## De Morgan with quantifiers

### De Morgan

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

not for all = at least for one not

not exists = for all not

Hence:  $\neg \forall = \exists \neg \text{ and } \neg \exists = \forall \neg$ 

It holds further that:

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

holds also for quantified formulas!

### Substitution

meta rule

### Simple

$$\phi \stackrel{val}{=} \psi$$

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

### Sequential

$$\phi \stackrel{val}{=} \psi$$

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

### Simultaneous

$$\phi \stackrel{val}{=} \psi$$

EVERY occurrence of P is substituted!

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

holds also for quantified formulas!

### The rule of Leibniz

### Leibniz

$$\phi \stackrel{val}{=} \psi$$

$$C[\phi] \stackrel{val}{=} C[\psi]$$

formula that has  $\phi$  as a sub formula

meta rule

single occurrence is replaced!

# Other equivalences with quantifiers

### Exchange trick

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

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

#### No wonder as

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

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

### Term splitting

$$\forall_x [P:Q \land R] \stackrel{val}{=} \forall_x [P:Q] \land \forall_x [P:R]$$

$$\exists_x [P:Q \lor R] \stackrel{val}{=} \exists_x [P:Q] \lor \exists_x [P:R]$$

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

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

still hold (in predicate logic)

Lemma W5: If  $Q \models R$  then  $\forall_x [P:Q] \models \forall_x [P:R]$ .

# Derivations / Reasoning

# Limitations of proofs by calculation

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

### Example

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

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

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

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

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  $(x \in \mathbb{Z})$ .

(sub)goal

Proof

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

We need to prove that x is even too.

generating hypothesis

pure hypothesis

conclusion

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.

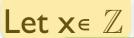
Thanks to Bas Luttik

## Exposing logical structure

Theorem

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

Proof



Assume x<sup>2</sup> 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  $(P_1 \land P_2 \land ... \land P_n) \stackrel{\text{val}}{\vDash} Q$ 

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) F

 $\parallel \parallel$ 

(k)  $P \wedge Q$ 

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

(m) Q

(k < m) (k < m)

## Implication elimination

How do we use an implication in a proof?

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

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

⇒-elimination

$$\parallel \parallel$$

$$(m)$$
 Q

$$(k \le m, l \le m)$$

## Conjunction introduction

How do we prove a conjunction?

∧-introduction

• • •

(k) F

• • •

(I) C

• • •

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

(m)  $P \wedge Q$ 

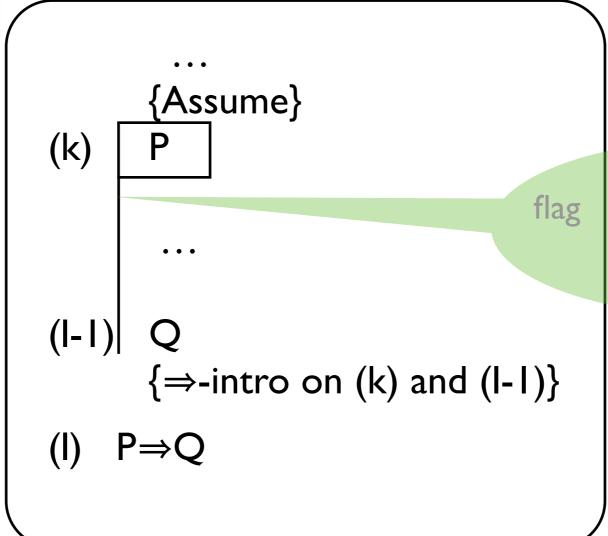
(k < m, l < m)

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

## Implication introduction

How do we prove an implication?

⇒-introduction

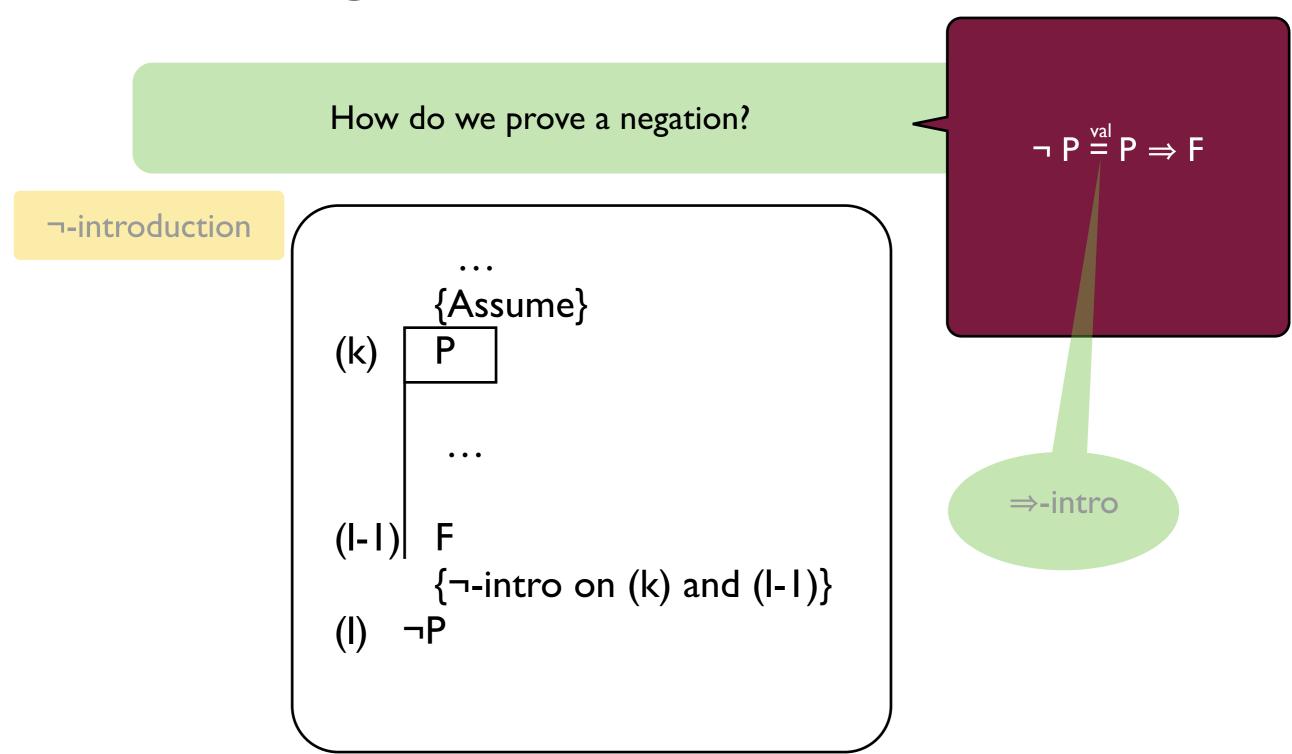


truly new
and
necessary for
reasoning with
hypothesis

shows the validity of a hypothesis

time for an example!

## Negation introduction



## Negation elimination

How do we use a negation in a proof?

¬-elimination

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

time for an example!

(k < m, l < m)

### F introduction

(k)

**(I)** 

 $\neg P$ 

the same as ¬-elim only intended bottom-up

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

 $(k \le m, l \le m)$ 

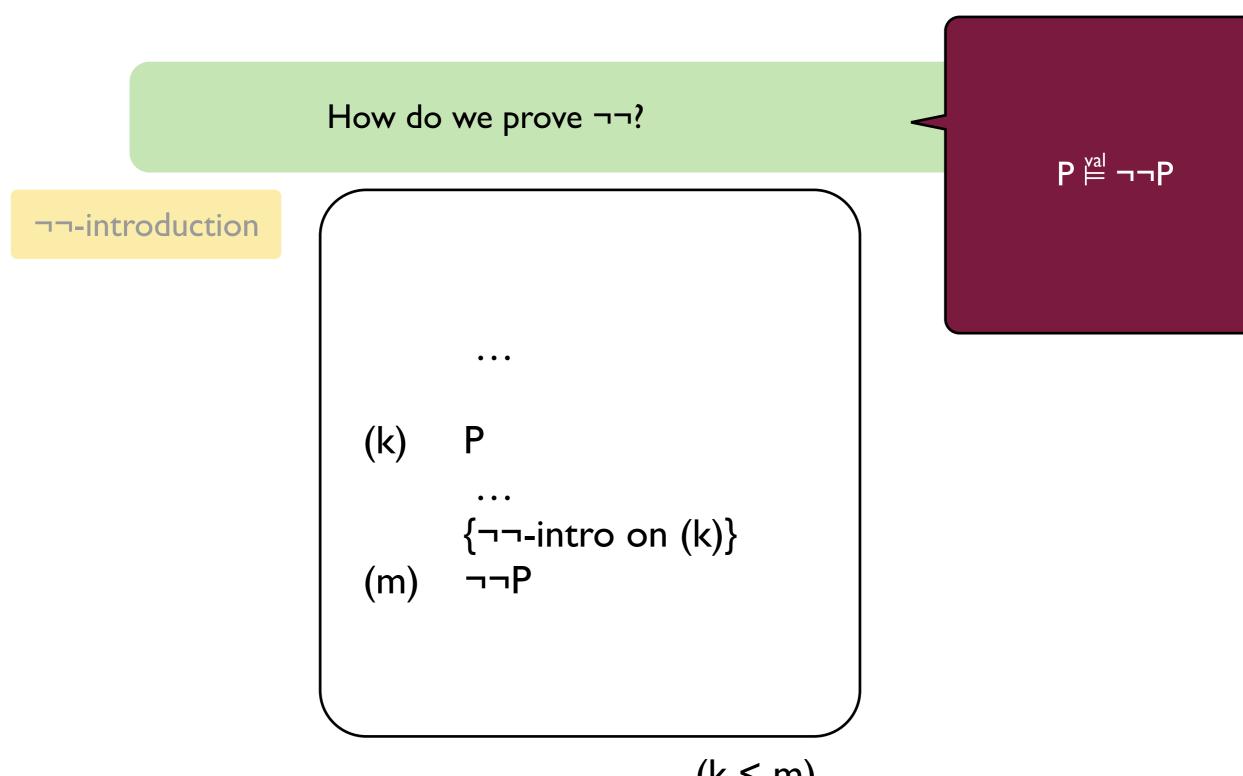
## **F** elimination

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

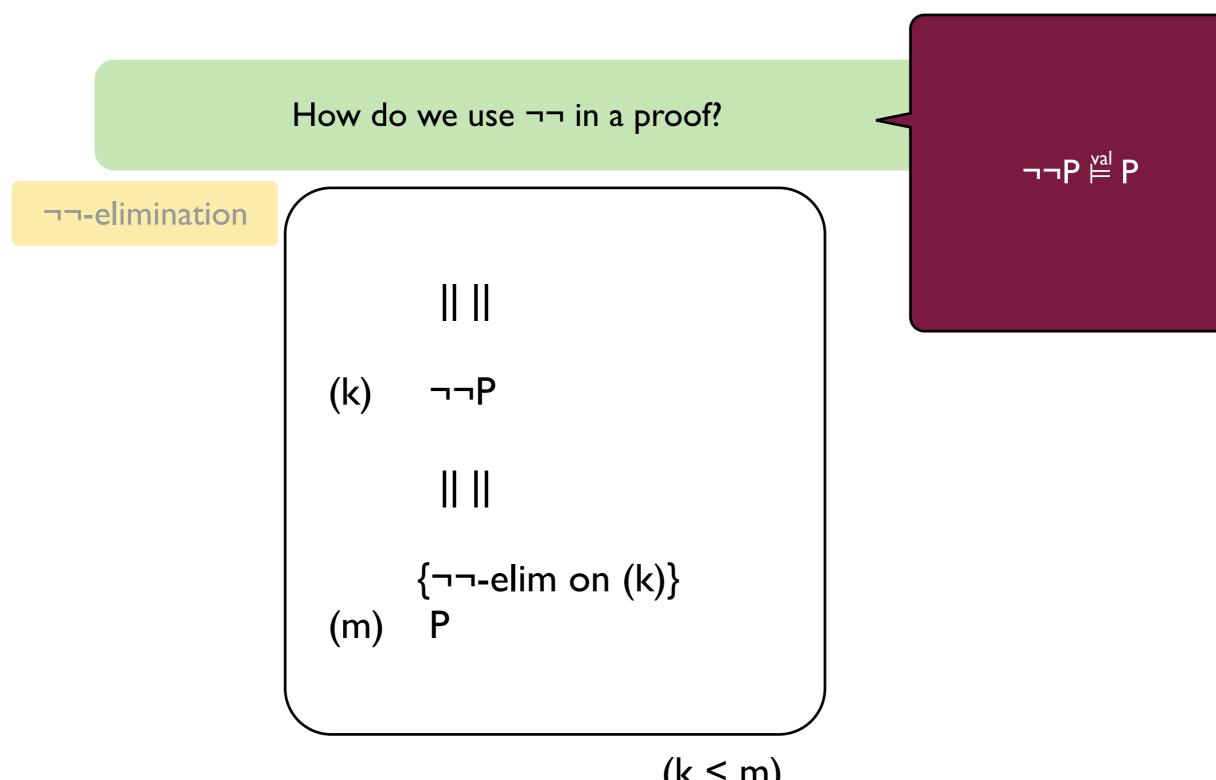
it's very useful!

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

## Double negation introduction



## Double negation elimination

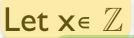


## Proof by contradiction

Theorem

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

Proof



Assume x<sup>2</sup> 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)
         ¬P
        \{\neg-intro on (k) and (I-I)\}
(l)
        \neg \neg P
        \{\neg\neg\text{-elim on (I)}\}\
(|+|)
```

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

¬-intro

¬¬-elim

time for an example!

(k < m)