

Derivations / Reasoning

Limitations of proofs by calculation

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

Example

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

we can prove this more intuitively by reasoning

Conclusions

$$P \wedge (P \vee Q) \stackrel{\text{val}}{=} P$$

$$P \wedge (P \vee Q) \Leftrightarrow P \stackrel{\text{val}}{=} T$$

An example of a mathematical proof

Theorem

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

(sub)goal

Proof

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

generating hypothesis

We need to prove that x is even too.

pure hypothesis

Assume that x is odd, towards a contradiction.

conclusion

If 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 too, and we have a contradiction.

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, \dots, P_n
iff
 $(P_1 \wedge P_2 \wedge \dots \wedge P_n) \models^{\text{val}} Q$

If $n=0$, then $P_1 \wedge P_2 \wedge \dots \wedge P_n \models^{\text{val}} T$

Note that $T \models^{\text{val}} Q$ means that $Q \models^{\text{val}} T$

Q holds
unconditionally

Derivation

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

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

Two types of inference rules:

elimination rules

for drawing
conclusions out of
premises

introduction rules

for simplifying goals

(particularly useful)
instances of the single
inference rule

and one new
special rule!

Conjunction elimination

How do we use a conjunction in a proof?

\wedge -elimination

$$P \wedge Q \stackrel{\text{val}}{=} P$$

$$P \wedge Q \stackrel{\text{val}}{=} Q$$

|| |

(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?

\Rightarrow -elimination

$\parallel \parallel$

(k) $P \Rightarrow Q$

$\parallel \parallel$

(l) P

$\parallel \parallel$
 $\{\Rightarrow\text{-elim on (k) and (l)}\}$

(m) Q

$(k < m, l < m)$

$P \Rightarrow Q \models^{\text{val}} ???$

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

Conjunction introduction

How do we prove a conjunction?

$$P \wedge Q \stackrel{\text{val}}{=} P \wedge Q$$

\wedge -introduction

...

(k) P

...

(l) Q

...

{ \wedge -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

\Rightarrow -introduction

...

{Assume}

(k) P

...

(l-1) Q

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

(l) $P \Rightarrow Q$

flag shows the validity of a hypothesis

time for an example!

Negation introduction

How do we prove a negation?

\neg -introduction

...

{Assume}

(k) P

...

(l-1) F

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

(l) $\neg P$

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

\Rightarrow -intro

Negation elimination

How do we use a negation in a proof?

\neg -elimination

	$\parallel \parallel$
(k)	P
	$\parallel \parallel$
(l)	$\neg P$
	$\parallel \parallel$
	{ \neg -elim on (k) and (l)}
(m)	F

$(k < m, l < m)$

$P \wedge \neg P \models^{\text{val}} F$

time for an
example!

F introduction

How do we prove F?

$$P \wedge \neg P \stackrel{\text{val}}{=} F$$

F-introduction

...

(k) P

...

(l) $\neg P$

...

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

(m) F

$(k < m, l < m)$

the same as \neg -elim
only intended bottom-up

F elimination

How do we use F in a proof?

it's very useful!

F-elimination

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

(k < m)

$F \stackrel{\text{val}}{=} P$

Double negation introduction

How do we prove $\neg\neg$?

$\neg\neg$ -introduction

...

(k) P

 ...

$\{\neg\neg\text{-intro on (k)}\}$

(m) $\neg\neg P$

$(k < m)$

$P \models^{\text{val}} \neg\neg P$

Double negation elimination

How do we use $\neg\neg$ in a proof?

$\neg\neg$ -elimination

$\parallel \parallel$
(k) $\neg\neg P$
 $\parallel \parallel$
 $\{\neg\neg\text{-elim on (k)}\}$
(m) P

$(k < m)$

$\neg\neg P \stackrel{\text{val}}{=} P$

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?

proof by
contradiction

	{Assume}
(k)	$\neg P$
	...
(l-1)	F { \neg -intro on (k) and (l-1)}
(l)	$\neg\neg P$ { $\neg\neg$ -elim on (l)}
(l+1)	P

(k < m)

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

\neg -intro

$\neg\neg$ -elim

time for an
example!

Disjunction introduction

How do we prove a disjunction?

$$\neg P \Rightarrow Q \stackrel{\text{val}}{=} P \vee Q$$

$$\neg Q \Rightarrow P \stackrel{\text{val}}{=} P \vee Q$$

\Rightarrow -intro

\vee -introduction

...

{Assume}

(k) $\neg P$

...

(l-1) Q

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

(l) $P \vee Q$

Disjunction introduction

How do we prove a disjunction?

$$\neg P \Rightarrow Q \stackrel{\text{val}}{=} P \vee Q$$

$$\neg Q \Rightarrow P \stackrel{\text{val}}{=} P \vee Q$$

\Rightarrow -intro

\vee -introduction

...

{Assume}

(k) $\neg Q$

...

(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?

v-elimination

|| ||
(k) $P \vee Q$
|| ||
{v-elim on (k)}
(m) $\neg P \Rightarrow Q$

$(k < m)$

$$P \vee Q \stackrel{\text{val}}{\models} \neg P \Rightarrow Q$$

$$P \vee Q \stackrel{\text{val}}{\models} \neg Q \Rightarrow P$$

Disjunction elimination

How do we use a disjunction in a proof?

v-elimination

|| ||

(k) $P \vee Q$

|| ||

{v-elim on (k)}

(m) $\neg Q \Rightarrow P$

(k < m)

$$P \vee Q \stackrel{\text{val}}{\models} \neg P \Rightarrow Q$$

$$P \vee Q \stackrel{\text{val}}{\models} \neg Q \Rightarrow P$$

Proof by case distinction

How do we prove R by a case distinction?

proof by
case distinction

|| ||
(k) $P \vee Q$

|| ||
(l) $P \Rightarrow R$

|| ||
(m) $Q \Rightarrow R$

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

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

$$(P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow R) \stackrel{\text{val}}{=} R$$

Bi-implication introduction

How do we prove a bi-implication?

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

\Leftrightarrow -introduction

...

(k) $P \Rightarrow Q$

...

(l) $Q \Rightarrow P$

...

{ \Leftrightarrow -intro on (k) and (l)}

(m) $P \Leftrightarrow Q$

$(k < m, l < m)$

\wedge -intro

Bi-implication elimination

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

\Leftrightarrow -elimination

$$P \Leftrightarrow Q \stackrel{\text{val}}{=} (P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

|| |
(k) $P \Leftrightarrow Q$

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

(k < m)

|| |
(k) $P \Leftrightarrow Q$

|| |
 $\{\Leftrightarrow\text{-elim on (k)}\}$
(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: $\forall x[x \in \mathbb{Z} \wedge x \geq 2 : x^2 - 2x \geq 0]$.

\forall introduction

How do we prove a universal quantification?

similar to
 \Rightarrow -intro
with
generating
hypothesis

\forall -introduction

...

{Assume}

(k) **var** x; P(x)

...

(l-1) Q(x)
{ \forall -intro on (k) and (l-1)}

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

flag shows the validity of a hypothesis

Using a universal quantification

We know

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

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 $52387 \geq 2$.

\forall elimination

How do we use a universal quantification in a proof?

similar to
implication
but we need
a witness

\forall -elimination

$\parallel \parallel$
(k) $\forall x[P(x) : Q(x)]$

$\parallel \parallel$
(l) $P(a)$

$\parallel \parallel$
 $\{\forall\text{-elim on (k) and (l)}\}$
(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!

$(k < m, l < m)$

\exists introduction

How do we prove an existential quantification?

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

\exists -introduction

...

{Assume}

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

...

(l-1) F

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

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

and \neg -intro

\exists elimination

How do we use an existential quantification in a proof?

\exists -elimination

$\parallel \parallel$

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

$\parallel \parallel$

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

$\parallel \parallel$
 $\{\exists\text{-elim on (k) and (l)}\}$

(m) F

$(k < m, l < m)$

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

and \neg -
elimination

time for an
example!