Domain splitting

Examples:

$$\forall_x[x \leqslant 1 \vee x \geqslant 5 \colon x^2 - 6x + 5 \geqslant 0]$$
$$\stackrel{val}{=} \forall_x[x \leqslant 1 \colon x^2 - 6x + 5 \geqslant 0] \wedge \forall_x[x \geqslant 5 \colon x^2 - 6x + 5 \geqslant 0]$$

$$\exists_k[0 \leqslant k \leqslant n : k^2 \leqslant 10]$$
$$\stackrel{val}{=} \exists_k[0 \leqslant k \leqslant n-1 \vee k = n : k^2 \leqslant 10]$$
$$\stackrel{val}{=} \exists_k[0 \leqslant k \leqslant n-1 : k^2 \leqslant 10] \vee \exists_k[k = n : k^2 \leqslant 10]$$

Domain splitting

$$\forall_x[P \vee Q : R] \stackrel{val}{=} \forall_x[P : R] \wedge \forall_x[Q : R]$$
$$\exists_x[P \vee Q : R] \stackrel{val}{=} \exists_x[P : R] \vee \exists_x[Q : R]$$

Equivalences with quantifiers

One-element domain

$$\forall_x[x = n : Q] \overset{val}{=} Q[n/x]$$

$$\exists_x[x = n : Q] \overset{val}{=} Q[n/x]$$

Example:

$$\forall_x[x = 3 : 2 \cdot x \geqslant 1] \overset{val}{=} 2 \cdot 3 \geqslant 1$$

Empty domain

$$\forall_x[F : Q] \overset{val}{=} T$$

$$\exists_x[F : Q] \overset{val}{=} F$$

"All Marsians are green"

Domain weakening

Intuition: The following are equivalent

$$\forall_x [x \in D : A(x)] \quad \text{and} \quad \forall_x [x \in D \Rightarrow A(x)]$$
$$\exists_x [x \in D : A(x)] \quad \text{and} \quad \exists_x [x \in D \wedge A(x)]$$

The same can be done to parts of the domain

Domain weakening

$$\forall_x [P \wedge Q : R] \stackrel{val}{=} \forall_x [P : Q \Rightarrow R]$$
$$\exists_x [P \wedge Q : R] \stackrel{val}{=} \exists_x [P : Q \wedge R]$$

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

De Morgan with quantifiers

De Morgan

$$\neg\forall_x[P:Q] \overset{val}{=} \exists_x[P:\neg Q]$$
$$\neg\exists_x[P:Q] \overset{val}{=} \forall_x[P:\neg Q]$$

not for all = at least for one not

not exists = for all not

Hence: $\neg\forall = \exists\neg$ and $\neg\exists = \forall\neg$

It holds further that:

$$\neg\forall_x\neg = \exists_x\neg\neg = \exists_x$$
$$\neg\exists_x\neg = \forall_x\neg\neg = \forall_x$$

Substitution

holds also for quantified formulas!

meta rule

Simple

$$\frac{\phi \overset{val}{=} \psi}{\phi[\xi/P] \overset{val}{=} \psi[\xi/P]}$$

EVERY occurrence of P is substituted!

Sequential

$$\frac{\phi \overset{val}{=} \psi}{\phi[\xi/P][\eta/Q] \overset{val}{=} \psi[\xi/P][\eta/Q]}$$

Simultaneous

$$\frac{\phi \overset{val}{=} \psi}{\phi[\xi/P, \eta/Q] \overset{val}{=} \psi[\xi/P, \eta/Q]}$$

The rule of Leibniz

holds also for quantified formulas!

meta rule

Leibniz

$$\frac{\phi \overset{val}{=} \psi}{C[\phi] \overset{val}{=} C[\psi]}$$

formula that has ϕ as a sub formula

single occurrence is replaced!

Other equivalences with quantifiers

Exchange trick

$$\forall_x[P{:}Q] \overset{val}{=} \forall_x[\neg Q{:}\neg P]$$

$$\exists_x[P{:}Q] \overset{val}{=} \exists_x[Q{:}P]$$

No wonder as

$$\forall_x[P{:}Q] \overset{val}{=} \forall_x[P \Rightarrow Q]$$

$$\exists_x[P{:}Q] \overset{val}{=} \exists_x[P \wedge Q]$$

Term splitting

$$\forall_x[P{:}Q \wedge R] \overset{val}{=} \forall_x[P{:}Q] \wedge \forall_x[P{:}R]$$

$$\exists_x[P{:}Q \vee R] \overset{val}{=} \exists_x[P{:}Q] \vee \exists_x[P{:}R]$$

Other equivalences with quantifiers

Monotonicity of quantifiers

$$\forall_x[P{:}Q \Rightarrow R] \Rightarrow (\forall_x[P{:}Q] \Rightarrow \forall_x[P{:}R]) \stackrel{val}{=} T$$

$$\forall_x[P{:}Q \Rightarrow R] \Rightarrow (\exists_x[P{:}Q] \Rightarrow \exists_x[P{:}R]) \stackrel{val}{=} T$$

tautologies

Lemma E1: $P \stackrel{val}{=} Q$ iff $P \Leftrightarrow Q$ is a tautology.

Lemma W4: $P \stackrel{val}{\models} Q$ iff $P \Rightarrow Q$ is a tautology.

still hold (in predicate logic)

Lemma W5: If $Q \stackrel{val}{\models} R$ then $\forall_x[P{:}Q] \stackrel{val}{\models} \forall_x[P{:}R]$.

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

elimination rules

for drawing conclusions out of premises

introduction rules

for simplifying goals

and one new special rule!

Conjunction elimination

How do we use a conjunction in a proof?

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

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

$\wedge$-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

$\ldots$

(k) $\quad P$

$\ldots$

(l) $\quad Q$

$\ldots$

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

(m) $\quad P \wedge Q$

$(k < m, l < m)$

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?

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

⇒-intro

¬-introduction

...

{Assume}

(k) $\boxed{P}$

...

(l-1) F

{¬-intro on (k) and (l-1)}

(l) ¬P

Negation elimination

How do we use a negation in a proof?

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

¬-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

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

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

||| |||

(k) F

||| |||

{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) ¬¬P

(k < m)

Double negation elimination

How do we use ¬¬ in a proof?

¬¬-elimination

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

|| ||

(k) ¬¬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?

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

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)

¬-intro

¬¬-elim

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) $P \vee Q$

|| ||

{$\vee$-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?

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

$\wedge$-intro

$\Leftrightarrow$-introduction

$\ldots$

(k) $P \Rightarrow Q$

$\ldots$

(l) $Q \Rightarrow P$

$\ldots$

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

(m) $P \Leftrightarrow Q$

($k < m, l < m$)

Bi-implication elimination

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

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

$\Leftrightarrow$-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