Conjunctions

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

Conjunction

Conjunctive statements are of the form

$$\boxed{\mathrm{P}\ \textbf{and}\ \mathrm{Q}}$$

or, in other words,

$$\boxed{\text{both } \mathrm{P} \text{ and also } \mathrm{Q} \text{ hold}}$$

or, in symbols,

$$\boxed{\mathrm{P} \wedge \mathrm{Q}} \qquad \text{or} \qquad \boxed{\mathrm{P}\ \&\ \mathrm{Q}}$$

The proof strategy for conjunction:

To prove a goal of the form

$$P \wedge Q$$

first prove P and subsequently prove Q (or vice versa).

Proof pattern:

In order to prove

$$P \wedge Q$$

1. Write: Firstly, we prove P. and provide a proof of P.
2. Write: Secondly, we prove Q. and provide a proof of Q.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \wedge Q$
$\vdots$	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	P		Q
$\vdots$		$\vdots$	

The use of conjunctions:

To use an assumption of the form $P \wedge Q$,
treat it as two separate assumptions: P and Q.

$P \Leftrightarrow Q =_{\text{def}} (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

Theorem 19 *For every integer* n, *we have that* $6 \mid n$ *iff* $2 \mid n$ *and* $3 \mid n$.

PROOF: $\forall$ int n. $6 | n \Leftrightarrow (2|n \wedge 3|n)$.

Let n be an arbitrary integer.

RTP: $6|n \Leftrightarrow (2|n \wedge 3|n)$.

($\Rightarrow$) RTP: $6|n \Rightarrow (2|n \wedge 3|n)$

Assume $6|n$; i.e. $n = 6k$ for some int k, (1)

RTP: $2|n \wedge 3|n$

RTP: $2|n$; ie $n = 2i$ for an int i.

By (1) $n = 6k = 2(3k)$ and we are done.

RTP: $3|n$

By (1) $n = 6k = 3(2k)$ and so $3|n$.

($\Leftarrow$) RTP: $(2|n \wedge 3|n) \Rightarrow 6|n$

$n = 2i$
$n = 3j$
$\Rightarrow 2i = 3j$
$i = \frac{3j}{2}$

Assume: $2|n \wedge 3|n$

RTP: $6|n$

Assuming (1) $2|n$ and (2) $3|n$ we need show $6|n$.

By (1), $n = 2i$ for an int i
By (2), $n = 3j$ for an int j.

RTP: $n \stackrel{?}{=} 6k$ for an int. k.

$n \stackrel{?}{=} 2.3.k$

$k = p + q$

$= 2.3(p+q) = 2.3p + 2.3q \ldots$

$$\begin{array}{rl} & 3n = 6i \\ - & 2n = 6j \\ \hline & n = 6i - 6j \\ & \quad = 6(i-j) \end{array}$$

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,

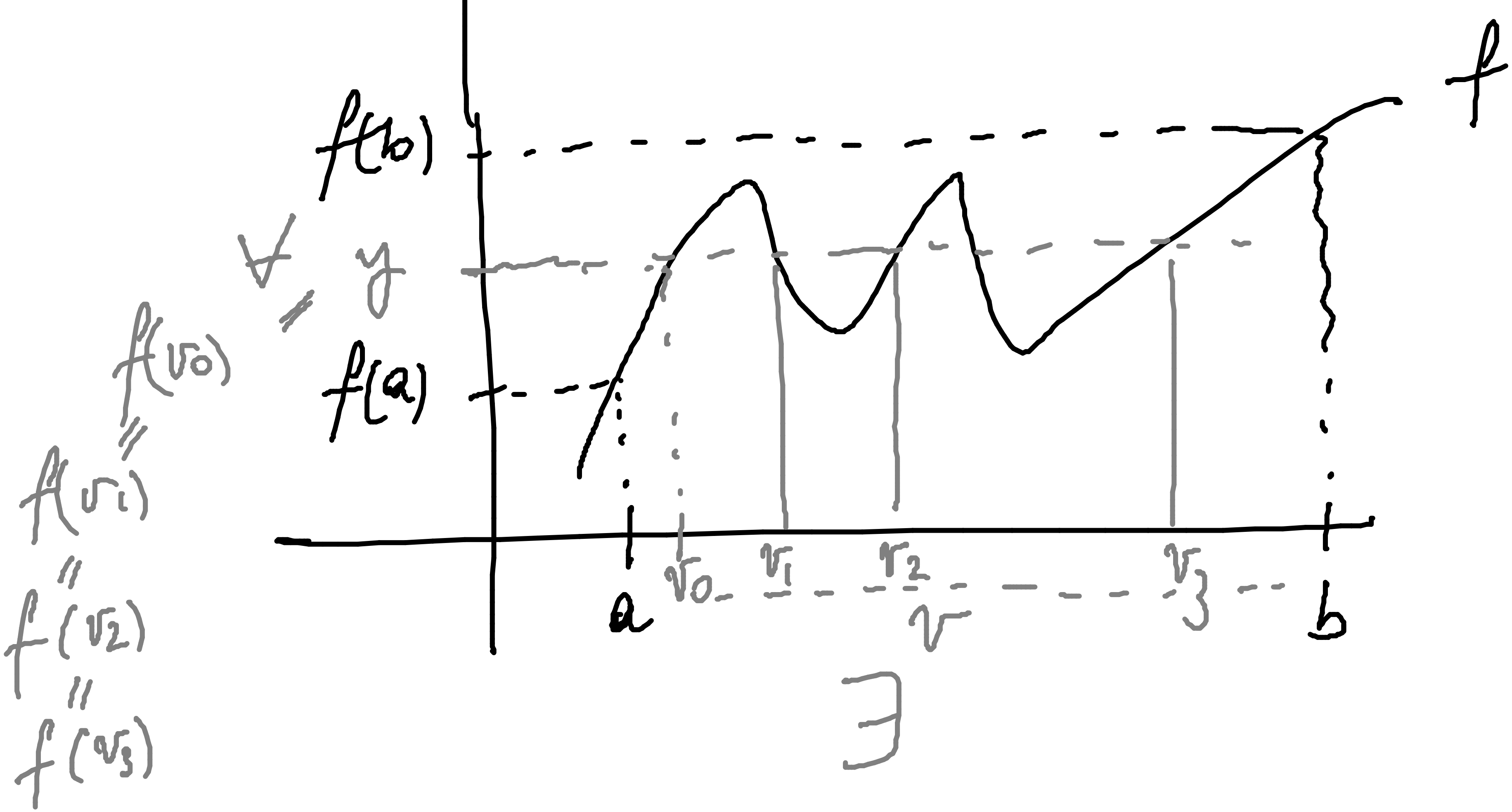
$$\boxed{\exists x.\, P(x)}$$

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:



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: 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. i and j. $4k = i^2 - j^2$.

1 Let k be an arbitrary positive integer.

RTP: $\exists$ nat. i and j. $4k = i^2 - j^2$.

Let $i = \ldots k \ldots$ and $j = \ldots k \ldots$

Show $i^2 - j^2 = (\ldots k \ldots)^2 - (\ldots k \ldots)^2 = \ldots = 4k$

$4k = 2 . 2k$ $\qquad$ $i^2 - j^2 = (i+j)(i-j) = 2 \cdot 2k$

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

k	$4k$	i	j	$i^2 - j^2$
1	4	2	0	
2	8	3	1	
3	12	$\boxed{4}$	$\boxed{2}$	✓
⋮	⋮			

guess: $k+1$ $k-1$

Let $i = k+1$ and $j = k-1$.

Then $i^2 - j^2 = (k+1)^2 - (k-1)^2 = \cdots = 4k$.

$\boxtimes$

Assumptions

$\vdots$

$\exists x. P(x)$

$\vdots$

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.

Assume x_0 is such that $P(x_0)$.

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

PROOF: $\forall \text{int. } l, m, n.\ (l \mid m \wedge m \mid n) \Rightarrow l \mid n$

1 Let l, m, n be arbitrary integers.

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

Assume: $l \mid m \wedge m \mid n$

That is, equivalently, 2 $l \mid m$ and 3 $m \mid n$.

Namely, 2 $\boxed{\exists \text{ int } i.\ m = l i}$ and 3 $\boxed{\exists \text{ int } j.\ n = m j}$

RTP $l \mid n$; That is, $\exists \text{ int. } k.\ n = l k$

By 2, we have int i_0 s.t. $m = l \cdot i_0$

By 3, we have int j_0 s.t. $n = m \cdot j_0$

Let $k = i_0 \cdot j_0$. Then,

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

$\boxtimes$

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,

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

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

$$P(z) = [\, 0 \leq z < m \;\wedge\; z \equiv n \pmod{m} \,] \quad .$$

Then

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

PROOF:

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.