Derivations / Reasoning

Limitations of proofs by calculation

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

Example

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

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

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

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

we can prove this more intuitively by reasoning

Conclusions

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

An example of a mathematical proof

Theorem

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

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

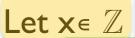
conclusion

Exposing logical structure

Theorem

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

Proof



Assume x² 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 $(P_1 \land P_2 \land ... \land P_n) \overset{\text{val}}{\vDash} Q$

If n=0, then
$$P_1 \wedge P_2 \wedge ... \wedge P_n \stackrel{\text{val}}{=} T$$

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

Q holds unconditionally

Derivation

Q is a correct conclusion from n premises $P_1, ..., P_n$ iff $(P_1 \land P_2 \land ... \land P_n) \overset{\text{val}}{\vDash} Q$

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

Two types of inference rules:

elimination rules

introduction rules

for drawing conclusions out of premises

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?

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

 $P \land Q \stackrel{\text{val}}{\models} Q$

∧-elimination

|| ||

(k) $P \wedge Q$

 $\parallel \parallel \parallel$

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

(m) P

 $\parallel \parallel$

(k) $P \wedge Q$

 $\parallel \parallel$

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

(m) Q

(k < m) (k < m)

Implication elimination

How do we use an implication in a proof?

 $P \Rightarrow Q \stackrel{\text{val}}{\vDash} ???$

 $(P \Rightarrow Q) \land P \stackrel{\text{val}}{\models} Q$

$$(m)$$
 Q

$$_{8}$$
 (k < m, l < m)

Conjunction introduction

How do we prove a conjunction?

∧-introduction

• • •

(k) F

• • •

(I) **Q**

• • •

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

(m) $P \wedge Q$

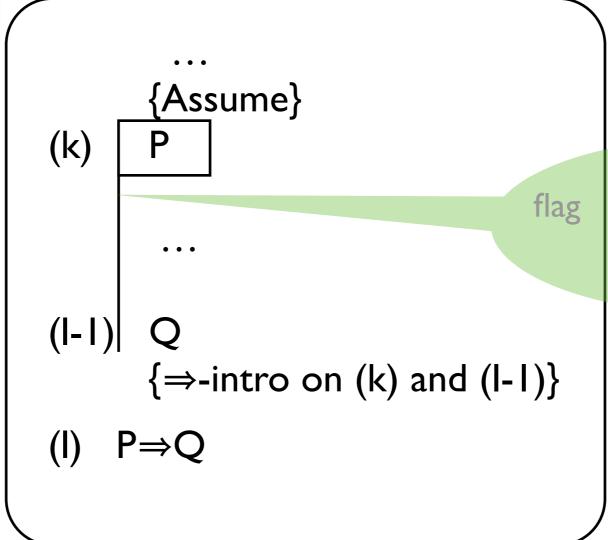
₉ (k < m, l < m)

 $P \land Q \stackrel{\text{val}}{\models} P \land Q$

Implication introduction

How do we prove an implication?

⇒-introduction

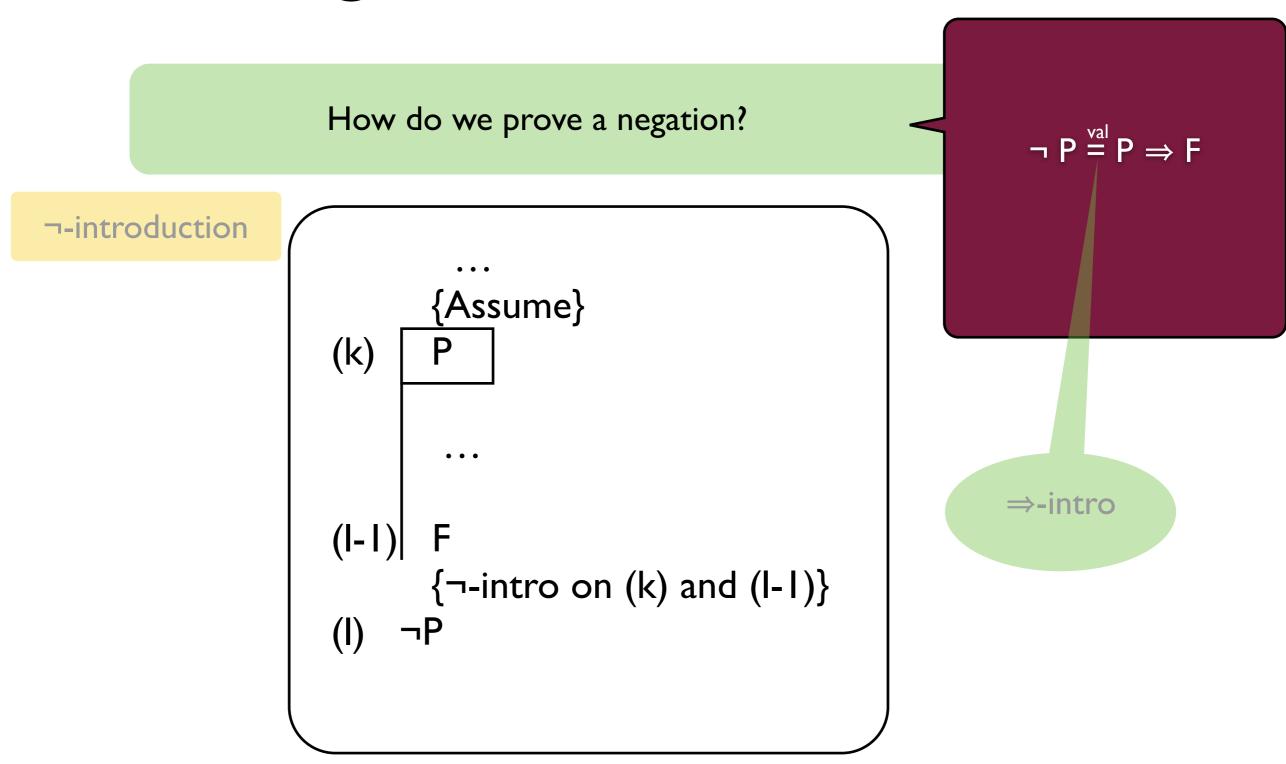


truly new and necessary for reasoning with hypothesis

shows the validity of a hypothesis

time for an example!

Negation introduction



Negation elimination

How do we use a negation in a proof?

¬-elimination

$$\parallel \parallel$$

(k) P

(I) ¬P

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

time for an example!

F introduction

How do we prove F?

F-introduction

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

(k) P ...

(I) ¬P

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

the same as ¬-elim only intended bottom-up

 $_{13}$ (k < m, l < m)

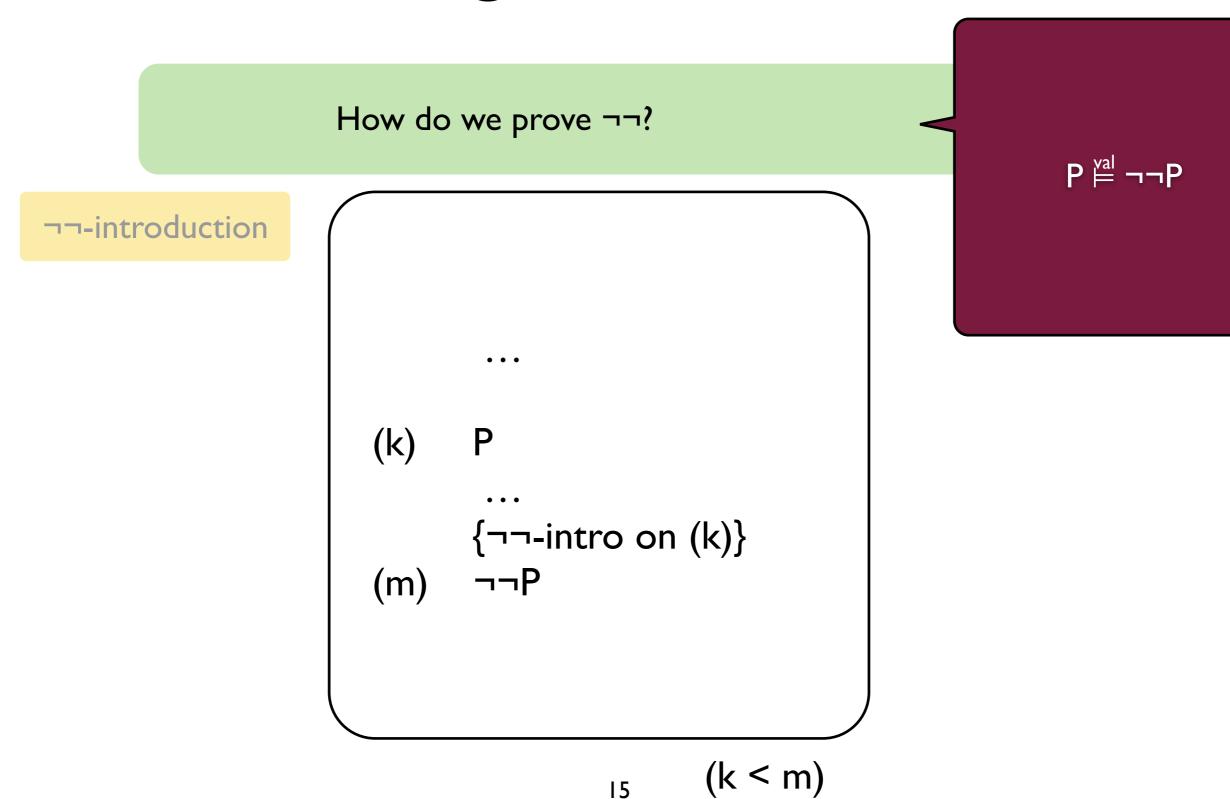
F elimination

How do we use F in a proof? F-elimination (k) $\{F-elim on (k)\}$ (m) 14

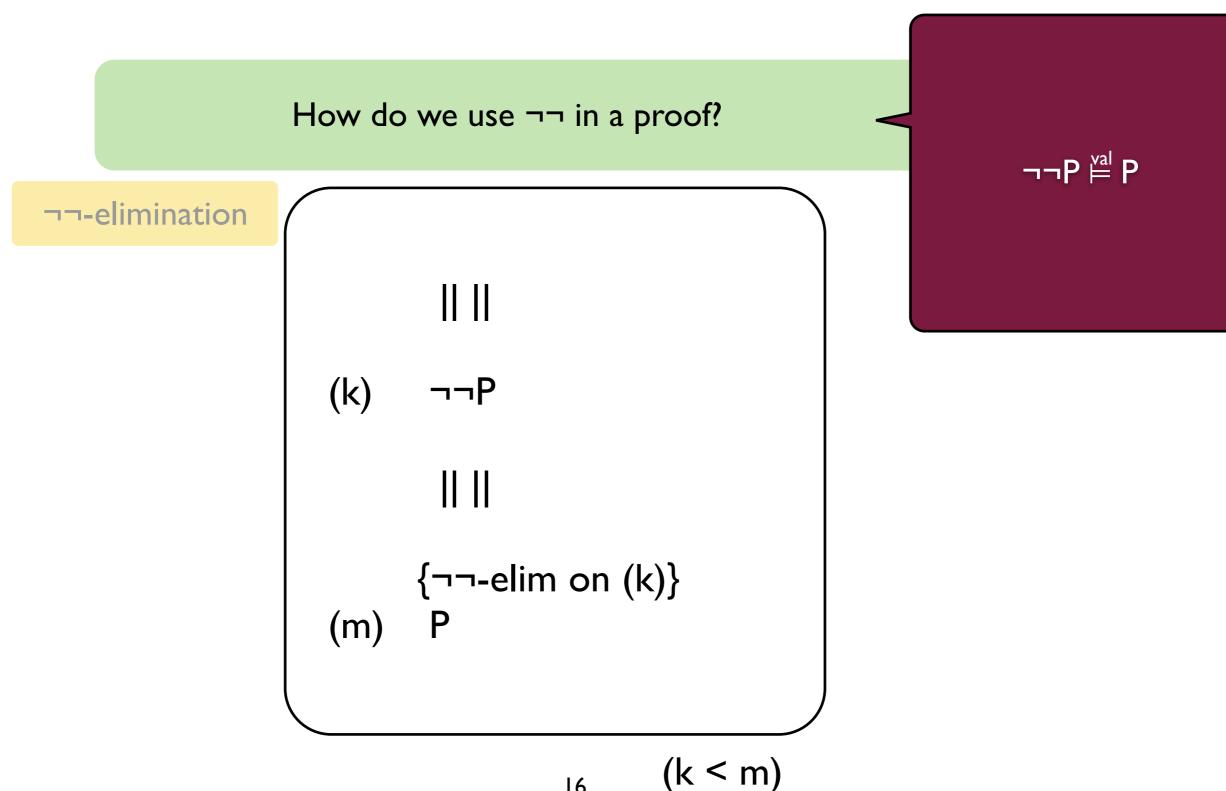
it's very useful!

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

Double negation introduction



Double negation elimination



Proof by contradiction

Theorem

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

Proof



Assume x² 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

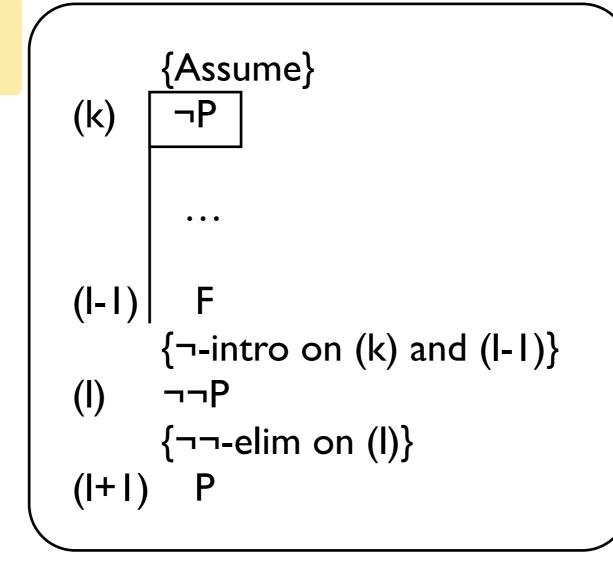
conclusion

Thanks to Bas Luttik

Proof by contradiction

How do we prove P by a contradiction?

proof by contradiction



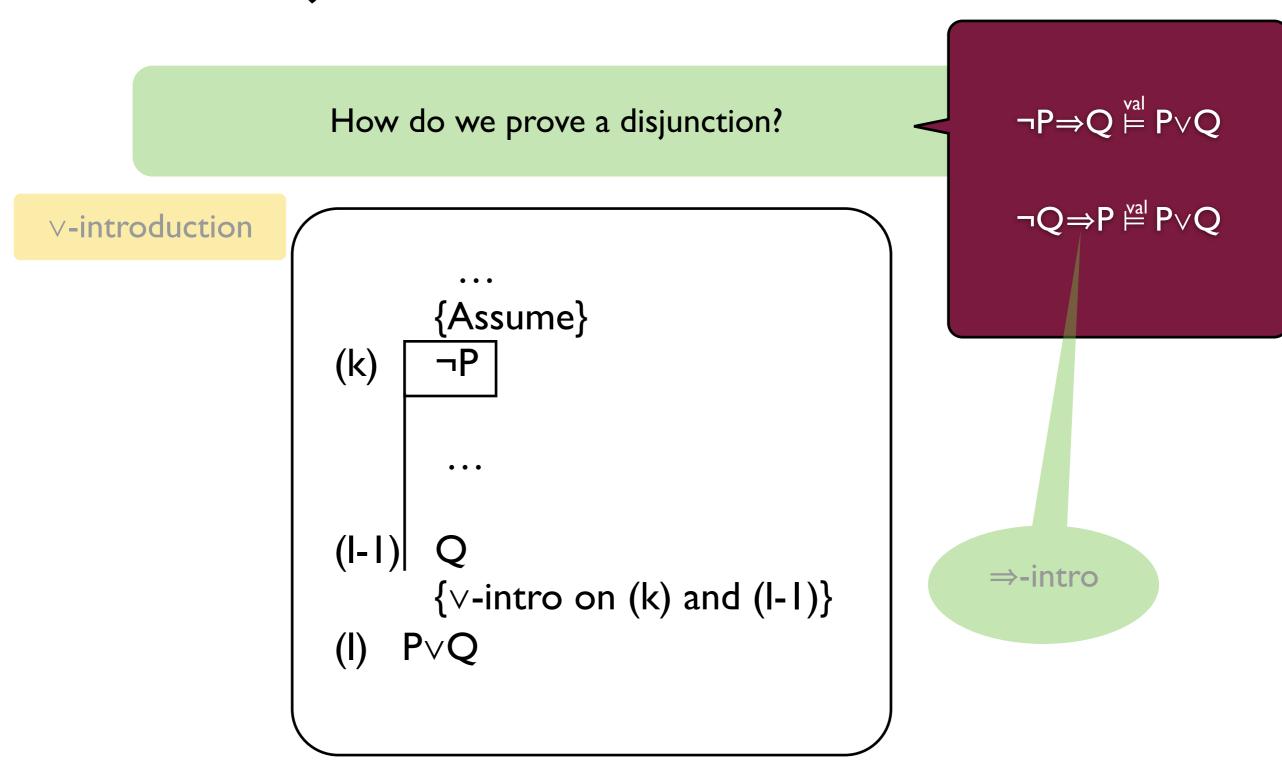
 $\neg P \Rightarrow F \stackrel{\text{val}}{\models} \neg \neg P \stackrel{\text{val}}{\models} P$

¬-intro

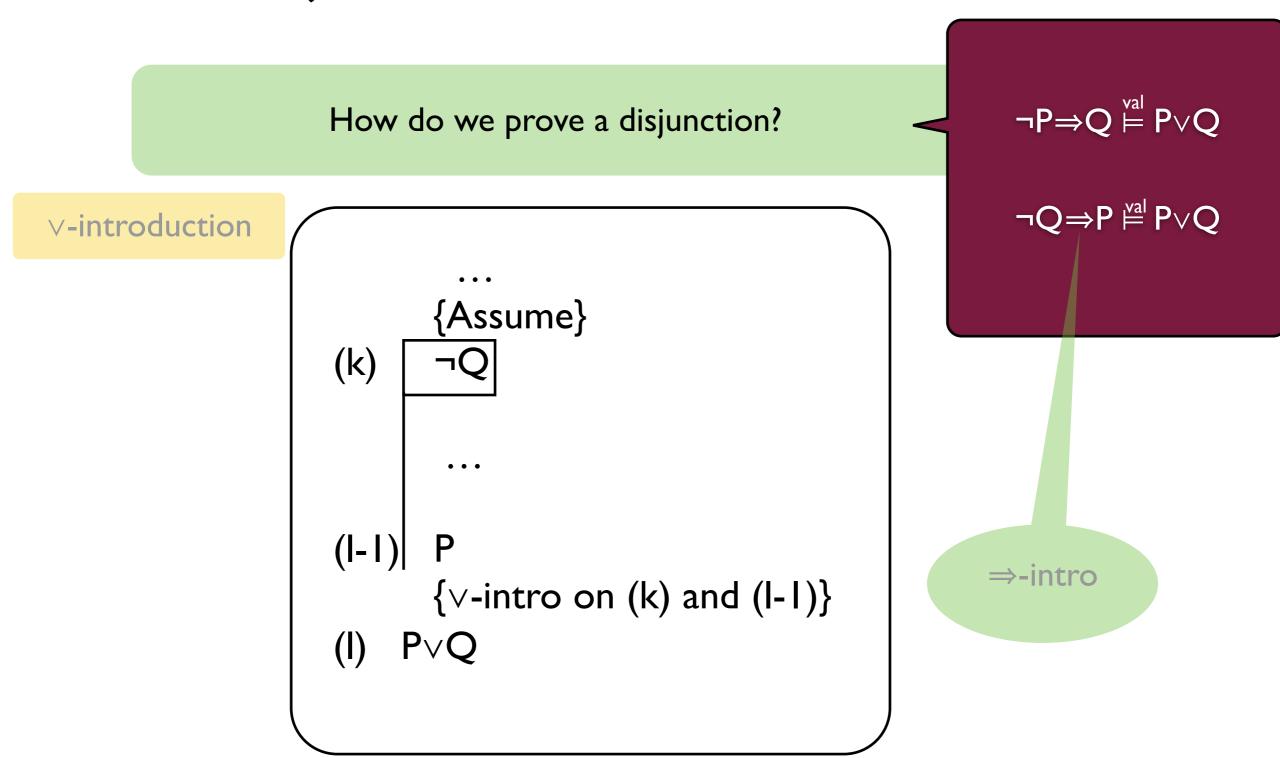
¬¬-elim

time for an example!

Disjunction introduction



Disjunction introduction



Disjunction elimination

How do we use a disjunction in a proof?

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

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

$$\parallel \parallel$$

$$(k)$$
 $P \lor Q$

$$(k \le m)$$

21

Disjunction elimination

How do we use a disjunction in a proof?

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

 $P \lor Q \stackrel{\text{Yal}}{\models} \neg Q \Rightarrow P$

$$\parallel \parallel$$

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

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

(m) $\neg Q \Rightarrow P$

Proof by case distinction

How do we prove R by a case distinction?

proof by case distinction

 $\| \|$

(k) $P\lor Q$

l) P⇒R

|| ||

(m) $Q \Rightarrow R$

 $\| \|$

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

(n) R

 $(P \lor Q) \land (P \Rightarrow R) \land (Q \Rightarrow R) \stackrel{\text{val}}{\models} R$

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

Bi-implication introduction

How do we prove a bi-implication?

 $(P \Rightarrow Q) \land (Q \Rightarrow P) \stackrel{\text{val}}{\models} P \Leftrightarrow Q$

⇔-introduction

• • •

(k) P⇒Q

• • •

(I) $Q \Rightarrow P$

• •

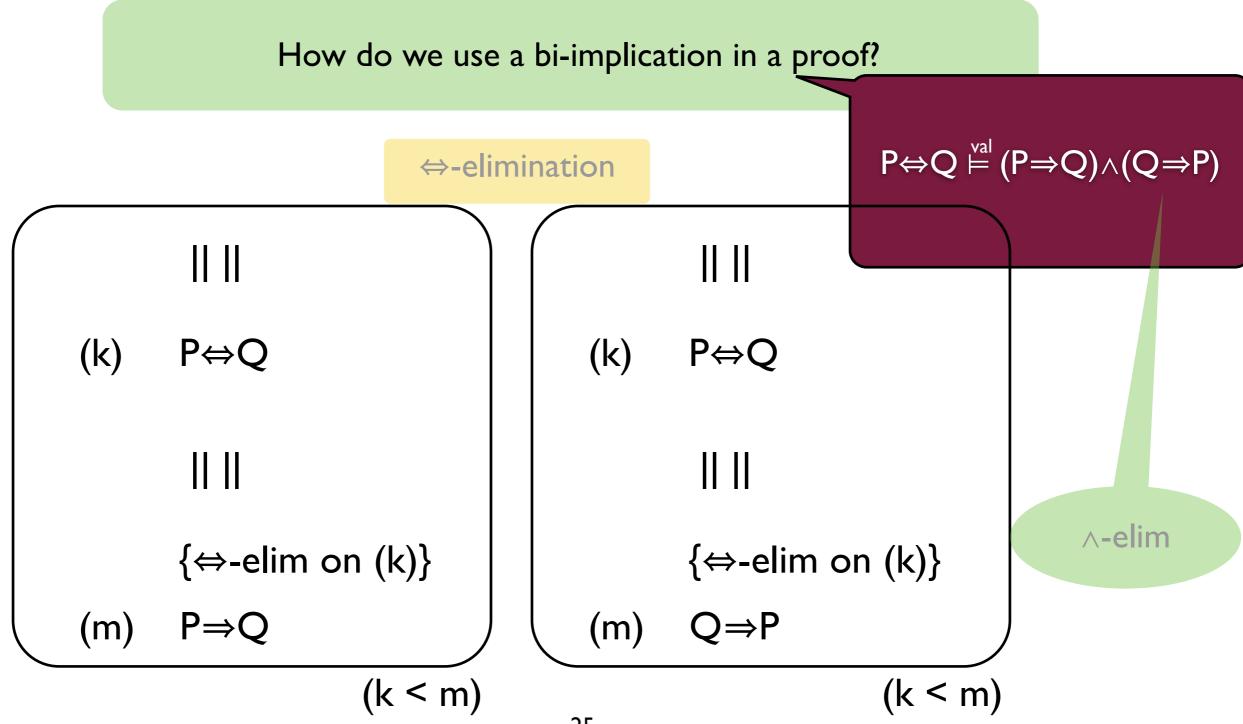
 $\{\Leftrightarrow$ -intro on (k) and (l) $\}$

(m) P⇔Q

∧-intro

(k < m, l < m)

Bi-implication elimination



Derivations / Reasoning with quantifiers

Proving a universal quantification

To prove

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

Proof

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

Then, for this particular x, it holds that $x^2 - 2x = x(x-2) \ge 0$ (Why?)

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

V introduction

How do we prove a universal quantification? -

1044 do 44c prove a diliversal qualitificación.

similar to
⇒-intro
with
generating
hypothesis

∀-introduction

(k) **Var** x; P(x)

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

shows the validity of a hypothesis

Using a universal quantification

We know

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

Whenever we encounter an $a \in \mathbb{Z}$ such that $a \ge 2$, we can conclude that $a^2 - 2a \ge 0$.

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

∀ elimination

How do we use a universal quantification in a proof?

∀-elimination

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

|| ||

(l) P(a)

(m)

 $\{\forall$ -elim on (k) and (l) $\}$ Q(a)

time for an example!

similar to implication but we need a witness

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

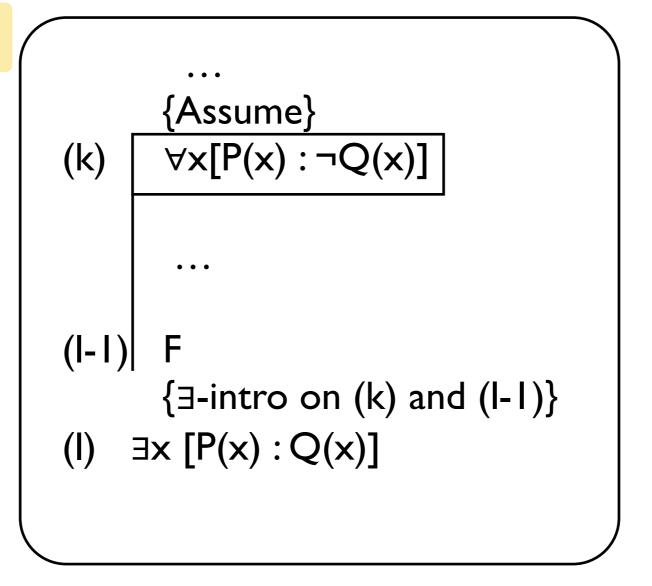
the same "a" from line (I)

$$_{30}$$
 (k < m, I < m)

3 introduction

How do we prove an existential quantification?

3-introduction



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

and ¬-intro

3 elimination

How do we use an existential quantification in a proof?

3-elimination

|| ||

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

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

|| || {∃-elim on (k) and (l)}

(m) F

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

and ¬- elimination

time for an example!

 $_{32}$ (k < m, l < m)

Proofs with 3-introduction and 3-elimination are unnecessarily long and cumbersome...

There are alternatives!

Proving an existential quantification

To prove

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

Proof

It suffices to find a witness, i.e., an $x \in \mathbb{Z}$ satisfying $x^3 - 2x - 8 \ge 0$.

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

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

also x = 5 is a witness...

Alternative 3 introduction

How do we prove an existential quantification?

3*-introduction

by finding a witness

(k) P(a)

• • •

(I) Q(a)

• • •

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

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

strategy: wait until a witness object appears

does not always work

35
 (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 3 elimination

How do we use an existential quantification in a proof?

∃*-elimination

 $\| \|$

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

 $\| \|$

{∃*-elim on (k)}

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

we pick a witness

x must be new!

time for an example!