# Existential quantifications

- How to *prove* them as goals.
- How to *use* them as assumptions.

# 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,

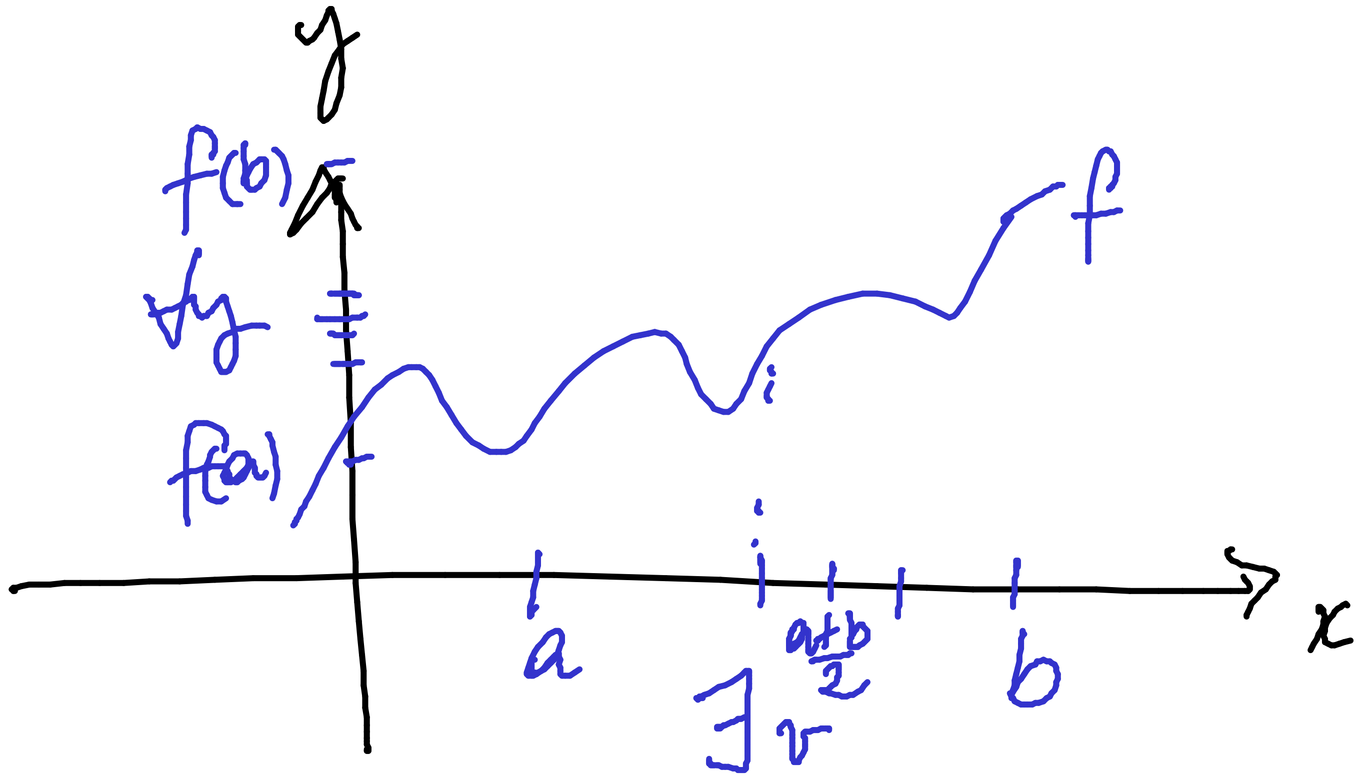
$$\boxed{\exists x.\, P(x)}$$

**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 20 (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:**



NB $\exists x. P(x) \equiv \exists y. P(y)$

**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 21** *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. $k$. $\exists$ nat. numbers $i, j$.

$$4k = i^2 - j^2$$

Let $k$ be an arbitrary positive integer.

Let $i_0$ be $k+1$

Let $j_0$ be $k-1$

RTP: $4k = i_0^2 - j_0^2$

$= (k+1)^2 - (k-1)^2$

$= \cdots$

| $k$ | $4k$ | $i$ | $j$ | $i^2 - j^2$ |
|---|---|---|---|---|
| 1 | 4 | 2 | 0 | 4 |
| 2 | 8 | 3 | 1 | 8 |
| 3 | 12 | 4 | 2 | 12 |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ |

Assumptions

$\vdots$

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

$\vdots$

let $x_0$ be such that $P(x_0)$

$\vdots$

Goal

$Q$

**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.

**Theorem 23** *For all integers* $l$, $m$, $n$, *if* $l \mid m$ *and* $m \mid n$ *then* $l \mid n$.

PROOF: Let $l, m, n$ be integers.

Assume $l \mid m \overset{①}{\iff} \exists i.\ l i = m$

$m \mid n \overset{②}{\iff} \exists j.\ m j = n$

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

By ①, let $i_0$ be such that $l \cdot i_0 = m$

By ②, let $j_0$ be such that $m \cdot j_0 = n$

Consider $k_0 = i_0 \cdot j_0$.

$l \cdot i_0 \cdot j_0 = m \cdot j_0 = n$

Then, $l \cdot k_0 = n$ and we are done.

$\boxtimes$

# Unique existence

The notation

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

stands for

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

That is,

$$\underbrace{\exists x.\, P(x)}_{\text{existence}} \;\wedge\; \underbrace{\Big(\forall y.\, \forall z.\, \big(P(y) \wedge P(z)\big) \implies y = z\Big)}_{\text{uniqueness.}}$$

**Example:** The congruence property modulo $m$ uniquely characterises the natural numbers from $0$ to $m-1$.

**Proposition 24** *Let $m$ be a positive integer and let $n$ be an integer.*

*Define*

$$P(z) = [0 \leq z < m \wedge z \equiv n \pmod m] \ .$$

*Then* Let m be a positive integer, let n be an integer

$$\forall x, y. P(x) \wedge P(y) \implies x = y \ .$$

PROOF: Let $x$ and $y$ be arbitrary.

Assume ① $0 \leq x < m$ and $x \equiv n \pmod m$

② $0 \leq y < m$ and $y \equiv n \pmod m$

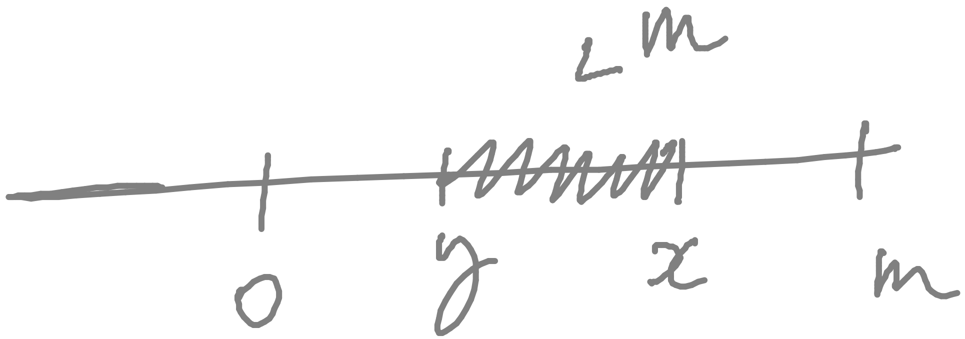
RTP: $x = y$

$$x \equiv y \pmod{m}$$

$0 \le x < m$

$0 \le y < m$

$x - y = km$ for some $k$.




Then, $x \ge y$,

$0 \le x - y < m$

So

$$0 \le km < m$$

thus $k = 0$.

Analogously, $y \ge x$, ...

$\boxtimes$

## A proof strategy

To prove

$$\forall\, x.\, \exists!\, y.\, P(x, y) \quad ,$$

for an arbitrary $x$ construct the unique witness and name it, say as $f(x)$, showing that

$$P\big(x, f(x)\big)$$

and

$$\forall\, y.\, P(x, y) \implies y = f(x)$$

hold.

## Disjunctions

- How to *prove* them as goals.
- How to *use* them as assumptions.

# 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: Let $n$ be an integer.

RTP: $n^2 \equiv 0 \pmod 4$ ∨ $n^2 \equiv 1 \pmod 4$.

$\boxed{?}$ $n^2 \equiv 0 \pmod 4$ ?

$n=0$ ✓

$n=1$ ✗

$\boxed{?}$ $n^2 \equiv 1 \pmod 4$

$n=0$ ✗

$n = \ldots -2, -1, 0, 1, 2, \ldots$

$\ldots\ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ldots$ $n^2$ modulo 4

Consider 2 cases

(1) let $n = 2i$ for an integer $i$.

Then $n^2 = 4i^2 \equiv 0 \pmod 4$

(2) let $n = 2i+1$ for an integer $i$

Then $n^2 = (2i+1)^2 = 4i^2 + 4i + 1$

$$= 4(i^2+i) + 1 \equiv 1 \pmod 4$$

In both cases, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$ hold.

$\boxtimes$

Assumptions

$\vdots$

$P_1 \vee P_2$

$\vdots$

Goal

$Q$

**The use of disjunction:**

To use a disjunctive assumption

$$P_1 \vee P_2$$

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.

# A little arithmetic

**Lemma 27** *For all positive integers* $p$ *and natural numbers* $m$, *if* $m = 0$ *or* $m = p$ *then* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF: Let p be a pos. int. and m a nat. number

Assume $m = 0 \vee m = p$

$$C^p_m = \binom{p}{m} = \frac{p!}{m!\,(p-m)!}$$

RTP: $\binom{p}{m} \equiv 1 \pmod{p}$

Consider $m = 0$. Then $\binom{p}{0} = 1$ and we are done.

Consider $m = p$. Then $\binom{p}{p} = 1$ and we are done. $\boxtimes$