## Derivations / Reasoning

## Limitations of proofs by calculation

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

#### Example

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

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

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

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

## Limitations of proofs by calculation

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

#### Example

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

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

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

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

#### Conclusions

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

## 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

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

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.

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.

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.

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.

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.

generating hypothesis

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.

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.

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

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



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

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

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

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

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

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 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

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

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

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

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

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

(particularly useful) instances of the single inference rule

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

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

(particularly useful) instances of the single inference rule

and one new special rule!

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

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

(particularly useful) instances of the single inference rule

and one new special rule!

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

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!

How do we use a conjunction in a proof?

How do we use a conjunction in a proof?

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

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

How do we use a conjunction in a proof?

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

How do we use a conjunction in a proof?

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

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

```
|| ||
```

(k)  $P \wedge Q$ 

 $\Pi$ 

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

(m) F

$$\parallel \parallel$$

(k)  $P \wedge Q$ 

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

(m) Q

 $(k \le m)$ 

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)  $P \wedge Q$ 

|| ||

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

(m) F

(k)  $P \wedge Q$ 

|| ||

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

(m) Q

(k < m) (k < m)

How do we use an implication in a proof?

How do we use an implication in a proof?

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

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

How do we use an implication in a proof?

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

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

How do we use an implication in a proof?

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

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

⇒-elimination

$$(m)$$
 Q

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

How do we prove a conjunction?

How do we prove a conjunction?



How do we prove a conjunction?

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

```
(k) P
```

(I) **C** 

 $\{\land\text{-intro on (k) and (l)}\}\$  (m)  $P \land Q$ 

(k < m, l < m)

How do we prove a conjunction?

∧-introduction

• • •

(k) F

• • •

(I) Q

• • •

 $\{\land$ -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?

How do we prove an implication?

```
{Assume}
\{\Rightarrow-intro on (k) and (I-I)\}
```

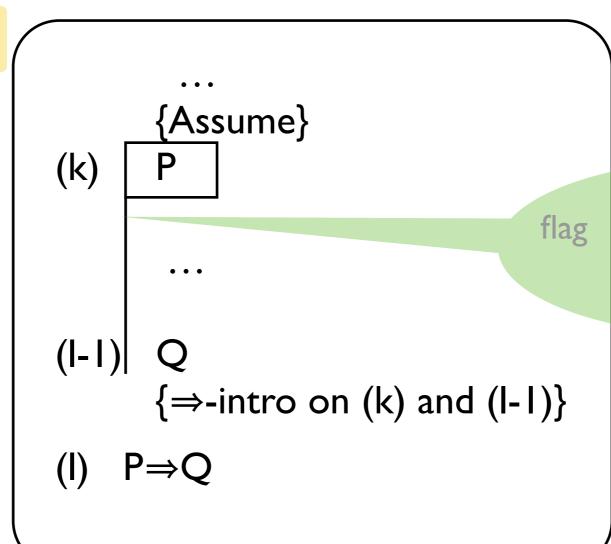
How do we prove an implication?

⇒-introduction

```
{Assume}
(k)
        \{\Rightarrow-intro on (k) and (I-I)\}
```

How do we prove an implication?

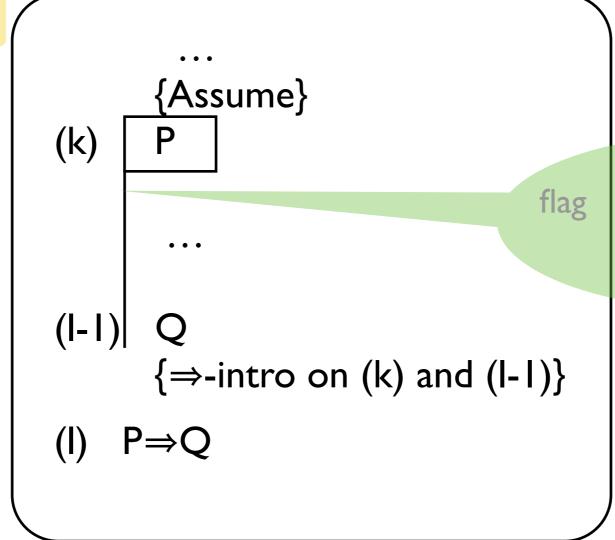
⇒-introduction



shows the validity of a hypothesis

How do we prove an implication?

⇒-introduction

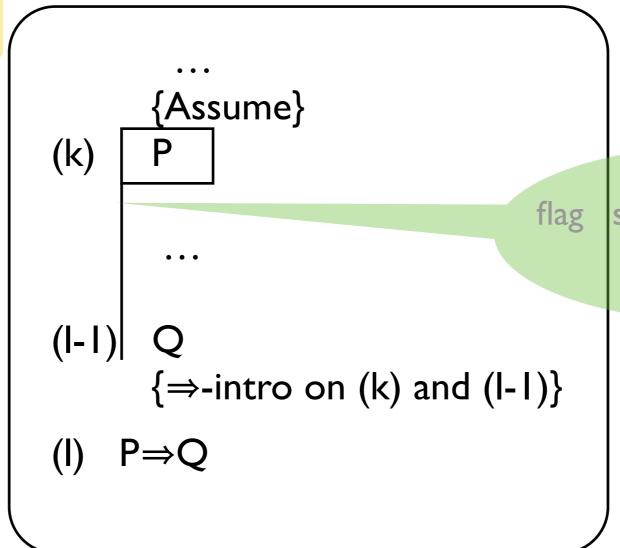


truly new and necessary for reasoning with hypothesis

shows the validity of a hypothesis

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!

How do we prove a negation?

How do we prove a negation?

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

How do we prove a negation?

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

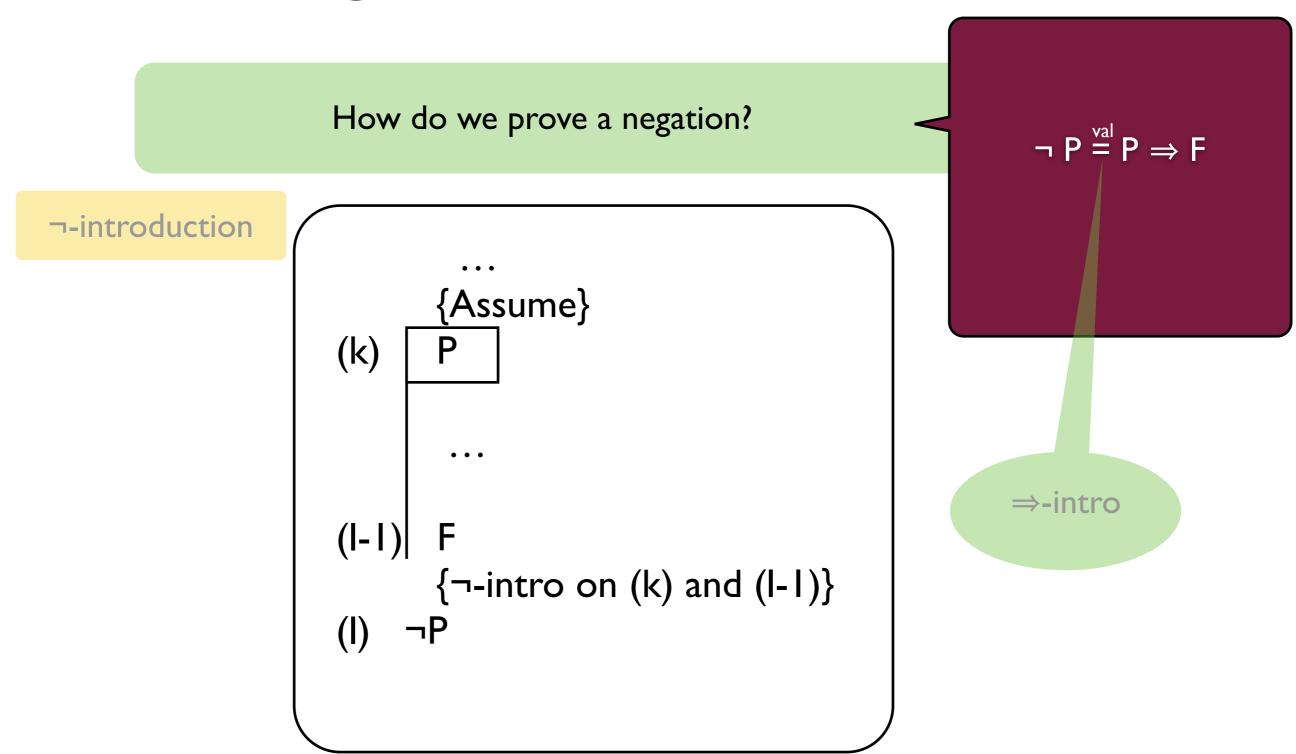
```
{Assume}
(k)
         \{\neg\text{-intro on }(k) \text{ and }(I-I)\}
```

How do we prove a negation?

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

¬-introduction

```
{Assume}
(k)
(I-I)
        \{\neg\text{-intro on (k) and (I-I)}\}\
```



How do we use a negation in a proof?

How do we use a negation in a proof?

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

How do we use a negation in a proof?

```
\{\neg-elim on (k) and (l)\}
```

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

(k < m, l < m)

How do we use a negation in a proof?

¬-elimination

(k)

```
|| || {¬-elim on (k) and (l)} (m) F
```

(k < m, l < m)

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

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!

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

How do we prove F?

How do we prove F?

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

How do we prove F? (k) **(l)** {F-intro on (k) and (l)} (m)

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

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

How do we prove F?

F-introduction

• • •

(k) F

. . .

(I) ¬P

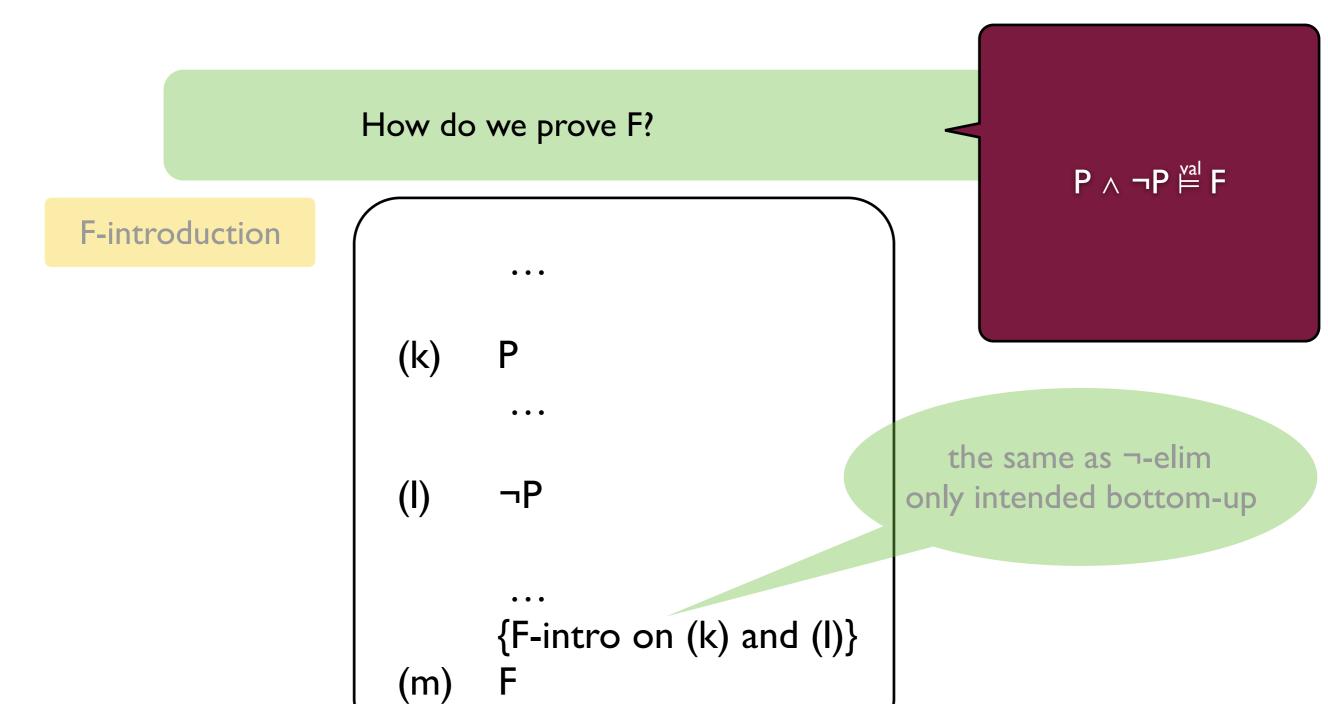
• • •

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

(m) F

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

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



(k < m, l < m)

How do we use F in a proof?

How do we use F in a proof?

it's very useful!

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

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

it's very useful!

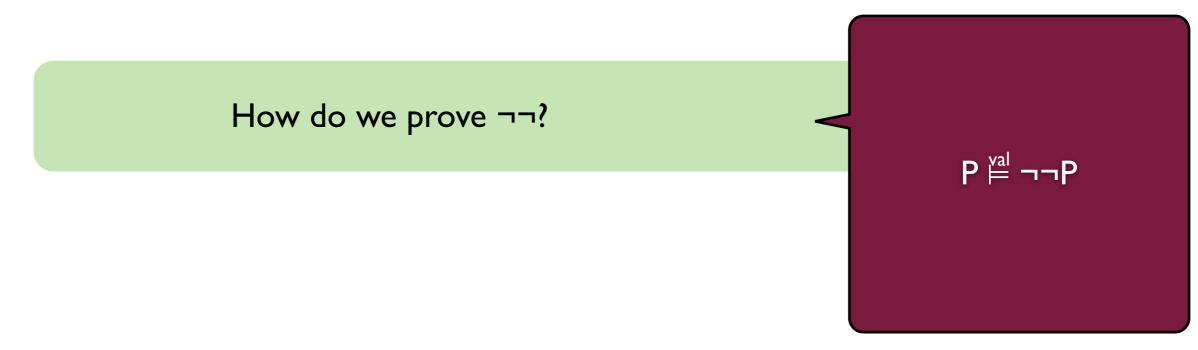
 $F \stackrel{\text{val}}{\models} P$ 

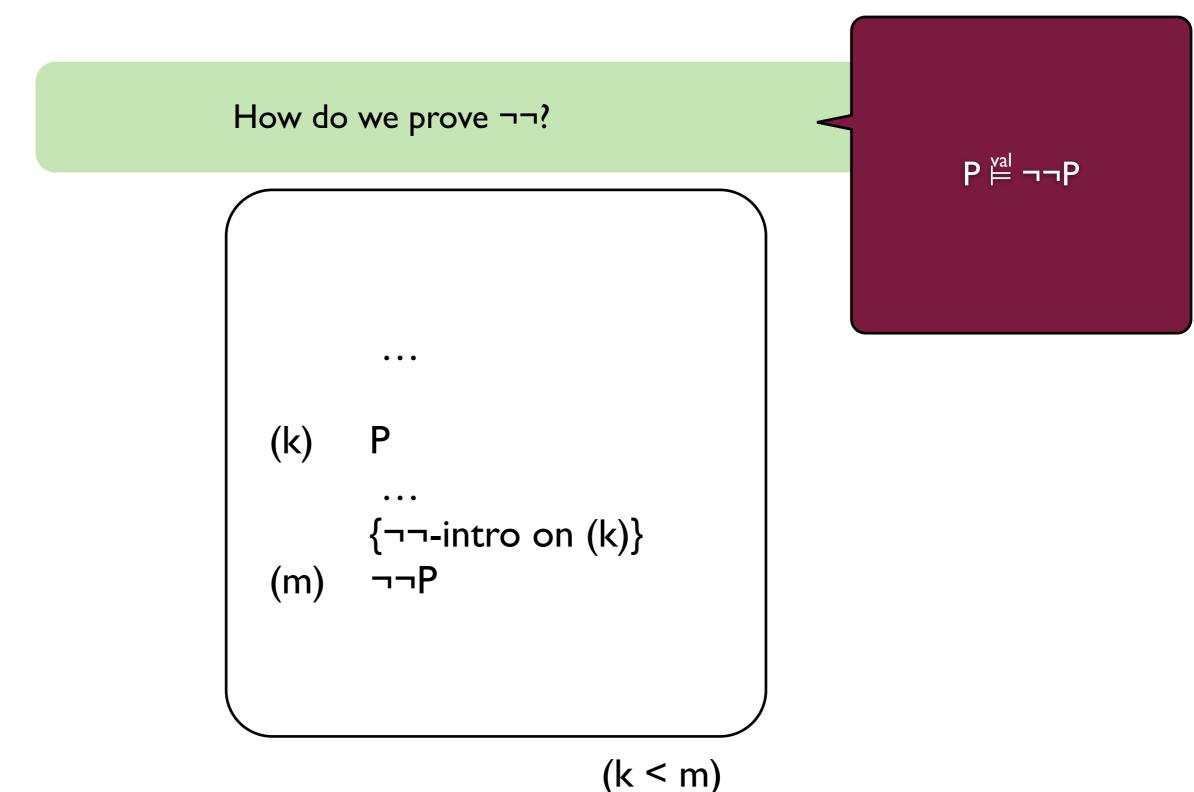
How do we use F in a proof? F-elimination (k)  $\{F-elim on (k)\}$ (m)

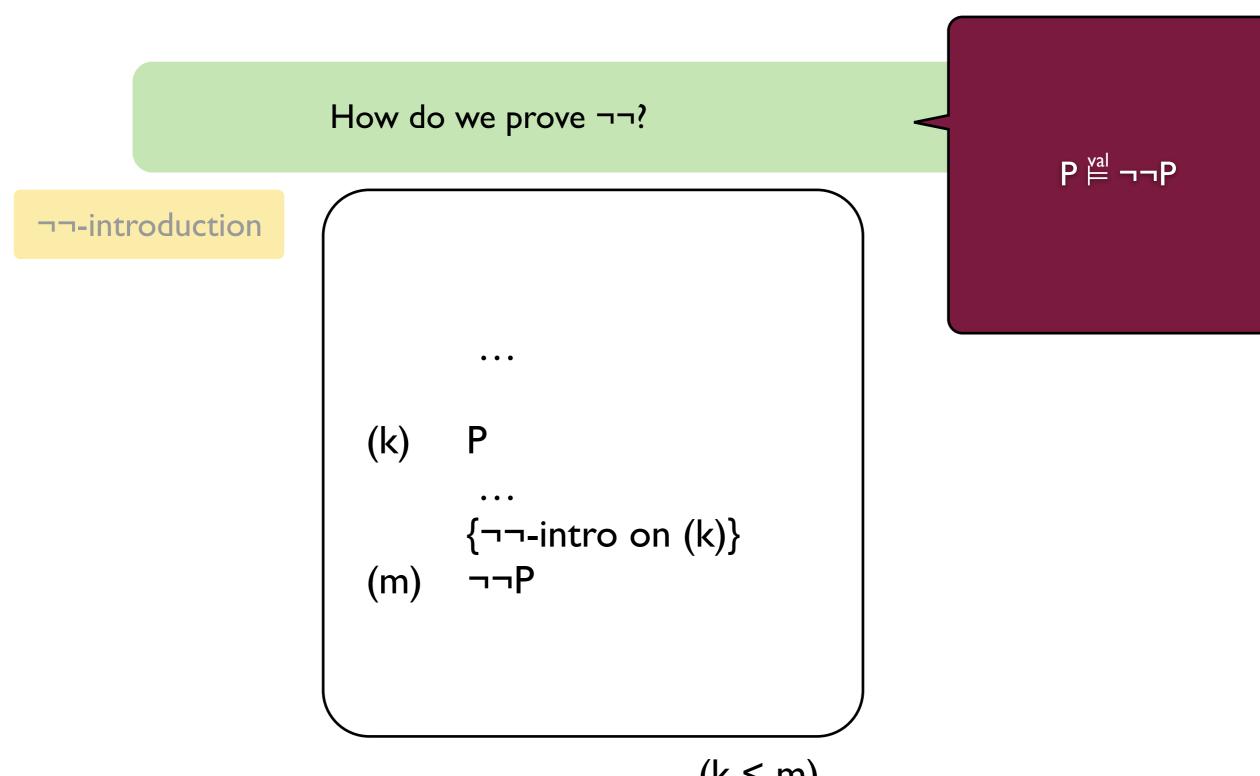
it's very useful!

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

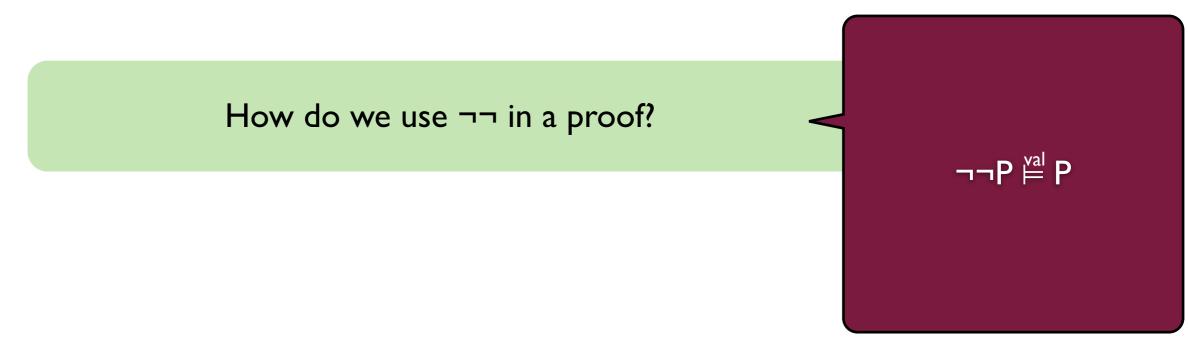
How do we prove ¬¬?

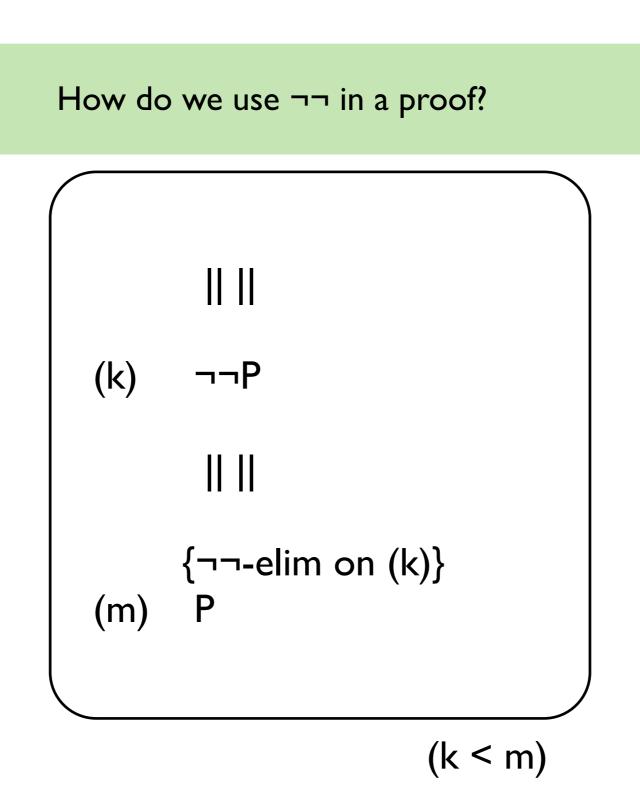




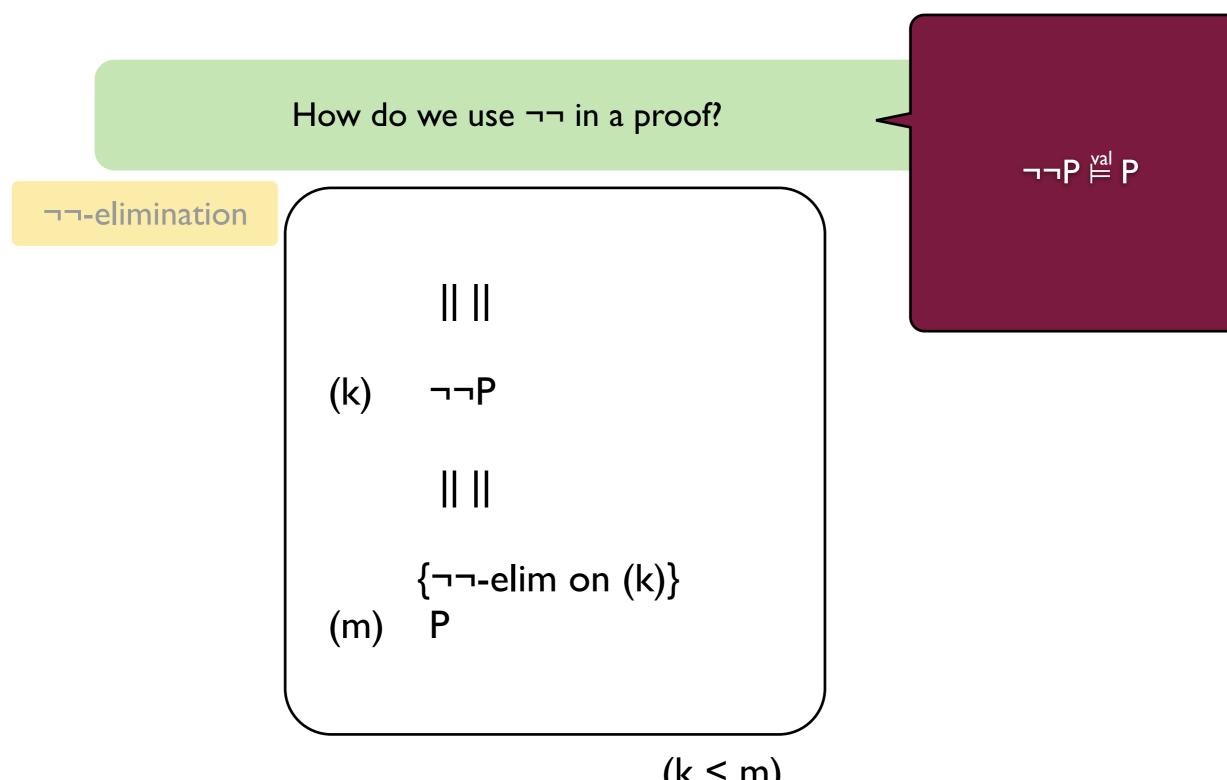


How do we use ¬¬ in a proof?





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



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

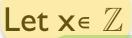
pure hypothesis

conclusion

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

How do we prove P by a contradiction?

How do we prove P by a contradiction?

```
{Assume}
        \{\neg\text{-intro on (k) and (I-I)}\}\
        \{\neg\neg\text{-elim on (I)}\}
(|+|)
```

(k < m)

How do we prove P by a contradiction?

proof by contradiction

```
{Assume}
(k)
        \{\neg-intro on (k) and (l-1)\}
        \neg \neg P
        \{\neg\neg\text{-elim on (I)}\}\
(|+|)
```

How do we prove P by a contradiction?

proof by contradiction

```
{Assume}
(k)
        \{\neg-intro on (k) and (l-1)\}
(l)
        \neg \neg P
        \{\neg\neg\text{-elim on (I)}\}\
(|+|)
```

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

(k < m)

How do we prove P by a contradiction?

proof by contradiction

```
{Assume}
(k)
         ¬P
        \{\neg-intro on (k) and (l-1)\}
(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

How do we prove P by a contradiction?

proof by contradiction

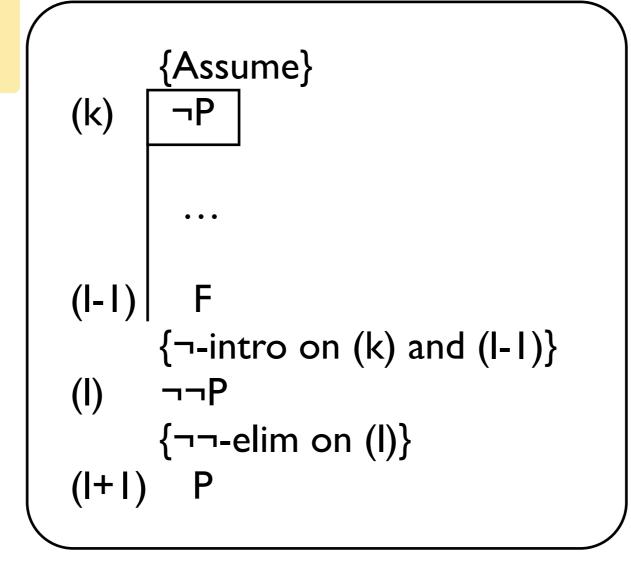
```
{Assume}
(k)
         ¬P
        \{\neg-intro on (k) and (l-1)\}
(l)
        \neg \neg P
       \{\neg\neg\text{-elim on (I)}\}\
(|+|)
```

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

(k < m)

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!

(k < m)

How do we prove a disjunction?

How do we prove a disjunction?

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

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

How do we prove a disjunction?

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

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

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

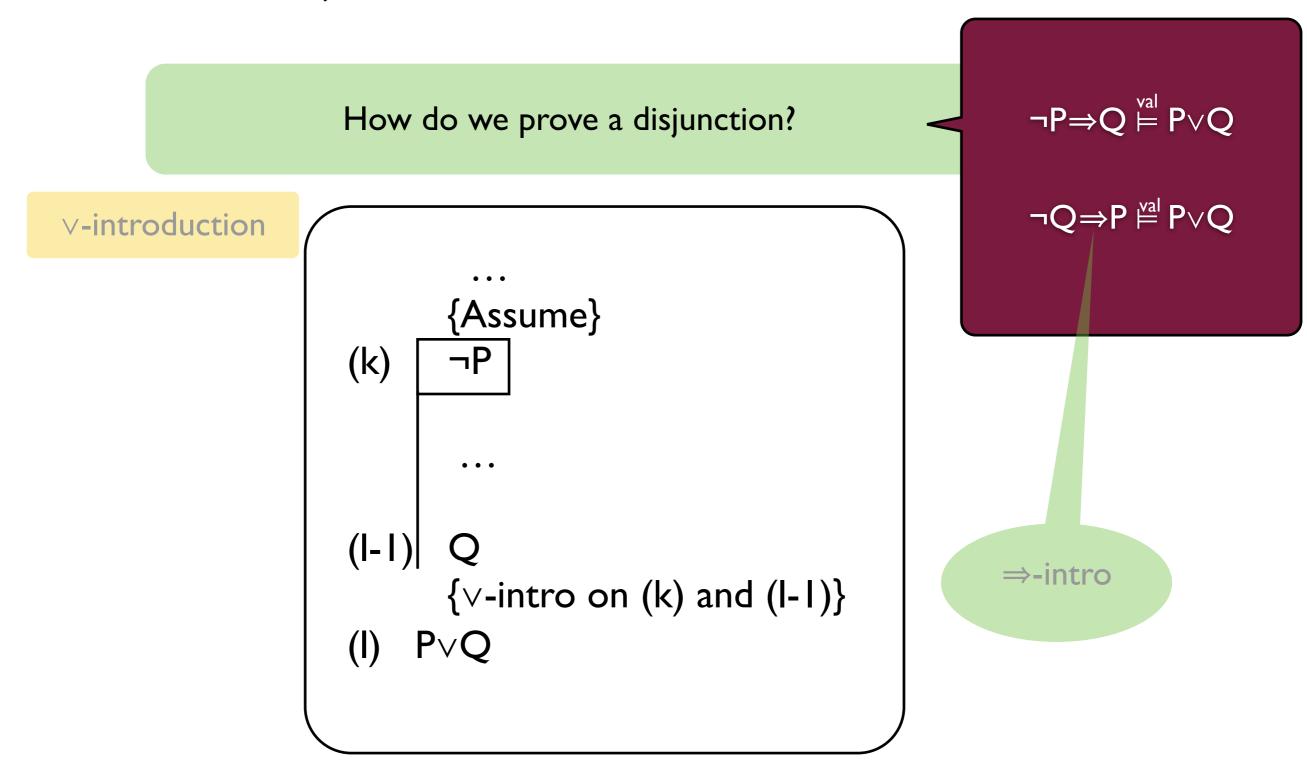
How do we prove a disjunction?

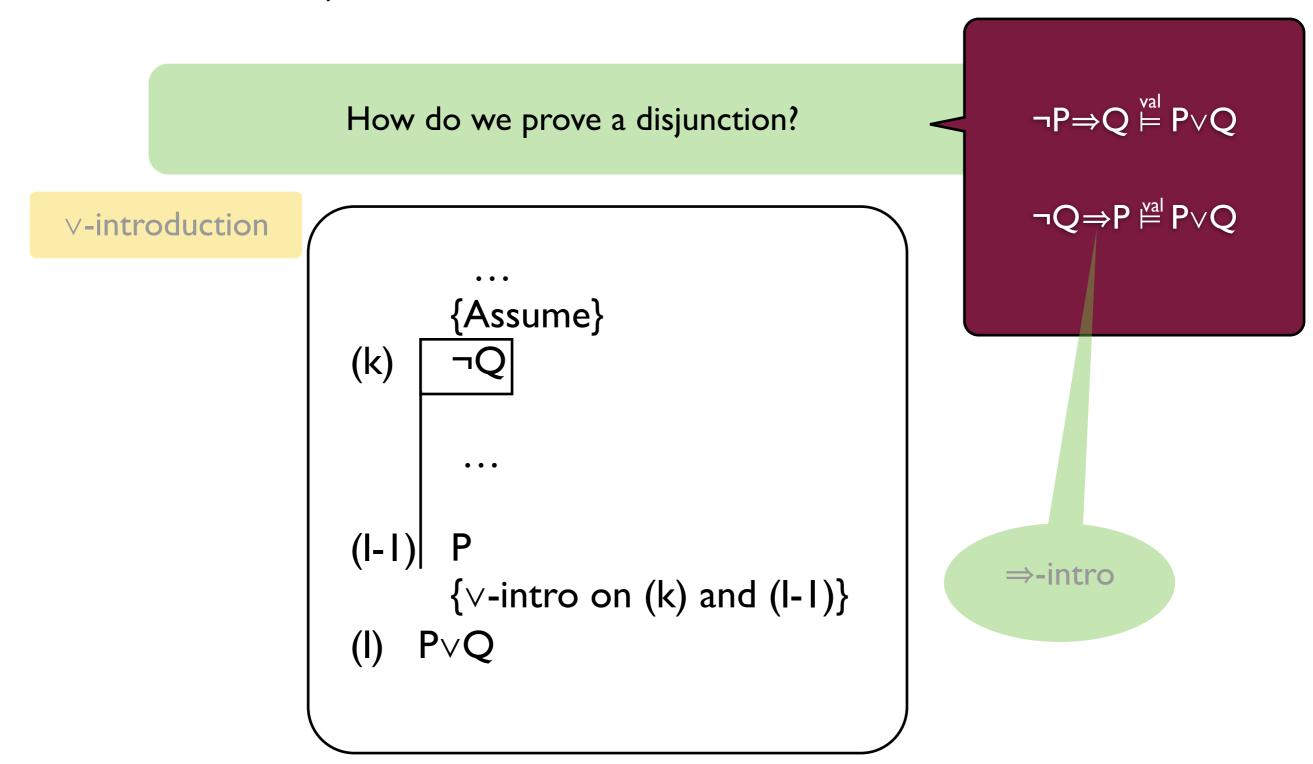
 $\neg P \Rightarrow Q \stackrel{\text{val}}{\vDash} P \lor Q$ 

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

∨-introduction

{Assume} (k)  $\{\lor$ -intro on (k) and (l-1) $\}$  $P \lor Q$ 





How do we use a disjunction in a proof?

How do we use a disjunction in a proof?

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

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

How do we use a disjunction in a proof?

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

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

$$(k \le m)$$

How do we use a disjunction in a proof?

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

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

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

How do we use a disjunction in a proof?

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

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

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

$$\{ \lor \text{-elim on (k)} \}$$
  
(m)  $\neg Q \Rightarrow P$ 

How do we prove R by a case distinction?

How do we prove R by a case distinction?

```
|| ||
      P⇒R
       \| \|
(m) Q \Rightarrow R
      || ||
      {case-dist on (k), (l), (m)}
(n)
```

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

How do we prove R by a case distinction?

proof by case distinction

```
\| \|
(k)
       P \lor Q
      || ||
      P⇒R
       || ||
(m) Q \Rightarrow R
      || ||
      {case-dist on (k), (l), (m)}
(n)
```

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

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

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

#### 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

#### 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

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

#### Bi-implication introduction

How do we prove a bi-implication?

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

⇔-introduction

• • •

(k) P⇒Q

• • •

(I)  $Q \Rightarrow P$ 

• • •

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

(m) P⇔Q

(k < m, l < m)

∧-intro

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

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

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

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

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

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

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

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

(k) P⇔Q

|| ||

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

(k < m)

(m) P⇒Q

(k) P⇔Q

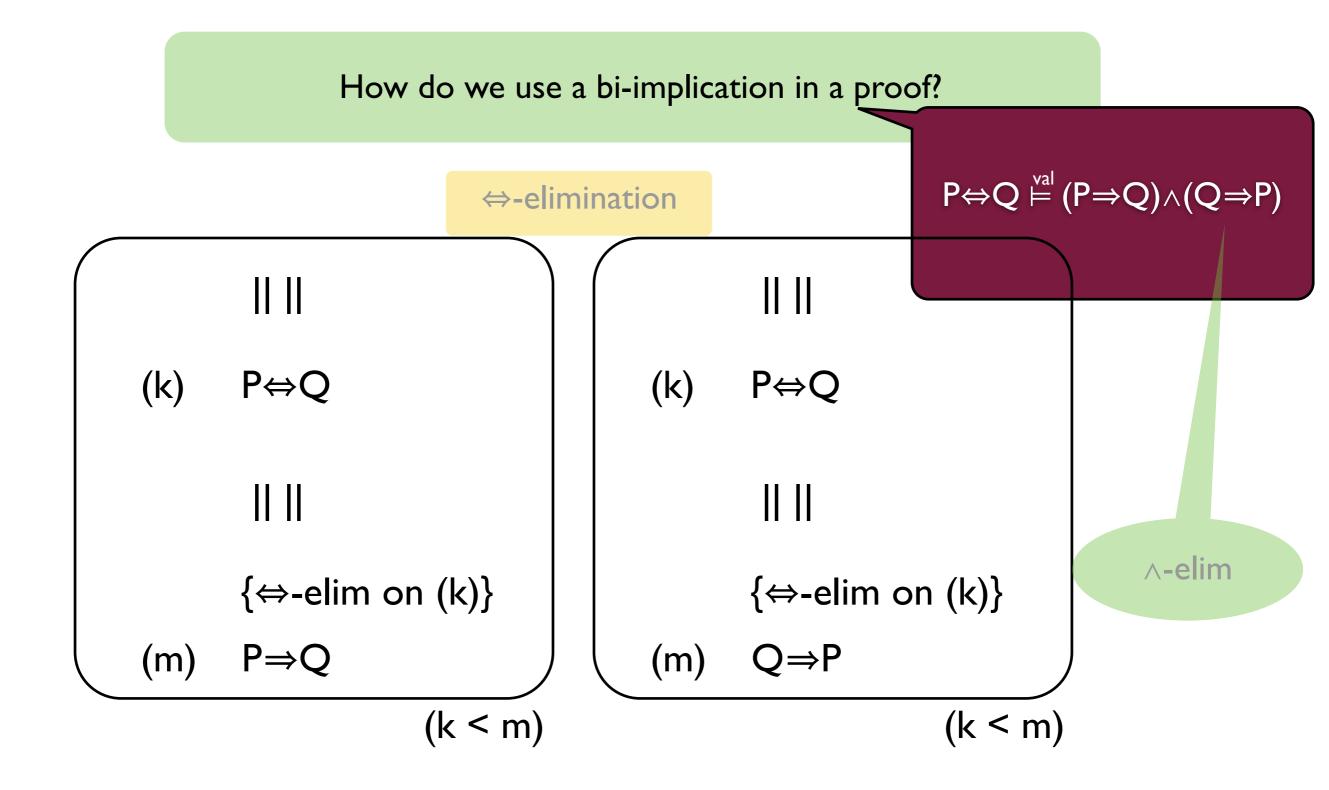
 $\parallel \parallel \parallel$ 

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

(m)  $Q \Rightarrow P$ 

 $(k \le m)$ 

How do we use a bi-implication in a proof?  $P\Leftrightarrow Q \stackrel{\text{val}}{\models} (P\Rightarrow Q) \land (Q\Rightarrow P)$ ⇔-elimination  $\parallel \parallel \parallel$ (k) (k) P⇔Q P⇔Q  $\parallel \parallel \parallel$  $\{\Leftrightarrow$ -elim on  $(k)\}$  $\{\Leftrightarrow$ -elim on  $(k)\}$ P⇒Q (m) (m)  $Q \Rightarrow P$ (k < m)(k < m)



# Derivations / Reasoning with quantifiers

# Proving a universal quantification

To prove

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

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

#### ∀ introduction

How do we prove a universal quantification?

#### ∀ introduction

How do we prove a universal quantification?

```
{Assume}
      \{\forall-intro on (k) and (I-I)\}
(I) \forall x[P(x):Q(x)]
```

#### **V** introduction

How do we prove a universal quantification?

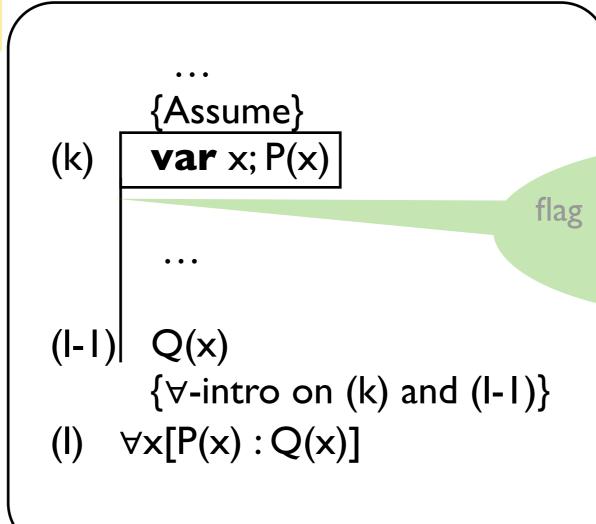
**∀-introduction** 

```
{Assume}
       var x; P(x)
(k)
      \{\forall-intro on (k) and (I-I)\}
(I) \forall x[P(x):Q(x)]
```

#### ∀ introduction

How do we prove a universal quantification?

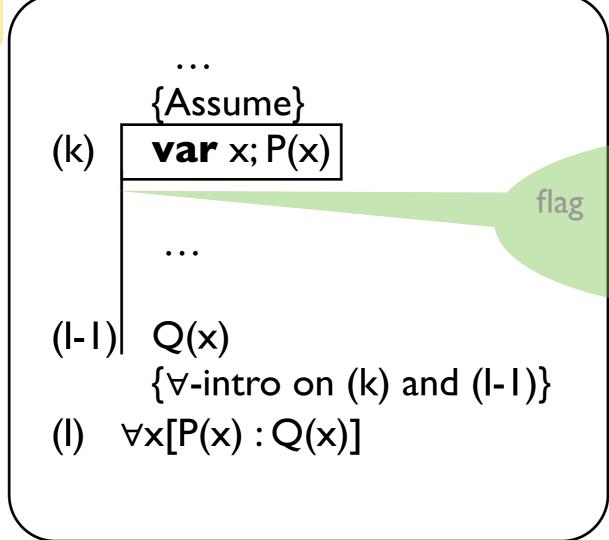
**∀-introduction** 



shows the validity of a hypothesis

How do we prove a universal quantification?

**∀-introduction** 



similar to ⇒-intro with generating hypothesis

shows the validity of a hypothesis

### Using a universal quantification

We know

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

### 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  $52387 \ge 2$ .

How do we use a universal quantification in a proof?

How do we use a universal quantification in a proof?

similar to implication but we need a witness

How do we use a universal quantification in a proof?

|| ||

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

 $\parallel \parallel$ 

(I) P(a)

|| || {∀-elim on (k) and (l)}

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

similar to implication but we need a witness

How do we use a universal quantification in a proof?

**∀-elimination** 

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

(I) P(a)

|| || {∀-elim on (k) and (l)}

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

similar to implication but we need a witness

How do we use a universal quantification in a proof? -

**∀-elimination** 

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

(I) P(a)

(m)

|| || {∀-elim on (k) and (l)}

(k < m, l < m)

similar to implication but we need a witness

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

How do we use a universal quantification in a proof? -

**∀-elimination** 

|| ||

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

(I) P(a)

(m) Q(a)

similar to implication but we need a witness

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

the same "a" from line (I)

(k < m, l < m)

How do we use a universal quantification in a proof?

**∀-elimination** 

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

(I) P(a)

similar to implication but we need a witness

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

the same "a" from line (I)

time for an example!

(k < m, l < m)

How do we prove an existential quantification?

How do we prove an existential quantification?

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

How do we prove an existential quantification?

```
{Assume}
(k)
        \{\exists-intro on (k) and (l-1)\}
(I) \exists x [P(x) : Q(x)]
```

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

How do we prove an existential quantification?

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

**3-introduction** 

```
{Assume}
(k)
        \forall x[P(x): \neg Q(x)]
(I-I)
        \{\exists-intro on (k) and (l-1)\}
(I) \exists x [P(x) : Q(x)]
```

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

How do we use an existential quantification in a proof?

How do we use an existential quantification in a proof?

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

How do we use an existential quantification in a proof?

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

and ¬elimination

How do we use an existential quantification in a proof?

(k)  $\exists x [P(x) : Q(x)]$ **(l)**  $\forall x[P(x): \neg Q(x)]$  $\{\exists$ -elim on (k) and (l) $\}$ (m)

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

and ¬elimination

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

How do we use an existential quantification in a proof?

**3-elimination** 

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

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

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

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

and ¬elimination

How do we use an existential quantification in a proof?

**3-elimination** 

|| ||

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

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

II II {∃-elim on (k) and (l)}

(m) F

(k < m, l < m)

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

and ¬- elimination

time for an example!

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

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

There are alternatives!

## Proving an existential quantification

To prove

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

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

## 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...

How do we prove an existential quantification?

How do we prove an existential quantification?

by finding a witness

How do we prove an existential quantification?

by finding a witness

```
(L) D(a)
```

• • •

(I) Q(a)

• • •

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

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

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

How do we prove an existential quantification?

∃\*-introduction

• • •

(k) P(a)

• • •

(I) Q(a)

• • •

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

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

by finding a witness

(k < m, l < m)

How do we prove an existential quantification?

∃\*-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

(k < m, l < m)

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

## Using an existential quantification

We know

 $\exists x[x \in \mathbb{R} : a - x < 0 < b - x]$ 

## 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.

How do we use an existential quantification in a proof?

How do we use an existential quantification in a proof?

we pick a witness

How do we use an existential quantification in a proof?

we pick a witness

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

 $\| \|$ 

 $\{\exists *-elim \ on \ (k)\}\$ (m) Pick x with P(x) and Q(x)

$$(k \le m)$$

How do we use an existential quantification in a proof?

∃\*-elimination

 $\| \|$ 

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

 $\| \|$ 

 $\{\exists *-elim \ on \ (k)\}\$ (m) Pick x with P(x) and Q(x) we pick a witness

(k < m)

How do we use an existential quantification in a proof?

**3\*-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!

 $(k \le m)$ 

How do we use an existential quantification in a proof?

∃\*-elimination

 $\| \|$ 

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

 $\parallel \parallel$ 

 $\{\exists *-elim on (k)\}$ 

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

we pick a witness

x must be new!

time for an example!

(k < m)