$. Then we know that $P(a)$ is false for this value a.

From this, argue somehow to a contradiction.

Theorem $(\exists x)\, P(x)$

Proof Assume $\sim (\exists x)\, P(x)$ or, equivalently, that $(\forall x) \sim P(x)$. From this, argue somehow to a contradiction.

Example

Theorem $(\forall n \in \mathbb{N})\ (n \text{ is even}) \Rightarrow (n^2 \text{ is even})$

Proof Assume n is a natural number. For this n, prove that
$(n \text{ is even}) \Rightarrow (n^2 \text{ is even})$. ....

We have done proofs like this before. Earlier, the theorem was worded in such a way as to avoid using the quantifier. For example, the following wording gives an equivalent theorem, and the proof starts out the same way.

Theorem Assume n is a natural number. Prove that if n is even, then n^2 is even.

Proof Assume n is a natural number. For this n, prove that
$(n \text{ is even}) \Rightarrow (n^2 \text{ is even})$. ....

Example

Theorem $(\forall x \in \mathbb{R})\,(\,(0 < x < \frac{\pi}{2}) \Rightarrow (\tan x + \cot x > 1))$

Proof (*by contradiction*)

Assume $\sim (\forall x \in \mathbb{R})\,(\,(0 < x < \frac{\pi}{2}) \Rightarrow (\tan x + \cot x > 1))$, which is equivalent to
$(\exists x) \sim (\,(0 < x < \frac{\pi}{2}) \Rightarrow (\tan x + \cot x > 1))$ which is equivalent (*why?*) to
$(\exists x)\ \ (0 < x < \frac{\pi}{2}) \wedge (\tan x + \cot x \leq 1))$

Pick such a real number x and (*optional*) call it a).

Since $0 < a < \frac{\pi}{2}$, $\tan a > 0$ and $\cot a = \frac{1}{\tan a} > 0$. Therefore we have

$0 < \tan a + \cot a \leq 1.$, Squaring both sides gives
$0 < \tan^2 a + 2 + \cot^2 a \leq 1$, so that
$\tan^2 a + \cot^2 a \leq -1.$

But this is a contradiction (*a sum of squares can't be negative*). So assuming the theorem is false leads to a contradiction, and therefore the theorem is true. •

Example

Theorem $(\exists n \in \mathbb{N})$ (n can be written as a sum of cubes in two different ways)
(*We could write this more formally as:*

for the universe $\mathbb{N}$:

$$(\exists n)\,(\,(\exists p)(\exists q)(\exists r)(\exists s)(\,(n = p^3 + q^3 \,\wedge\, n = r^3 + s^3 \,\wedge\, p \neq r \,\wedge\, p \neq s))$$

Proof Let $n = 1729$. This proves the theorem because $1729 = 10^3 + 9^3 = 12^3 + 1^3$. •

This theorem comes from an anecdote about the English mathematician G.H. Hardy and the Indian mathematician Srinivasa Ramanujan set around the time of World War I. Ramanujan was an untaught natural mathematical genius who had sent some of his work, unsolicited, to Hardy at Cambridge. Hardy was sufficiently impressed to bring him to England where, after a while, he became ill. Visiting him in the hospital, Hardy remarked that the number of the cab in which he had arrive was 1729, "not a very interesting number." To which Ramanujan immediately responded, "No, no Hardy. It is a very interesting number. It is the smallest number that can be expressed as a sum of cubes in two different ways."

You can read a bit about Hardy and Ramanujan in Hardy's little book, A Mathematician's Apology. Also, there was recently published an historical novel about Ramanujan called The Indian Clerk by David Leavitt. Also see the course web syllabus for a little more about Ramanujan.

The Intermediate Value Theorem

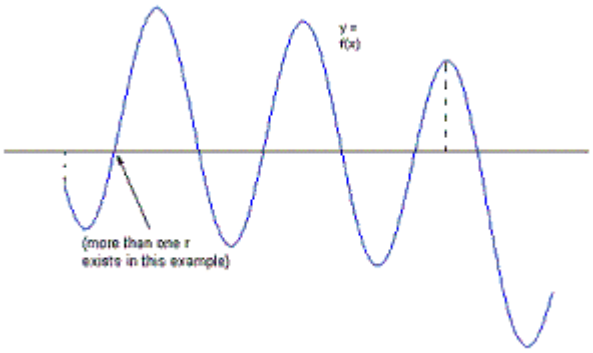
In Calculus I, you should have seen the Intermediate Value Theorem. It was probably motivated and presented as "intuitively true" (which it is). It's usually not proven until a more advanced course (Math 4111, for example) because the proof depends on a careful, proof-oriented definition for continuity and on a fairly subtle property of the real number system.

Intermediate Value Theorem Suppose that f is a continuous function whose domain is the closed interval $[a, b]$. If $f(a)$ and $f(b)$ have opposite signs, then there exists a number r in the open interval (a, b) where $f(r) = 0$.

More formally: if U is the universe of all continuous functions defined on a given closed interval $[a, b]$, then the Intermediate Value Theorem says:

$$(\forall f)\ [\ (f(a) \cdot f(b) < 0)\ \Rightarrow (\exists r)\,((a < r < b)\ \wedge (f(r) = 0))\ ]$$

Note that the theorem does <u>not</u> use the quantifier $(\exists\,!\,r)$ – because there <u>might</u> be more than one r that works.



Theorem $(\exists!\, x)P(x)$
Proof Such a proof usually has two parts:

i) Existence Prove $(\exists!\, x)P(x)$
ii) Uniqueness Prove $(\forall x)(\forall(y)\,(\,(P(x) \wedge P(y)) \Rightarrow (x = y)\,)$

Example Prove that the equation $x^5 - 2x + 1 = 0$ has a unique root between -2 and 0.
More formally, with U = the set of real numbers, $\mathbb{R}$:

Prove that $(\exists!\, r)\,[\,(-2 < r < -1\,) \wedge (r^5 - 2r + 1 = 0)$

The figure on the next page is not used in the proof; but having it there helps the reader to understand the argument. The proof assumes that the reader knows certain facts from Calculus I.

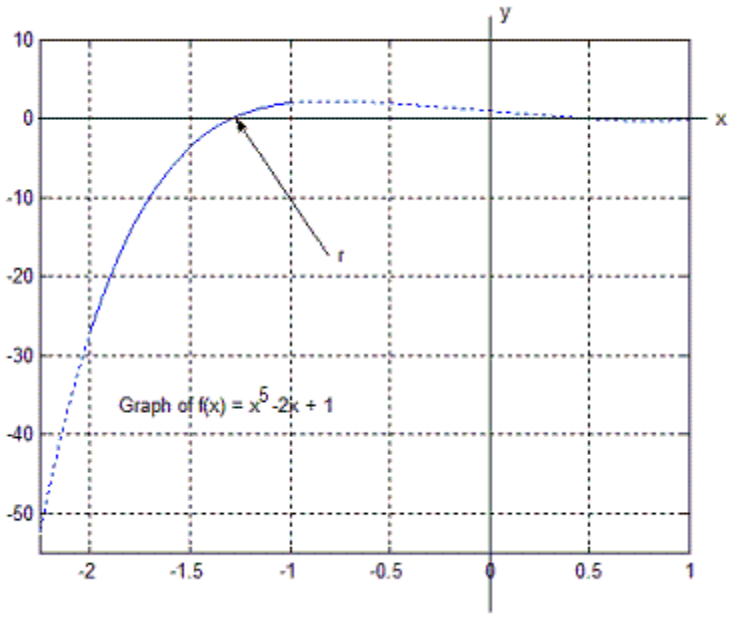
Proof i) Existence Let $f(x) = x^5 - 2x + 1$. The function f is continuous on the interval $[-2, -1]$ (because f is a polynomial) and $f(-2) = -27$ and $f(-1) = 2$. Since $f(-2)$ and $f(-1)$ have opposite signs, the Intermediate Value Theorem says that there is a number r is the interval $(-2, -1)$ for which $f(r) = 0$, that is, for which r is a root of the equation $x^5 - 2x + 1 = 0$.

ii) Uniqueness $f'(x) = 5x^4 - 2$. Since $-2 < x < -1$, we know that $5x^2 > 5$, so $f'(x) > 0$ on the interval $(-2, -1)$. Therefore f is an increasing function on theis interval so its graph can cross the x-axis at most once. Therefore there is at most one r in the interval for which $f(r) = 0$.

By i) and ii) $x - 2x + 1 = 0$ has a unique root in the interval $(-2, -1)$. •

Note that part ii) does not, by itself, show that there exists an r that works, only that there is at most one such r. The job of part i) is to show that there is at least one such r. Taken together, i) and ii) show that there is exactly one r that works.

The preceding proof is an example of what mathematicians sometimes call a "pure existence proof" : this refers to a proof of $(\exists x)P(x)$ or $(\exists! x)P(x)$ where it is argued that some value $x = r$ must exist that makes $P(r)$ true, but the proof does not actually give the value of r or show an exact method for finding it.


y
x
10
0
-10
-20
-30
-40
-50
-2
-1.5
-1
-0.5
0
0.5
1
r
Graph of f(x) = x^5 -2x + 1

Example (Multiple quantifiers)

Let the universe $U = \mathbb{R}$

Theorem $(\forall\epsilon)\,(\,(\epsilon > 0) \Rightarrow (\,(\exists k \in \mathbb{N})\,(\forall n \in \mathbb{N})\;\; (n > k) \Rightarrow (\,\frac{1}{n^2} < \epsilon)\,)$

Proof Let ϵ be an arbitrary real number

> *We now need to show that*
> $(\epsilon > 0) \Rightarrow (\,(\exists k \in \mathbb{N})\,(\forall n \in \mathbb{N})\;\; (n > k) \Rightarrow (\,\frac{1}{n^2} < \epsilon)$ is true

and assume $\epsilon > 0$.

> *We now need to show that*
> $(\exists k \in \mathbb{N})\,(\forall n \in \mathbb{N})\;\; (n > k) \Rightarrow (\,\frac{1}{n^2} < \epsilon)$ is true
>
> *We do some scratchwork: We want to force* $\frac{1}{n^2} < \epsilon$. *This inequality will be true if* $n^2 < \frac{1}{\epsilon}$ *or* $n > \sqrt{\frac{1}{\epsilon}}$. *We can't use* $\sqrt{\frac{1}{\epsilon}}$ *for* k *because* k *needs to be an integer. But <u>any</u>* $k \geq \sqrt{\frac{1}{\epsilon}}$ *will work: if* $n > k \geq \sqrt{\frac{1}{\epsilon}}$ *, then* $n > \sqrt{\frac{1}{\epsilon}}$ *so* $\frac{1}{n^2} < \epsilon$.
>
> *Just to be as <u>efficient</u> as possible, we'll pick the <u>smallest integer k</u>* $\geq \sqrt{\frac{1}{\epsilon}}$ *, which can be denoted using the <u>ceiling function</u>* : $k = \lceil \sqrt{\frac{1}{\epsilon}} \rceil$

Let $k = \lceil \sqrt{\frac{1}{\epsilon}} \rceil$.

> *For this* k*, we need to show that*
> $(\forall n \in \mathbb{N})\;\; (n > k) \Rightarrow (\,\frac{1}{n^2} < \epsilon)$ *is true*

Pick an arbitrary natural number n.

> *For this n (and the k already chosen) we need to show that*
> $(n > k) \Rightarrow (\,\frac{1}{n^2} < \epsilon)$ *is true*

Assume $n > k$. Then $n > \sqrt{\frac{1}{\epsilon}}$, so $n^2 > \frac{1}{\epsilon}$ and therefore $\frac{1}{n^2} < \epsilon$. •

(OVER → →)

Notes: 1) All the italicized material is commentary. The whole proof, without commentary, is very short:

Proof Consider an arbitrary $\epsilon > 0$, and let $k = \lceil \sqrt{\frac{1}{\epsilon}} \rceil$. If $n > k$, then $n^2 > \frac{1}{\epsilon}$ and therefore $\frac{1}{n^2} < \epsilon$. •

2) In the original statement of the theorem: ϵ starts as an arbitrary real number, but then the following conditional "if $\epsilon > 0$, then ..." immediately forces you to assume, in addition, that ϵ is positive. Because of this observation, a mathematician would probably "build-in" that $\epsilon > 0$ using notation like this:

Instead of	$(\forall\epsilon)\,(\,(\epsilon > 0) \Rightarrow (\,(\exists k \in \mathbb{N})\,(\forall n \in \mathbb{N})\;\; (n > k) \Rightarrow (\frac{1}{n^2} < \epsilon)\;)$
write	$(\forall \epsilon > 0)\;\,(\,(\exists k \in \mathbb{N})\,(\forall n \in \mathbb{N})\;\; (n > k) \Rightarrow (\frac{1}{n^2} < \epsilon)\;)$

In the second version, the informal "quantifier notation"

$(\forall \epsilon > 0)$ *** is just a shorthand for

$(\forall \epsilon)\;\; (\epsilon > 0) \Rightarrow$ ***

3) Suppose we have a sequence $a_1 = \frac{1}{1^2}$, $a_1 = \frac{1}{2^2}$, ... , $a_n = \frac{1}{n^2}$, ...

In the more informal language of Calculus II

$$(\forall \epsilon > 0)\;\,(\,(\exists k \in \mathbb{N})\,(\forall n \in \mathbb{N})\;\; (n > k) \Rightarrow (\tfrac{1}{n^2} < \epsilon)\;)$$

says that $\lim\limits_{n\to\infty} \frac{1}{n^2} = 0$. (*Agreed?*)