Existential quantification

Existential statements are of the form

> **there exists** an individual x in the universe of discourse for which the property $P(x)$ holds

or, in other words,

> **for some** individual x in the universe of discourse, the property $P(x)$ holds

or, in symbols,

$$\boxed{\exists x.\, P(x)}$$

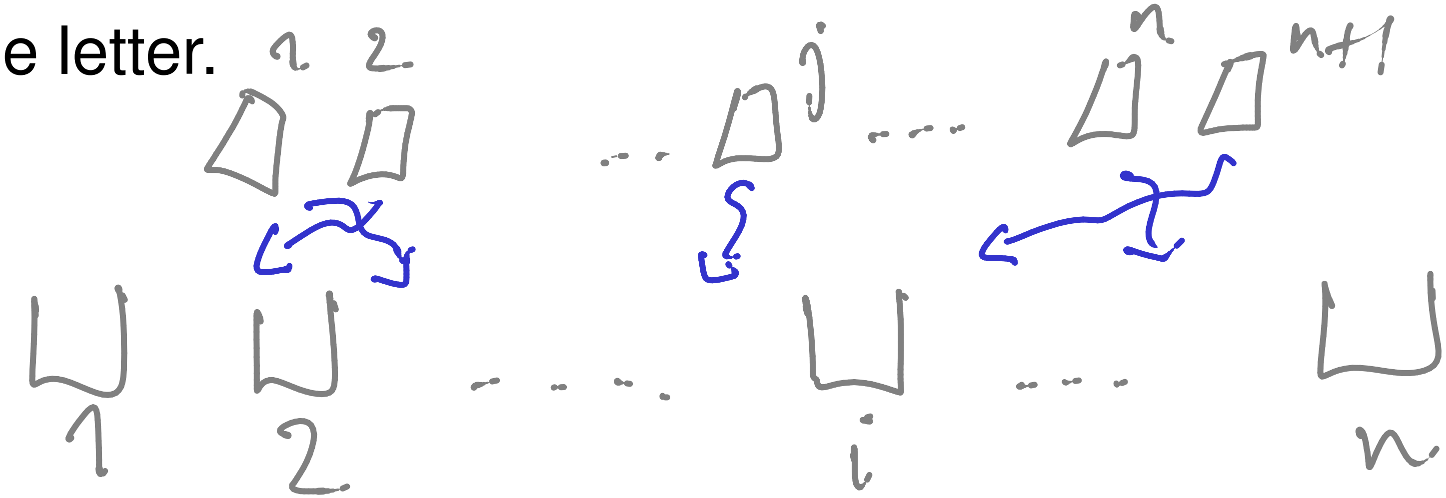
the same as $\exists y.\, P(y)$, $\exists z.\, P(z)$, etc.

$\forall$ pos. int. n

$\left(\begin{array}{l} n+1 \text{ letters in } n \\ \text{pigeonholes, say } 1, 2, \ldots, n \end{array} \right) \Longrightarrow \left(\exists\, 1 \le i \le n.\ \begin{array}{l} i^{\text{th}} \text{ pigeonhole} \\ \text{has more} \\ \text{than} \\ \text{one letter} \end{array} \right)$

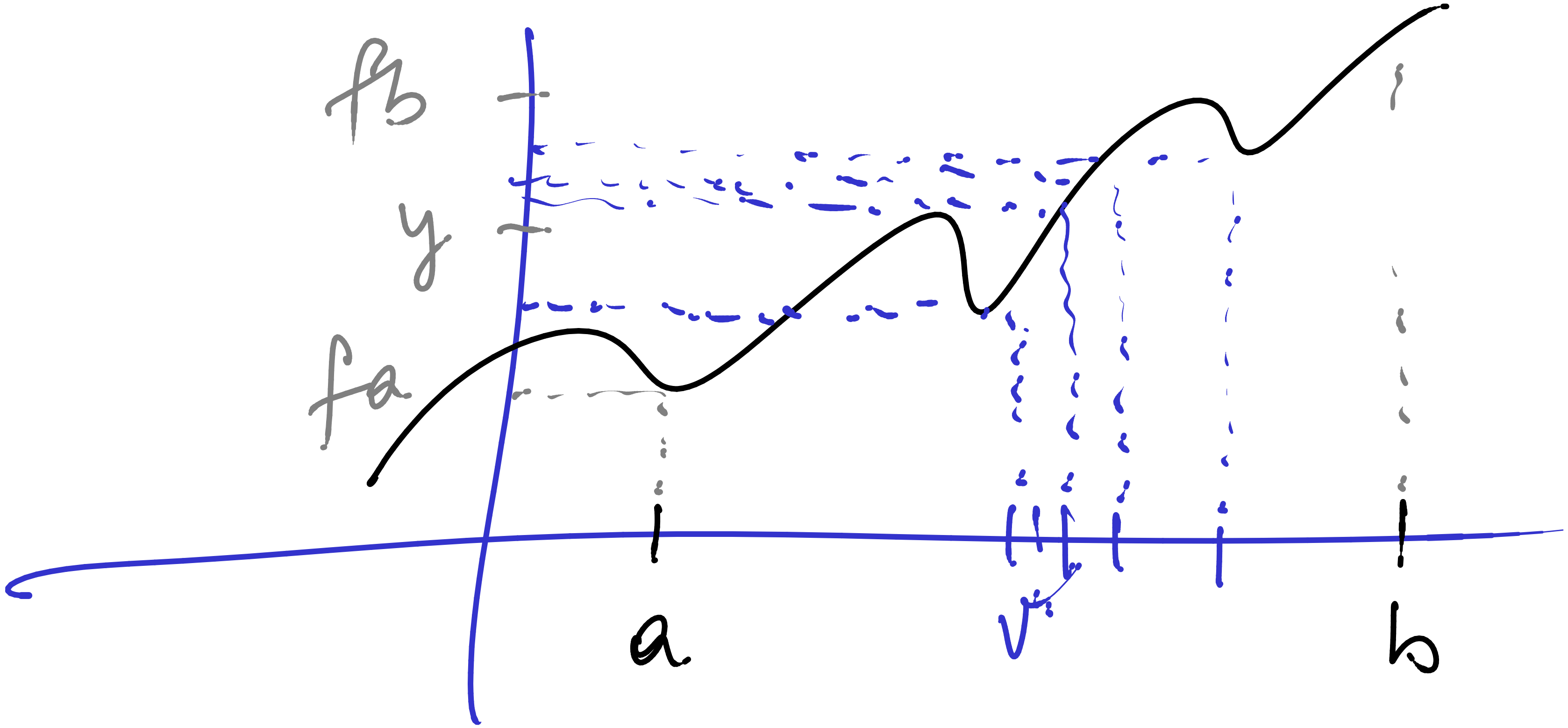
Example: The Pigeonhole Principle.

Let n be a positive integer. If $n+1$ letters are put in n pigeonholes then there will be a pigeonhole with more than one letter.



Theorem 21 (Intermediate value theorem) *Let f be a real-valued continuous function on an interval $[a, b]$. For every y in between $f(a)$ and $f(b)$, there exists v in between a and b such that $f(v) = y$.*

Intuition:



The main proof strategy for existential statements:

To prove a goal of the form

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

find a ***witness*** for the existential statement; that is, a value of x, say w, for which you think $P(x)$ will be true, and show that indeed $P(w)$, i.e. the predicate $P(x)$ instantiated with the value w, holds.

Proof pattern:

In order to prove

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

1. Write: $\text{Let } w = \ldots$ (the witness you decided on).
2. Provide a proof of $P(w)$.

Scratch work:

Before using the strategy

Assumptions	Goal
	$\exists x.\, P(x)$
$\vdots$	

After using the strategy

Assumptions	Goals
	$P(w)$
$\vdots$	

$w = \ldots$ (the witness you decided on)

Proposition 22 *For every positive integer* k, *there exist natural numbers* i *and* j *such that* $4 \cdot k = i^2 - j^2$.

PROOF:

$\forall$ pos. int k. $\exists$ i nat. $\exists$ j nat.

$$4 \cdot k = i^2 - j^2.$$

$4k$	k	w	w^2	v	v^2
4	1	$\boxed{2}$	4	$\boxed{0}$	0
8	2	$\boxed{3}$	9	$\boxed{1}$	1
12	3	$\boxed{4}$		$\boxed{2}$	
16	4				

Assume k is an arbitrary pos. int.

RTP: Find w a nat, find v a nat.

RTP: $4k = w^2 - v^2$.

$\underbrace{k+1}_{}$ $\underbrace{k-1}_{}$

witnesses.

Assumptions

Goal

G

... y, ... z ...

$\exists x. P(x)$

$P(x_0)$

The use of existential statements:

To use an assumption of the form $\exists x.\, P(x)$, introduce a new variable x_0 into the proof to stand for some individual for which the property $P(x)$ holds. This means that you can now assume $P(x_0)$ true.

for a new/fresh x_0

NB: $a \mid b \stackrel{\text{def}}{=} \exists \text{ int } d.\ a d = b$.

Theorem 24 *For all integers* l, m, n, *if* $l \mid m$ *and* $m \mid n$ *then* $l \mid n$.

PROOF: $\forall \text{ int. } l, m, n.$

$$(l \mid m \wedge m \mid n) \Rightarrow l \mid n$$

Equiv. $\forall \text{ int. } l, m, n.$

$$\big[(\exists i.\ i l = m) \wedge (\exists j.\ j m = n) \big] \Rightarrow (\exists k.\ k l = n)$$

Let l, m, n be int.

Assume (1) $(\exists i.\ i l = m)$ and (2) $(\exists j.\ j m = n)$

RTP. $\exists k.\ k l = n$

RTD: Find w s.t. $w \cdot l = n$

By (1) consider u s.t. $u \cdot l = m$

By ② consider v s.t. $v \cdot m = n$

Note that $u \cdot l = m$ so $u \cdot l \cdot v = v \cdot m = n$

Hence $w = u \cdot l$ satisfies $w \cdot l = n$. $\boxtimes$

Unique existence

unique

The notation

$$\exists!\, x.\, P(x)$$

stands for

the *unique existence* of an x for which the property $P(x)$ holds .

existence

That is,

$$\exists x.\, P(x) \;\wedge\; \Big(\forall y.\, \forall z.\, \big(P(y) \wedge P(z)\big) \implies y = z\Big)$$

uniqueness.

Disjunction

Disjunctive statements are of the form

$$\boxed{P \text{ or } Q}$$

or, in other words,

$$\boxed{\text{either } P,\ Q, \text{ or both hold}}$$

or, in symbols,

$$\boxed{P \vee Q}$$

The main proof strategy for disjunction:

To prove a goal of the form

$$P \vee Q$$

you may

1. try to prove P (if you succeed, then you are done); or
2. try to prove Q (if you succeed, then you are done); otherwise
3. break your proof into cases; proving, in each case, either P or Q.

Proposition 25 *For all integers* n*, either* $n^2 \equiv 0 \pmod 4$ *or* $n^2 \equiv 1 \pmod 4$.

PROOF: $\forall$ int n. $(n^2 \equiv 0 \pmod 4) \vee (n^2 \equiv 1 \pmod 4)$

Consider arbitrary n an integer.

① We try to show $n^2 \equiv 0 \pmod 4$ — we cannot!

② We try to show $n^2 \equiv 1 \pmod 4$ — we cannot!

③ We break the proof in cases aiming at establishing either disjunct.

We look at two case:

(i) n is even, that is of the form $2i$ for an int i

So $n^2 = (2i)^2 = 4i^2$ and we are done.

as $n^2 \equiv 0 \pmod 4$

(ii) n is odd, that is, $n = 2j+1$ for some int j.

So $n^2 = (2j+1)^2 = 4j^2 + 4j + 1$

$= 4(j^2+j)+1$

Hence $n^2 - 1 = 4(j^2+j)$ and so $4 \mid n^2 - 1$

That is $n^2 \equiv 1 \pmod 4$.

Assumptions

$P_1 \vee P_2$

Goal

Q

The use of disjunction:

To use a disjunctive assumption

$$P_1 \lor P_2$$

to establish a goal Q, consider the following two cases in turn: (i) assume P_1 to establish Q, and (ii) assume P_2 to establish Q.

Scratch work:

Before using the strategy

Assumptions	Goal
	Q
$\vdots$	
$P_1 \vee P_2$	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	Q		Q
$\vdots$		$\vdots$	
P_1		P_2	

Proof pattern:

In order to prove Q from some assumptions amongst which there is

$$P_1 \vee P_2$$

write: We prove the following two cases in turn: (i) that assuming P_1, we have Q; and (ii) that assuming P_2, we have Q. Case (i): Assume P_1. and provide a proof of Q from it and the other assumptions. Case (ii): Assume P_2. and provide a proof of Q from it and the other assumptions.