Proofs involving quantifiers: (Came to me idea:
⇒ Cover topics as fast as possible!)

$\forall n A(n)$

"For all natural numbers n some property A(n) holds"

- where the quantification occurs over all natural numbers is often proved by method called induction.

(Number theory) ⇐ Studies the properties of nat. numbers: 1, 2, 3

what are methods? [methods of induction]

⇐ lets see how to prove an existence statement ⇒

To prove $\exists x A(x)$

"we exist an x of A(x)" — ("Ag x")

- the obvious way is to find an object a of A(a)

eg. To show there is an irrational number,
(just prove that $\sqrt{2}$ is irrational [Euclid])

But this does Not always work.

Sometimes we use indirect proofs: (2)

Eg:

Theorem: There are irrationals r, s such that r^2 is rational

ASIDE:

Could not exist! rational number can be written as a fraction (or ratio) using integers

$\therefore$ $3/2$ (two integers) = quotient (1.5)

so too 7, $7/1 = 7$

so too 0.317 $= 317/1000 = 0.317$.

But some number CANNOT be written as ratio or fraction (using integers)

Proof: involves considering two cases:

Case 1: if $\sqrt{2}^{\sqrt{2}}$ is rational, we take $r = s = \sqrt{2}$

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is irrational, take

$$r = \sqrt{2}^{\sqrt{2}} \text{ and } s = \sqrt{2}$$

Then $r^2 = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$.

and 2 is rational $(2/1 = 2)$

From the above we looked at Case 1 and 2

- we don't need to know if $\sqrt{2}^{\sqrt{2}}$ is rational.

⇒ method: Proof by Cases

Read) Now let's look at ~~method~~ statement involving universal quantifier

Prove: $\forall x A(x)$

One way is to take an arbitrary x and show that it satisfies $A(x)$

e.g. To prove $\forall n \exists m [m > n^2]$

for all n, there is m, $m > n^2$ $(m, n \in \mathbb{N})$

⇒ how do we now handle the two quantifiers in proof.

—where the first quantifier $\forall$ is a universal quantifier

Let n be an arbitrary natural number.

Set $m = n^2 + 1$ } [our trivial argument]

∴ then $m > n^2$

This proves the statement:

$$\exists m (m > n^2)$$

"There is an m, $m > n^2$"

And it follows that $\forall n \exists m (m > n^2)$ (is true)

So how did we do it: (logical reasoning): we want to prove statement involving 2 quantifiers in form $\forall n \exists m$

—we eliminate one quantifier ($\forall n$)

by replacing it by arbitrary natural number

—why arbitrary? ⇒

—then we carry out same reasoning,

or provide an argument ($m = n^2 + 1$)

— $n^2 + 1$, and let m be this number.

— so we explicitly find an m that satisfies ($m > n^2$)

In practice, there may be pages of arguments

- since the argument satisfies (wants) an arbitrary natural number it follows it proves $\forall n$ [Eliminated quantifier]

↳ He For all has been handled by arbitrary (argument) natural number.

Note: he wants because the "n" we picked is arbitrary

Another method to use is method of Contradiction

To prove $\forall x A(x)$, assume $\neg \forall x A(x)$

This is equivalent to:

$$\exists x \neg A(x).$$

$\therefore$ Let c be object such that $\neg A(c)$

↳ not arbitrary object

Now we reason with c (and the fact that $\neg A(c)$) to derive a Contradiction.

Quiz Is this a valid proof?

To prove: $(\forall x>0)(\exists y>0)[y<x]$, where variable range over natural numbers

(This says given any positive number, you can always find a smaller one)

To prove it: pick a positive ~~number~~ rational number p arbitrarily, say $p = 0.001$ 1/1000

take $q = 0.0001$.

$\therefore 0 < q < p$

"q is less than p and greater than 0"

Since our choice of p was arbitrary, this proves the result!

But is this right?

But picking a positive ~~arbitrary~~ arbitrary number for p is not the same as letting p be arbitrary

$\Rightarrow$ the choice of p may be arbitrary, but once you made it 0.001, you have a specific p!

⇒ we even said what it is! $p=0.001$ ← (specific)

⇒ that is different from saying let p be arbitrary.

⇒ Subtle, but important point

∴ Proof is not valid

– in Century arguing with an arbitrary P,
we don't know what it is, and we not specific

Let's look at Proof by Induction

To prove statements of the form $\forall n A(n)$,
where n (quantifies) ranges over
the natural numbers

Eg. Prove that $1+2+\dots+n = \frac{1}{2}n(n+1)$

First Step: check the first few cases
(get sense of what is going on)

∴ $n=1$

$1 = \frac{1}{2}(1)(1+1) = \frac{1}{2}(2) = 1$ ✓ true for case

∴ $n=2$

$1+2 = \frac{1}{2}(2)(2+1) = 1 \cdot$

$3 = 1(3) = 3$ (true) ✓

$2\times\frac{1}{2}$
$\frac{2}{1}\times\frac{1}{2}$
$= \frac{2}{2} = 1$

$n=3$

$1+2+3 = \frac{1}{2}3(3+1)$

$6 = \frac{3}{2}(4) = \frac{12}{2} = 6$ (true)

So far this is not a proof, it's just checking the first two cases. [Beware of this]

Consider formula:

$P(n) = n^2 - n + 41$, all values of $P(n)$ for $n = 1, 2, \ldots$ etc are prime numbers

$\Rightarrow$ Not quite, until you reach $n = 41$

$P(41) = 1681 = 41^2$

↳ Leonard Euler, 1772 $\Rightarrow$

⟶

$\Rightarrow$ method of induction depends principle of, known as principle of mathematical induction

Here's what it says:

To prove $\forall n(A_n)$, establish the following 2 statements:

① $A(1)$ initial step / case

② Prove following statement $(\forall n)[A(n) \Rightarrow A(n+1)]$

↳ Called induction step

Intuitively, this gives $\forall n A(n)$ as follows:

By induction step ; $A(1)$.

If we now apply the induction step

$\therefore A[n] \Rightarrow A(n+1)$

$\therefore A(1) \Rightarrow A(2)$

So from $A(1)$ we can conclude $A(2)$

$\therefore$ next use

By $A(2)$ (first step) and then induction step

$A(2) \Rightarrow A(3)$, we can

Conclude $A(3)$ .... etc.

$\therefore$ You need axiom (or principle) to make this to work, called the principle of mathematical induction.

The PMI is what tells you that Step 1 and 2 above yield $\forall n A(n)$

Now let apply the method ....

Lets prove theorem:

for any natural n, $1+2+3\ldots+n=\frac{1}{2}n(n+1)$

Calling it theorem, I dont yet know proof.

Proof: By mathematical induction: [tell reader how you going to prove & method used]

* [So I have to ~~prove~~ show that this is true for $n=1$, then ① I to show that it is true ~~for~~, it follows for $n+1$ ②]

→ not an equation, [identity: two sides are always equal]

Step ①

∴ for $n=1$, the identity reduces to:

$$1=\frac{1}{2}(1)(1+1)=1, \text{ (true)}$$

(since Both sides equal 1)

∴ Step ② [new induction step]: Assume the identity holds for n

i.e. $1+2+\ldots n=\frac{1}{2}n(n+1)$ [original] ⊛

[induction step] → [want to deduce: $1+2+\ldots+n+1=\frac{1}{2}(n+1)(n+1)$]

Lets add $(n+1)$ to both sides ⊛:

$$1+2+\ldots n(n+1)=\frac{1}{2}n(n+1)+(n+1)$$

remove $\frac{1}{2}$ as common factor:

$1+2+\cdots+n+(n+1) = \frac{1}{2}n(n+1)+(n+1) = \frac{1}{2}[n(n+1)+2(n+1)]$

$= \frac{1}{2}[n^2+n+2n+2] = \frac{1}{2}[n^2+3n+2]$

$= \frac{1}{2}[(n+1)(n+2)]$ = same as above

$\therefore$ Same as $= \frac{1}{2}(n+1)((n+1)+1)$

which is the identity with $n+1$ in place of n.

Hence, by principle of mathematical induction, the identity holds for all n

Another example of induction proof:

Theorem: If $x > 0$ (a positive real number), then for any n (natural number), $(1+x)^{n+1} > 1+(n+1)x$

Proof: By mathematical induction

Let $A(n)$ be the statement $(1+x)^{n+1} > 1+(n+1)x$.

I will prove: $\forall n\, A(n)$.

Step 1: Prove $A(1)$

$A(1)$ is the statement $(1+x)^2 > 1+2x$ True!

True by binomial theorem,

$(1+x)^2 = 1+2x+x^2 > 1+2x$ (since $x^2 > 0$)

Step 2 (induction step):

Prove: $\forall n\, [A(n) \Rightarrow A(n+1)]$

(we pick an arbitrary n and prove $A(n) \Rightarrow A(n+1)$

$\therefore$ we assume antecedent and deduce a consequence.

∴ we assume $A(n)$ and deduce $A(n+1)$

$(1+x)^{n+1} > 1+(n+1)x$

"Assuming this"

$(1+x)^{n+2} > 1+(n+2)x$

"and deducing this"

(Concentrate on this one)

$\therefore (1+x)^{n+2} = (1+x)(1+x)^{n+1}$ ↓ Pull out (refactor)

$> (1+x)[1+(n+1)x]$

$= 1+(n+1)x+x+(n+1)x^2$

$= 1+(n+2)x+(n+1)x^2 >$

$1+(n+2)x$

this proves $A(n+1)$

Induction Summary.

(1) You want to prove that some statement $A(n)$ is valid for all natural numbers n.

(2) First proof $A(1)$. Usually matter of simple observation

(3) Give an algebraic argument to establish the conditional $A(n) \Rightarrow A(n+1)$

– reduce $A(n+1)$ to a form where you can use $A(n)$

(4) Conclusion: By principle of Math Induction, this proves $\forall n\, A(n)$ ⟹ □ ✓

Another variant [Common] of Induction.

We sometimes need proof a statement of form $(\forall n \geq n_0) A(n)$

– where n_0 is some fixed number e.g. 5.

In this case, the first step is to verify $A(n_0)$

$A(1)$ may not be true

(Where you $\neq n_0$, the first occurrence $A(1)$ is normally not true, we have told some other natural number as starting point)

$\Rightarrow$ general induction start at 1, But this variant starts at some point beyond 1. (otherwise not, the argument is the same)

Now the induction step is to prove:

$$(\forall n \geq n_0)[A(n) \Rightarrow A(n+1)]$$

This induction is part of famous Induction lecture called: "The fundamental theorem of arithmetic"

But lets first look at Quiz.

"Idea" Is 1 a prime number?

$\Rightarrow$ it is not a prime number, bec of definition:

1) must be positive
2) greater than 1
3) and exact divisors are 1 and n.

Another definition:

0 is not a natural number,
it's an integer, but ↑

⇒ natural number are Counting number

Fundamental Theorem of arithmetic to be proved:

Theorem: Every natural number greater than 1 is either prime or a product of primes.

[use variant of induction here (nat n=1) n=2,7]

Proof: By induction

The induction Statement, A(n) is:

$\forall m [2 \leq m \leq n \Rightarrow m$ is either a prime or product of primes$]$

For $n=2$, A(2) says:

"2 is either prime or a product of primes" [True]

Assume: $A(n)$, & deduce $A(n+1)$

Let m be natural number, $2 \leq m \leq n+1$

If $m \leq n$, then by $A(n)$, m is either prime product of primes

If $m = n+1$, and if $n+1$ is prime, then m is prime

If $m = n+1$ and $n+1$ is not prime, then (then we can find two smaller nubers whose product is $n+1$)

there are natural numbers p, q such that $1 \leq p, q \leq n+1$ and $n+1 = pq$.

Since $2 \leq p, q \leq n$, by $A(n)$, p, q are either prime or product of primes.

Hence $n+1$ is a product of primes.

The theorem follows by induction.

$\longrightarrow$