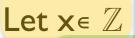
Proof by contradiction

Theorem

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

Proof



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

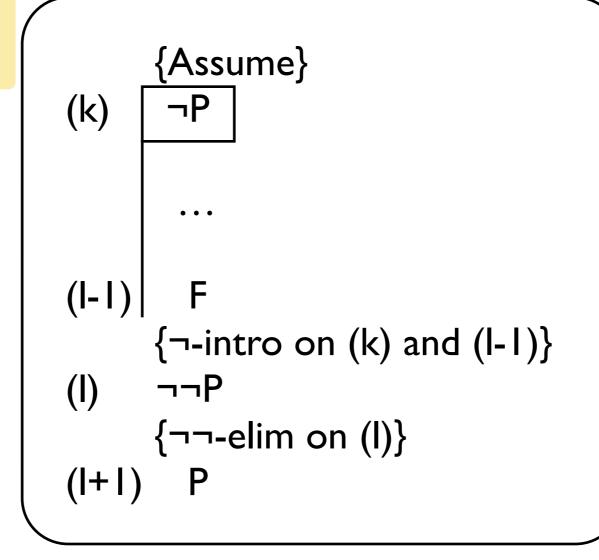
conclusion

Thanks to Bas Luttik

Proof by contradiction

How do we prove P by a contradiction?

proof by contradiction



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

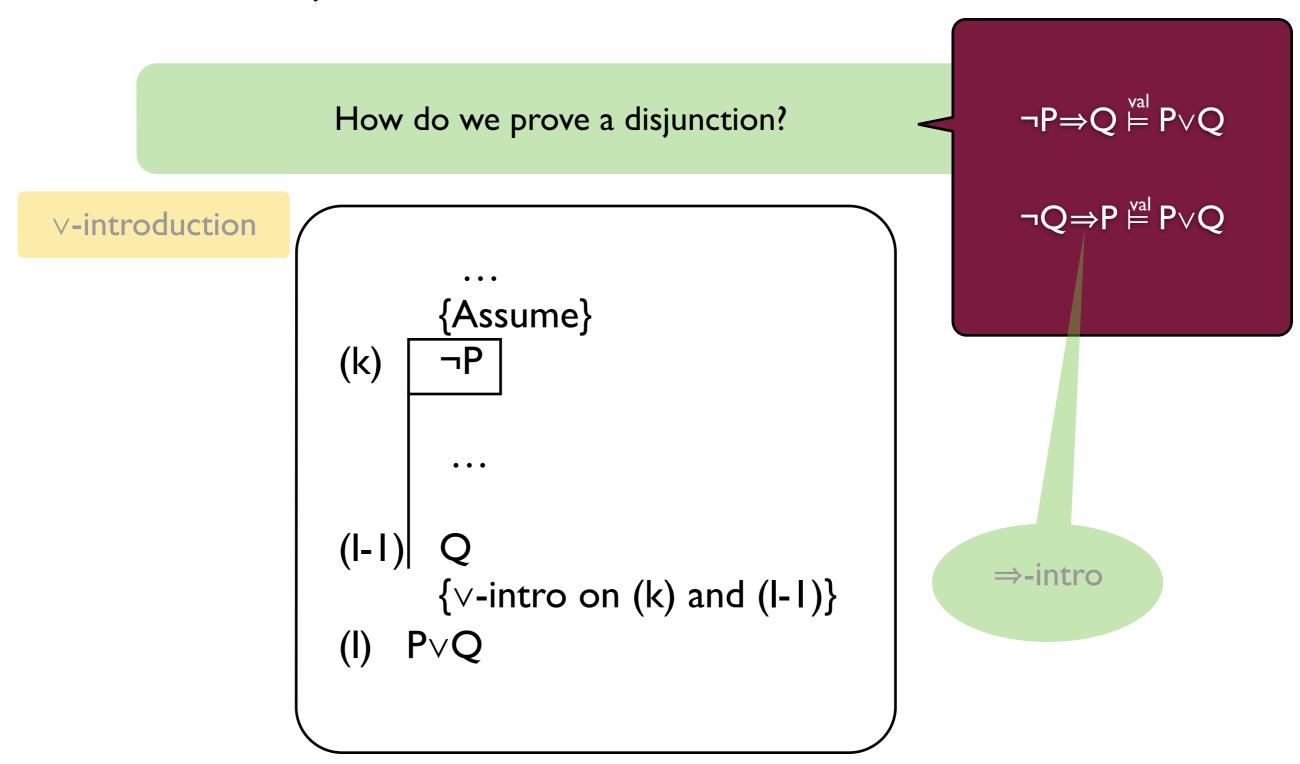
¬-intro

¬¬-elim

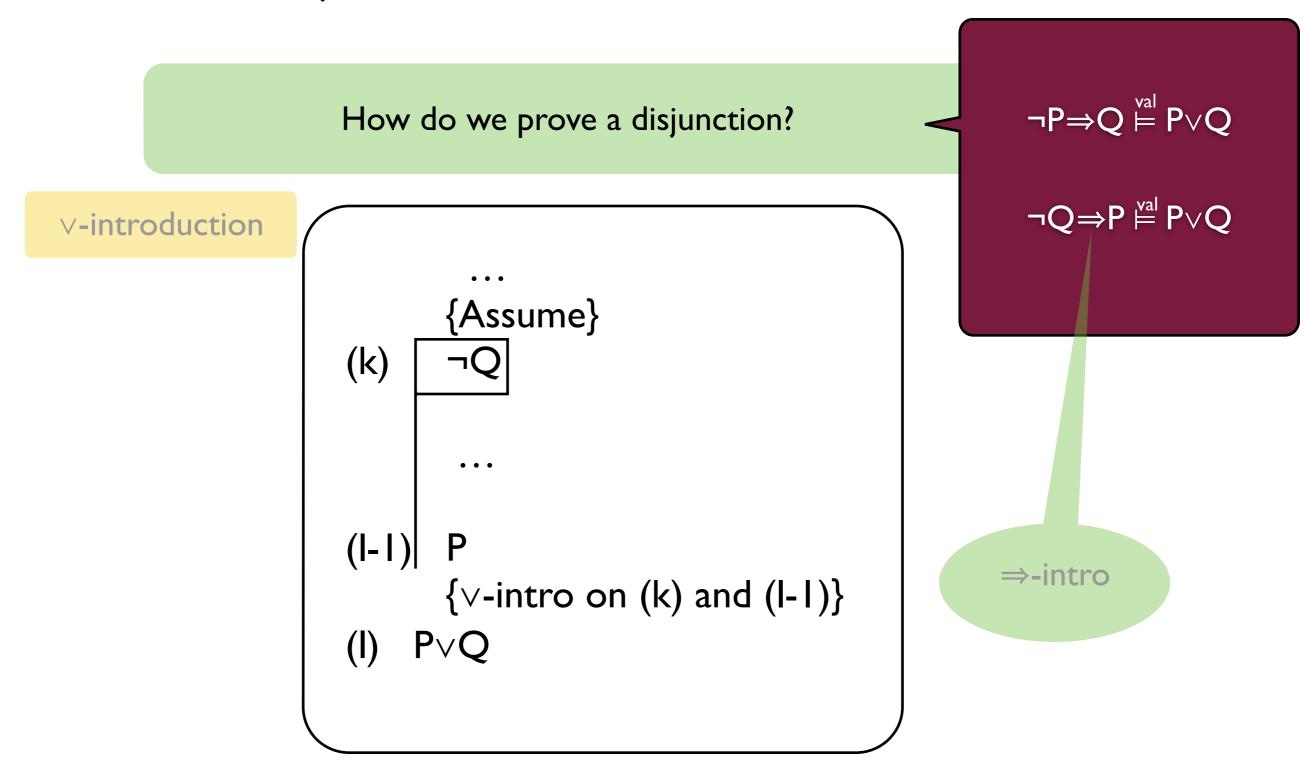
time for an example!

(k < m)

Disjunction introduction



Disjunction introduction



Disjunction elimination

How do we use a disjunction in a proof?

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

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

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

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

(m) $\neg P \Rightarrow Q$

Disjunction elimination

How do we use a disjunction in a proof?

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

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

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

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

(m) $\neg Q \Rightarrow P$

Proof by case distinction

How do we prove R by a case distinction?

proof by case distinction

|| ||

(k) $P\lor Q$

|| ||

) P⇒R

|| ||

(m) $Q \Rightarrow R$

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

(n) R

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

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

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) $Q \Rightarrow P$

• • •

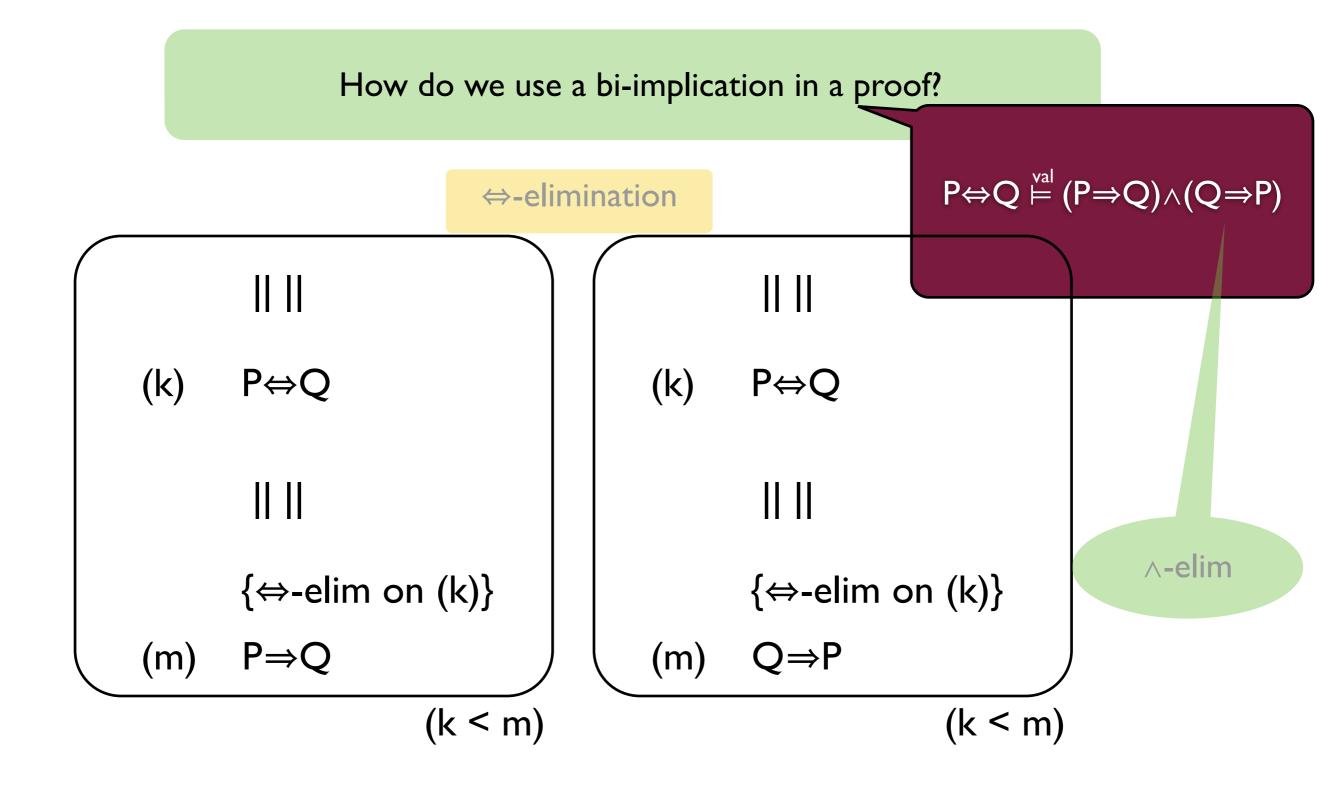
 $\{\Leftrightarrow$ -intro on (k) and (l) $\}$

(m) P⇔Q

(k < m, l < m)

∧-intro

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

∀ introduction

How do we prove a universal quantification? -

⇒-intro

similar to

with

generating hypothesis

∀-introduction

(k) var x; P(x)

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

|| ||

(I) P(a)

| II | I| {∀-elim on (k) and (l)} (m) Q(a)

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)

time for an example!

(k < m, l < m)

3 introduction

How do we prove an existential quantification?

3-introduction

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

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

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

(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...

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?

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

(k < m, l < m)

 \exists

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?

we pick a witness

|| ||

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

|| ||

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

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

x must be new!

time for an example!

(k < m)

 \exists