Derivations / Reasoning

Limitations of proofs by calculation

Proofs by calculation are formal and well-structured, but often undirected and not particularly intuitive.

Example

$$
\begin{aligned}
P \wedge (P \vee Q) &\overset{val}{=} (P \vee F) \wedge (P \vee Q) \\
&\overset{val}{=} P \vee (F \wedge Q) \\
&\overset{val}{=} P \vee F \\
&\overset{val}{=} P
\end{aligned}
$$

we can prove this more intuitively by reasoning

Conclusions

$P \wedge (P \vee Q) \overset{val}{=} P$ $\quad$ $P \wedge (P \vee Q) \Leftrightarrow P \overset{val}{=} T$

An example of a mathematical proof

Theorem

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

Proof

Let $x \in \mathbb{Z}$ be such that x^2 is even.

We need to prove that x is even too.

Assume that x is odd, towards a contradiction.

If x is odd than $x = 2y+1$ 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 too, and we have a contradiction.

(sub)goal

generating hypothesis

pure hypothesis

conclusion

Thanks to Bas Luttik

Exposing logical structure

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

Single inference rule

Q is a correct conclusion from n premises $P_1, .., P_n$
iff
$(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \overset{val}{\models} Q$

If n=0, then $P_1 \wedge P_2 \wedge \ldots \wedge P_n \overset{val}{=} T$

Note that $T \models Q$ means that $Q \overset{val}{=} T$

Q holds unconditionally

Derivation

a formal system based on the single inference rule for proofs that closely follow our intuitive reasoning

Q is a correct conclusion from n premises $P_1, .., P_n$
iff
$(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \overset{val}{\models} Q$

Two types of inference rules:

(particularly useful) instances of the single inference rule

and one new special rule!

elimination rules

for drawing conclusions out of premises

introduction rules

for simplifying goals

Conjunction elimination

How do we use a conjunction in a proof?

$P \wedge Q \overset{val}{\vDash} P$

$P \wedge Q \overset{val}{\vDash} Q$

$\wedge$-elimination

	⁞
(k)	$P \wedge Q$
	⁞
	{$\wedge$-elim on (k)}
(m)	P

(k < m)

	⁞
(k)	$P \wedge Q$
	⁞
	{$\wedge$-elim on (k)}
(m)	Q

(k < m)

Implication elimination

How do we use an implication in a proof?

$P \Rightarrow Q \overset{val}{\models}$???

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

⇒-elimination

|| ||

(k) $P \Rightarrow Q$

|| ||

(l) P

|| ||

{⇒-elim on (k) and (l)}

(m) Q

$(k < m, l < m)$

Conjunction introduction

How do we prove a conjunction?

$P \wedge Q \overset{val}{\models} P \wedge Q$

$\wedge$-introduction

$\dots$

(k) P

$\dots$

(l) Q

$\dots$

$\{\wedge\text{-intro on (k) and (l)}\}$

(m) $P \wedge Q$

$(k < m, l < m)$

Implication introduction

How do we prove an implication?

truly new
and
necessary for
reasoning with
hypothesis

⇒-introduction

…
{Assume}
(k) $\boxed{P}$

…

(l-1) Q
{⇒-intro on (k) and (l-1)}
(l) P⇒Q

flag shows the validity of a hypothesis

time for an example!

Negation introduction

How do we prove a negation?

$\neg P \overset{\text{val}}{=} P \Rightarrow F$

⇒-intro

¬-introduction

$$
\begin{array}{ll}
 & \ldots \\
 & \{\text{Assume}\} \\
(k) & \boxed{P} \\
 & \ldots \\
(l-1) & F \\
 & \{\neg\text{-intro on } (k) \text{ and } (l-1)\} \\
(l) & \neg P
\end{array}
$$

Negation elimination

How do we use a negation in a proof?

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

¬-elimination

|| ||

(k) P

|| ||

(l) ¬P

|| ||

{¬-elim on (k) and (l)}

(m) F

$(k < m, l < m)$

time for an example!

F introduction

How do we prove F?

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

F-introduction

...

(k) P

...

(l) ¬P

...

{F-intro on (k) and (l)}

(m) F

the same as ¬-elim
only intended bottom-up

(k < m, l < m)

F elimination

How do we use F in a proof?

it's very useful!

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

F-elimination

$\vdots$

(k) F

$\vdots$

{F-elim on (k)}
(m) P

(k < m)

Double negation introduction

How do we prove ¬¬?

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

¬¬-introduction

…

(k) P

…

{¬¬-intro on (k)}

(m) $\neg\neg P$

(k < m)

Double negation elimination

How do we use ¬¬ in a proof?

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

¬¬-elimination

|| ||

(k) $\neg\neg P$

|| ||

{¬¬-elim on (k)}
(m) P

$(k < m)$

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?

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

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

$\vee$-introduction

...

{Assume}

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

...

(l-1) Q

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

(l) $P \vee Q$

$\Rightarrow$-intro

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) $P \vee Q$

$||\,||$

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

(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?

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

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

$\dots$

(k) $P \Rightarrow Q$

$\dots$

(l) $Q \Rightarrow P$

$\dots$

{⇔-intro on (k) and (l)}

(m) $P \Leftrightarrow Q$

$\wedge$-intro

(k < m, l < m)

Bi-implication elimination

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

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

⇔-elimination

|| ||

(k) $P \Leftrightarrow Q$

|| ||

{⇔-elim on (k)}

(m) $P \Rightarrow Q$

(k < m)

|| ||

(k) $P \Leftrightarrow Q$

|| ||

{⇔-elim on (k)}

(m) $Q \Rightarrow P$

(k < m)

∧-elim

Derivations / Reasoning with quantifiers

Proving a universal quantification

To prove

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

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

∀ introduction

How do we prove a universal quantification?

similar to
⇒-intro

with
generating
hypothesis

∀-introduction

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

flag shows the validity of a hypothesis

...

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

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) $Q(a)$

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

the same "a" from line (l)

time for an example!

$(k < m, l < m)$

∃ 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?

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

∃-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 $3^3 - 2 \cdot 3 - 8 = 13 \geq 0$

also $x = 5$ is a witness…

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

Alternative ∃ introduction

How do we prove an existential quantification?

by finding a witness

∃∗-introduction

$\ldots$

(k) P(a)

$\ldots$

(l) Q(a)

$\ldots$

{∃∗-intro on (k) and (l)}

(m) ∃x [P(x) : Q(x)]

(k < m, l < m)

strategy: wait until a witness object appears

does not always work

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

∃∗-elimination

|| ||

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

|| ||

{∃∗-elim on (k)}

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

x must be new!

time for an example!

(k < m)