Proof by contradiction

Theorem

If x^2 is even, then x is even ($x \in \mathbb{Z}$).

Proof

Let $x \in \mathbb{Z}$

Assume x^2 is even.

Assume that x is odd.

Then $x = 2y+1$ for some $y \in \mathbb{Z}$.

Then $x^2 = (2y+1)^2 = 4y^2 + 4y + 1 = 2(2y^2 + 2y) + 1$ and $2y^2 + 2y \in \mathbb{Z}$.

So, x^2 is odd

a contradiction.

So, x is even

(sub)goal

generating hypothesis

pure hypothesis

conclusion

Thanks to Bas Luttik

Proof by contradiction

How do we prove P by a contradiction?

$\neg P \Rightarrow F \overset{val}{\models} \neg\neg P \overset{val}{\models} P$

¬-intro

¬¬-elim

proof by contradiction

{Assume}

(k) $\boxed{\neg P}$

…

(l-1) F

{¬-intro on (k) and (l-1)}

(l) ¬¬P

{¬¬-elim on (l)}

(l+1) P

(k < m)

time for an example!

Disjunction introduction

How do we prove a disjunction?

$\neg P \Rightarrow Q \overset{val}{\vDash} P \vee Q$

$\neg Q \Rightarrow P \overset{val}{\vDash} P \vee Q$

$\vee$-introduction

$\Rightarrow$-intro

...
{Assume}
(k) $\boxed{\neg P}$

...

(l-1) Q
{$\vee$-intro on (k) and (l-1)}
(l) $P \vee Q$

Disjunction introduction

How do we prove a disjunction?

$\neg P \Rightarrow Q \overset{val}{\models} P \vee Q$

$\neg Q \Rightarrow P \overset{val}{\models} P \vee Q$

$\vee$-introduction

$\Rightarrow$-intro

...

{Assume}

(k) $\boxed{\neg Q}$

...

(l-1) P

{$\vee$-intro on (k) and (l-1)}

(l) $P \vee Q$

Disjunction elimination

How do we use a disjunction in a proof?

$P \vee Q \overset{val}{\models} \neg P \Rightarrow Q$

$P \vee Q \overset{val}{\models} \neg Q \Rightarrow P$

$\vee$-elimination

|| ||

(k) $P \vee Q$

|| ||

{$\vee$-elim on (k)}

(m) $\neg P \Rightarrow Q$

(k < m)

Disjunction elimination

How do we use a disjunction in a proof?

$P \vee Q \overset{val}{\models} \neg P \Rightarrow Q$

$P \vee Q \overset{val}{\models} \neg Q \Rightarrow P$

$\vee$-elimination

||||

(k) $P \vee Q$

||||

{$\vee$-elim on (k)}

(m) $\neg Q \Rightarrow P$

(k < m)

Proof by case distinction

How do we prove R by a case distinction?

$(P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow R) \overset{val}{\vDash} R$

proof by case distinction

|| ||

(k) $P \vee Q$

|| ||

(l) $P \Rightarrow R$

|| ||

(m) $Q \Rightarrow R$

|| ||

{case-dist on (k), (l), (m)}

(n) R

(k < n, l< n, m<n)

Bi-implication introduction

How do we prove a bi-implication?

$(P \Rightarrow Q) \wedge (Q \Rightarrow P) \overset{val}{\models} P \Leftrightarrow Q$

⇔-introduction

$\cdots$

(k) $P \Rightarrow Q$

$\cdots$

(l) $Q \Rightarrow P$

$\cdots$

{⇔-intro on (k) and (l)}

(m) $P \Leftrightarrow Q$

($k < m, l < m$)

∧-intro

Bi-implication elimination

How do we use a bi-implication in a proof?

$P \Leftrightarrow Q \overset{val}{\models} (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

$\Leftrightarrow$-elimination

	$\vdots$
(k)	$P \Leftrightarrow Q$
	$\vdots$
	{$\Leftrightarrow$-elim on (k)}
(m)	$P \Rightarrow Q$

(k < m)

	$\vdots$
(k)	$P \Leftrightarrow Q$
	$\vdots$
	{$\Leftrightarrow$-elim on (k)}
(m)	$Q \Rightarrow P$

(k < m)

$\wedge$-elim

Derivations / Reasoning with quantifiers

Proving a universal quantification

To prove

$\forall x[x \in \mathbb{Z} \wedge x \geq 2 : x^2 - 2x \geq 0]$

Proof

Let $x \in \mathbb{Z}$ be arbitrary and assume that $x \geq 2$.

Then, for this particular x, it holds that

$$x^2 - 2x = x(x-2) \geq 0 \quad \text{(Why?)}$$

Conclusion: $\forall x[x \in \mathbb{Z} \wedge x \geq 2 : x^2 - 2x \geq 0]$.

∀ introduction

How do we prove a universal quantification?

similar to
⇒-intro

with
generating
hypothesis

∀-introduction

...
{Assume}
(k) $\boxed{\textbf{var } x; P(x)}$

...

(l-1) Q(x)
{∀-intro on (k) and (l-1)}
(l) ∀x[P(x) : Q(x)]

flag shows the validity of a hypothesis

Using a universal quantification

We know $\forall x[x \in \mathbb{Z} \land x \geq 2 : x^2 - 2x \geq 0]$

Whenever we encounter an $a \in \mathbb{Z}$ such that $a \geq 2$,

we can conclude that $a^2 - 2a \geq 0$.

For example, $(52387^2 - 2 \cdot 52387) \geq 0$
since $52387 \in \mathbb{Z}$ and $52387 \geq 2$.

∀ elimination

How do we use a universal quantification in a proof?

similar to implication but we need a witness

∀-elimination

	|| ||
(k)	$\forall x[P(x) : Q(x)]$
	|| ||
(l)	$P(a)$
	|| ||
	{∀-elim on (k) and (l)}
(m)	$Q(a)$

$(k < m, l < m)$

a is an object (variable, number,..) which is "known" in line (l)

the same "a" from line (l)

time for an example!

∃ introduction

How do we prove an existential quantification?

$\neg \forall x[P(x) : \neg Q(x)] \overset{val}{\models} \exists x\, [P(x) : Q(x)]$

∃-introduction

$\ldots$

{Assume}

(k) $\boxed{\forall x[P(x) : \neg Q(x)]}$

$\ldots$

(l-1) F

{∃-intro on (k) and (l-1)}

(l) $\exists x\, [P(x) : Q(x)]$

and ¬-intro

∃ elimination

How do we use an existential quantification in a proof?

$\exists x\ [P(x) : Q(x)] \stackrel{val}{\models} \neg\ \forall x[P(x) : \neg Q(x)]$

∃-elimination

|| ||

(k) $\exists x\ [P(x) : Q(x)]$

|| ||

(l) $\forall x[P(x) : \neg Q(x)]$

|| ||

{∃-elim on (k) and (l)}

(m) F

($k < m, l < m$)

and ¬-elimination

time for an example!

Proofs with ∃-introduction and ∃-elimination are unnecessarily long and cumbersome…

There are alternatives!

Proving an existential quantification

To prove

$\exists x[x \in \mathbb{Z} : x^3 - 2x - 8 \geq 0]$

Proof

It suffices to find a witness, i.e., an $x \in \mathbb{Z}$ satisfying

$$x^3 - 2x - 8 \geq 0.$$

$x = 3$ is a witness, since $3 \in \mathbb{Z}$ and $3^3 - 2 \cdot 3 - 8 = 13 \geq 0$

Conclusion: $\exists x[x \in \mathbb{Z} : x^3 - 2x - 8 \geq 0]$.

also x = 5 is a witness…

Alternative ∃ introduction

How do we prove an existential quantification?

by finding
a witness

∃

	...
(k)	$P(a)$
	...
(l)	$Q(a)$
	...
	{∃∗-intro on (k) and (l)}
(m)	$\exists x\,[P(x) : Q(x)]$

strategy: wait until a witness object appears

does not always work

$(k < m, l < m)$

Using an existential quantification

We know $\exists x[x \in \mathbb{R} : a - x < 0 < b - x]$

We can declare an $x \in \mathbb{Z}$ (a witness) such that

$$a - x < 0 < b - x$$

and use it further in the proof. For example:

From $a - x < 0$, we get $a < x$.

From $b - x > 0$, we get $x < b$.

Hence, $a < b$.

Alternative ∃ elimination

How do we use an existential quantification in a proof?

we pick a witness

∃

|| ||

(k) ∃x [P(x) : Q(x)]

x must be new!

|| ||

{∃*-elim on (k)}

(m) Pick x with P(x) and Q(x)

time for an example!

(k < m)