# CS4004/CS4504: FORMAL VERIFICATION

## Lecture 11: Proofs in First Order Logic and classical vs. intuitionistic logic

Vasileios Koutavas

School of Computer Science and Statistics
Trinity College Dublin

# Proofs in First Order Logic

# FIRST ORDER LOGIC RULES (1/2)

$$\frac{A_1 \qquad A_2}{A_1 \wedge A_2}\wedge i \qquad\qquad \frac{A_1 \wedge A_2}{A_1}\wedge e_1 \qquad\qquad \frac{A_1 \wedge A_2}{A_2}\wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2}\vee i_1 \qquad\qquad \frac{A_2}{A_1 \vee A_2}\vee i_2 \qquad\qquad \frac{A_1 \vee A_2 \qquad \boxed{\begin{array}{c} A_1 \\ \dots \\ B \end{array}} \qquad \boxed{\begin{array}{c} A_2 \\ \dots \\ B \end{array}}}{B}\vee e$$

$$\frac{\boxed{\begin{array}{c} A \\ \dots \\ B \end{array}}}{A \to B}\to i \qquad\qquad \frac{A \qquad A \to B}{B}\to e$$

$$\frac{A \qquad \neg A}{\bot}\neg e \qquad\qquad \frac{\boxed{\begin{array}{c} A \\ \dots \\ \bot \end{array}}}{\neg A}\neg i \qquad\qquad \frac{\bot}{A}\bot e \qquad\qquad \frac{\neg\neg A}{A}\neg\neg e^{*}$$

---

*Only in classical FOL

# FIRST ORDER LOGIC RULES (2/2)

$$\frac{}{t = t} =i \quad \text{(reflexivity)} \qquad\qquad \frac{t_1 = t_2 \qquad A[t_1/x]}{A[t_2/x]} =e$$

$$\frac{t_1 = t_2}{t_2 = t_1} =sym \qquad\qquad \frac{t_1 = t_2 \qquad t_2 = t_3}{t_1 = t_3} =trans$$

$$\frac{\forall x.A}{A[t/x]} \forall e \qquad \frac{\boxed{\begin{array}{l} x_0 \\ \quad \dots \\ \quad A[x_0/x] \end{array}}}{\forall x.A} \forall i$$

$$\frac{A[t/x]}{\exists x.A} \exists i \qquad \frac{\exists x.A \qquad \boxed{\begin{array}{lr} x_0 & A[x_0/x] \\ \dots & \\ C & \end{array}}}{C} \exists e$$

When we prove first order logic sequents we often use known theorems to shorten our proofs.

Some of these theorems we express as *derived rules*.

**Theorem (Law of Excluded Middle†)**

$\vdash A \vee \neg A$ *or equivalently* $$\dfrac{}{A \vee \neg A}\ \mathit{LEM}$$

**Theorem (Lemma†)**

$\vdash ((A \to B) \to A) \to A$

† Only in classical logic (stay tuned).

# USEFUL THEOREMS IN FIRST-ORDER LOGIC

Theorem

$$\neg\forall x.A \dashv\vdash \exists x.\neg A$$

$$\neg\exists x.A \dashv\vdash \forall x.\neg A$$

let $x$ not appear free in $B$. Then

$$\forall x.B \dashv\vdash B \qquad\qquad \exists x.B \dashv\vdash B$$

# MORE THEOREMS

let $x$ not appear free in $B$. Then

$$\forall x.B \dashv\vdash B \qquad \exists x.B \dashv\vdash B$$

$$(\forall x.A) \wedge B \dashv\vdash \forall x.(A \wedge B) \qquad (\exists x.A) \wedge B \dashv\vdash \exists x.(A \wedge B)$$

$$(\forall x.A) \vee B \dashv\vdash \forall x.(A \vee B) \qquad (\exists x.A) \vee B \dashv\vdash \exists x.(A \vee B)$$

let $x$ not appear free in $B$. Then

$$\forall x.B \dashv\vdash B \qquad \exists x.B \dashv\vdash B$$

$$(\forall x.A) \wedge B \dashv\vdash \forall x.(A \wedge B) \qquad (\exists x.A) \wedge B \dashv\vdash \exists x.(A \wedge B)$$

$$(\forall x.A) \vee B \dashv\vdash \forall x.(A \vee B) \qquad (\exists x.A) \vee B \dashv\vdash \exists x.(A \vee B)$$

$$\forall x.(B \to A) \dashv\vdash B \to (\forall x.A) \qquad \exists x.(B \to A) \dashv\vdash B \to (\exists x.A)$$

$$\forall x.(A \to B) \dashv\vdash (\exists x.A) \to B \qquad \exists x.(A \to B) \dashv\vdash (\forall x.A) \to B$$

# EVEN MORE THEOREMS

$$(\forall x.A) \wedge (\forall x.B) \dashv\vdash \forall x.(A \wedge B)$$

$$(\exists x.A) \vee (\exists x.B) \dashv\vdash \exists x.(A \vee B)$$

# EVEN MORE THEOREMS

$$(\forall x.A) \land (\forall x.B) \dashv\vdash \forall x.(A \land B)$$

$$(\exists x.A) \lor (\exists x.B) \dashv\vdash \exists x.(A \lor B)$$

$$\forall x.\forall y.A \dashv\vdash \forall y.\forall x.A$$

$$\exists x.\exists y.A \dashv\vdash \exists y.\exists x.A$$

# EVEN MORE THEOREMS

$$(\forall x.A) \wedge (\forall x.B) \dashv\vdash \forall x.(A \wedge B)$$

$$(\exists x.A) \vee (\exists x.B) \dashv\vdash \exists x.(A \vee B)$$

$$\forall x.\forall y.A \dashv\vdash \forall y.\forall x.A$$

$$\exists x.\exists y.A \dashv\vdash \exists y.\exists x.A$$

wrong: $\cancel{\forall x.\exists y.A \dashv\vdash \exists y.\forall x.A}$

wrong: $\cancel{\exists x.\forall y.A \dashv\vdash \forall y.\exists x.A}$

# Classical vs. Constructive logic

## FIRST ORDER LOGIC RULES (1/2)

$$\frac{A_1 \qquad A_2}{A_1 \wedge A_2}\wedge i \qquad \frac{A_1 \wedge A_2}{A_1}\wedge e_1 \qquad \frac{A_1 \wedge A_2}{A_2}\wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2}\vee i_1 \qquad \frac{A_2}{A_1 \vee A_2}\vee i_2 \qquad \frac{A_1 \vee A_2 \qquad \boxed{\begin{array}{c} A_1 \\ \cdots \\ B \end{array}} \qquad \boxed{\begin{array}{c} A_2 \\ \cdots \\ B \end{array}}}{B}\vee e$$

$$\frac{\boxed{\begin{array}{c} A \\ \cdots \\ B \end{array}}}{A \to B}\to i \qquad \frac{A \qquad A \to B}{B}\to e$$

$$\frac{A \qquad \neg A}{\bot}\neg e \qquad \frac{\boxed{\begin{array}{c} A \\ \cdots \\ \bot \end{array}}}{\neg A}\neg i \qquad \frac{\bot}{A}\bot e \qquad \frac{\neg\neg A}{A}\neg\neg e^{\ddagger}$$

‡Only in classical FOL

$$\frac{}{t = t} =i \quad \text{(reflexivity)} \qquad \frac{t_1 = t_2 \qquad A[t_1/x]}{A[t_2/x]} =e$$

$$\frac{t_1 = t_2}{t_2 = t_1} =sym \qquad \frac{t_1 = t_2 \qquad t_2 = t_3}{t_1 = t_3} =trans$$

$$\frac{\forall x.A}{A[t/x]} \forall e \qquad \frac{\boxed{\begin{array}{l} x_0 \\ \quad \dots \\ \quad A[x_0/x] \end{array}}}{\forall x.A} \forall i$$

$$\frac{A[t/x]}{\exists x.A} \exists i \qquad \frac{\exists x.A \qquad \boxed{\begin{array}{lr} x_0 & A[x_0/x] \\ \quad \dots & \\ \quad C & \end{array}}}{C} \exists e$$

Consider the formula

$$\exists x.(P(x) \to \forall y.P(y))$$

To prove this we need use rule $\exists i$ and provide a term $t$ for which we can show

$$(P(t) \to \forall y.P(y))$$

Consider the formula

$$\exists x.(P(x) \to \forall y.P(y))$$

To prove this we need use rule $\exists i$ and provide a term $t$ for which we can show

$$(P(t) \to \forall y.P(y))$$

Classically this is a tautology:

- If $\forall y.P(y)$ holds then we can pick arbitrarily term $t_0$ and show

  $$P(t_0) \to \forall y.P(y)$$

  using rule $\to i$ (also see truth table of implication).

Consider the formula

$$\exists x.(P(x) \rightarrow \forall y.P(y))$$

To prove this we need use rule $\exists i$ and provide a term $t$ for which we can show

$$(P(t) \rightarrow \forall y.P(y))$$

Classically this is a tautology:

- If $\forall y.P(y)$ holds then we can pick arbitrarily term $t_0$ and show

  $$P(t_0) \rightarrow \forall y.P(y)$$

  using rule $\rightarrow i$ (also see truth table of implication).
- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show

  $$P(t_1) \rightarrow \forall y.P(y)$$

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \rightarrow \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show

$$P(t_1) \rightarrow \forall y.P(y)$$

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \to \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show

$$P(t_1) \to \forall y.P(y)$$

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \rightarrow \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show
$$P(t_1) \rightarrow \forall y.P(y)$$
    - Assume logic's terms $\mathcal{F}$ contain natural numbers and predicates $\mathcal{P}$ standard predicates over them.
    - if $P(x) = \text{even}(x)$ then $t_1$ can be 3

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \to \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show

$$P(t_1) \to \forall y.P(y)$$

  - Assume logic's terms $\mathcal{F}$ contain natural numbers and predicates $\mathcal{P}$ standard predicates over them.
  - if $P(x) = \text{even}(x)$ then $t_1$ can be 3
  - if $P(x) = \text{odd}(x)$ then $t_1$ can be 4

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \to \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show

$$P(t_1) \to \forall y.P(y)$$

  - Assume logic's terms $\mathcal{F}$ contain natural numbers and predicates $\mathcal{P}$ standard predicates over them.
  - if $P(x) = \mathrm{even}(x)$ then $t_1$ can be 3
  - if $P(x) = \mathrm{odd}(x)$ then $t_1$ can be 4
  - if $P(x) = (x \leq 1000)$ then $t_1$ can be 1001

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \to \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show

$$P(t_1) \to \forall y.P(y)$$

  - Assume logic's terms $\mathcal{F}$ contain natural numbers and predicates $\mathcal{P}$ standard predicates over them.
  - if $P(x) = \text{even}(x)$ then $t_1$ can be 3
  - if $P(x) = \text{odd}(x)$ then $t_1$ can be 4
  - if $P(x) = (x \leq 1000)$ then $t_1$ can be 1001
  - ...

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \rightarrow \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show

$$P(t_1) \rightarrow \forall y.P(y)$$

  - Assume logic's terms $\mathcal{F}$ contain natural numbers and predicates $\mathcal{P}$ standard predicates over them.
  - if $P(x) = \text{even}(\text{x})$ then $t_1$ can be 3
  - if $P(x) = \text{odd}(\text{x})$ then $t_1$ can be 4
  - if $P(x) = (\text{x} \leq 1000)$ then $t_1$ can be 1001
  - ...
  - we can't provide a $t_1$ if we don't know $P$ and the parameters $\mathcal{F}, \mathcal{P}$

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \to \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show
$$P(t_1) \to \forall y.P(y)$$
  - Assume logic's terms $\mathcal{F}$ contain natural numbers and predicates $\mathcal{P}$ standard predicates over them.
  - if $P(x) = \text{even}(x)$ then $t_1$ can be 3
  - if $P(x) = \text{odd}(x)$ then $t_1$ can be 4
  - if $P(x) = (x \leq 1000)$ then $t_1$ can be 1001
  - ...
  - we can't provide a $t_1$ if we don't know $P$ and the parameters $\mathcal{F}, \mathcal{P}$
  - but there is always one.

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \rightarrow \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show

$$P(t_1) \rightarrow \forall y.P(y)$$

  - Assume logic's terms $\mathcal{F}$ contain natural numbers and predicates $\mathcal{P}$ standard predicates over them.
  - if $P(x) = \text{even}(\text{x})$ then $t_1$ can be 3
  - if $P(x) = \text{odd}(\text{x})$ then $t_1$ can be 4
  - if $P(x) = (\text{x} \leq 1000)$ then $t_1$ can be 1001
  - ...
  - we can't provide a $t_1$ if we don't know $P$ and the parameters $\mathcal{F}, \mathcal{P}$
  - but there is always one.
  - Classical logic is OK with that!

However notice how we didn't have to provide any concrete term $t_1$ in the second case to complete the proof of $\exists x.(P(x) \to \forall y.P(y))$

Let's see this again:

- If $\neg\forall y.P(y)$ then there exists a term $t_1$ such that $\neg P(t_1)$, which we can use to show

$$P(t_1) \to \forall y.P(y)$$

  - Assume logic's terms $\mathcal{F}$ contain natural numbers and predicates $\mathcal{P}$ standard predicates over them.
  - if $P(x) = \mathrm{even}(\mathrm{x})$ then $t_1$ can be 3
  - if $P(x) = \mathrm{odd}(\mathrm{x})$ then $t_1$ can be 4
  - if $P(x) = (\mathrm{x} \leq 1000)$ then $t_1$ can be 1001
  - ...
  - we can't provide a $t_1$ if we don't know $P$ and the parameters $\mathcal{F}$, $\mathcal{P}$
  - but there is always one.
  - Classical logic is OK with that!
  - Constructive logic is not! It requires us to give a concrete $t_1$, before we know what $P$ is.

**Theorem**

*There are irrational $a$ and $b$ for which $a^b$ is rational.*

**Proof.**

We know that $\sqrt{2}$ is irrational (known theorem of arithmetic which we will not prove here).

Suppose $\sqrt{2}^{\sqrt{2}}$ is rational. Then pick $a = b = \sqrt{2}$ and we're done.

Otherwise $\sqrt{2}^{\sqrt{2}}$ is irrational. Pick $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$.

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

which is rational. $\square$

**Theorem**

*There are irrational $a$ and $b$ for which $a^b$ is rational.*

**Proof.**

We know that $\sqrt{2}$ is irrational (known theorem of arithmetic which we will not prove here).

Suppose $\sqrt{2}^{\sqrt{2}}$ is rational. Then pick $a = b = \sqrt{2}$ and we're done.

Otherwise $\sqrt{2}^{\sqrt{2}}$ is irrational. Pick $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$.

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

which is rational. $\square$

Correct but we never identified two definitely irrational numbers $a$ and $b$.

# EXAMPLE CLASSICAL PROOF

**Theorem**

*There are irrational $a$ and $b$ for which $a^b$ is rational.*

**Proof.**

We know that $\sqrt{2}$ is irrational (known theorem of arithmetic which we will not prove here).

Suppose $\sqrt{2}^{\sqrt{2}}$ is rational. Then pick $a = b = \sqrt{2}$ and we're done.

Otherwise $\sqrt{2}^{\sqrt{2}}$ is irrational. Pick $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$.

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

which is rational. $\square$

Correct but we never identified two definitely irrational numbers $a$ and $b$. In fact knowing whether $\sqrt{2}^{\sqrt{2}}$ is rational is a difficult problem!

Consider the predicate

$$A(n,m) \stackrel{\text{def}}{=} ((\{n\}(n)\downarrow) \rightarrow (m=0)) \quad \wedge \quad ((m=0) \rightarrow (\{n\}(n)\downarrow))$$

where $\{n\}(n)\downarrow$ means "the $n^{th}$ turing machine given $n$ as an input terminates".

Prove: $\forall x.\exists y.A(x,y)$

**Proof.**

We need to use rule $\forall i$, and prove for arbitrary $n$: $\exists y.A(n,y)$

Consider the predicate

$$A(n, m) \stackrel{\text{def}}{=} ((\{n\}(n)\downarrow) \to (m = 0)) \quad \wedge \quad ((m = 0) \to (\{n\}(n)\downarrow))$$

where $\{n\}(n)\downarrow$ means "the $n^{th}$ turing machine given $n$ as an input terminates".

Prove: $\forall x.\exists y.A(x, y)$

**Proof.**

We need to use rule $\forall i$, and prove for arbitrary $n$: $\exists y.A(n, y)$ If $\{n\}(n)\downarrow$ then pick $y = 0$.

Otherwise pick $y = 1$. $\square$

Consider the predicate

$$A(n,m) \stackrel{\text{def}}{=} ((\{n\}(n)\downarrow) \to (m=0)) \quad \wedge \quad ((m=0) \to (\{n\}(n)\downarrow))$$

where $\{n\}(n)\downarrow$ means "the $n^{th}$ turing machine given $n$ as an input terminates".

Prove: $\forall x.\exists y.A(x,y)$

**Proof.**

We need to use rule $\forall i$, and prove for arbitrary $n$: $\exists y.A(n,y)$ If $\{n\}(n)\downarrow$ then pick $y=0$.

Otherwise pick $y=1$. $\square$

- → Here we can think of the two cases as appealing to some oracle that knows the truth of turing machine termination. Our proof works by case analysis on what the oracle would answer.
- → Constructive logic does not want to have proofs involving appealing to an oracle.
- → Constructive proofs can be translated into programs!

The rule that allows us to do classical proofs is this:

$$\frac{\neg\neg A}{A}\ \neg\neg e$$

This rule is in fact equivalent to the following rules:

$$\frac{}{A \vee \neg A}\ \text{LEM(Law of Excluded Middle)} \qquad \frac{\boxed{\begin{array}{c}\neg A \\ \cdots \\ \bot\end{array}}}{A}\ \text{PBC(Proof by contradictio}$$

$$((A \to B) \to A) \to A$$

In fact from any of the 3 we can derive the other two.

Prove LEM using $\neg\neg e$

$$\vdash A \vee \neg A$$

$$\frac{\neg\neg A}{A}\ \neg\neg e$$

# CLASSICAL PROOF 2

Prove using $\neg\neg e$

$$\vdash ((A \to B) \to A) \to A$$

$$\frac{\neg\neg A}{A}\ \neg\neg e$$

Prove using LEM

$$\vdash ((A \to B) \to A) \to A$$

$$\dfrac{}{A \vee \neg A}\ \text{LEM}$$

# CLASSICAL PROOF 4

Prove using PBC

$$\vdash ((A \to B) \to A) \to A$$

$$\dfrac{\boxed{\begin{array}{c} \neg A \\ \cdots \\ \bot \end{array}}}{A}\ \mathrm{PBC}$$

Prove the following using PBC

$$\neg\forall x.A \vdash \exists x.\neg A$$

$$\cfrac{\boxed{\begin{array}{c}\neg A\\ \cdots\\ \bot\end{array}}}{A}\ \text{PBC}$$

Prove the following using $\neg\neg e$

$$\neg\forall x.A \vdash \exists x.\neg A$$

$$\frac{\neg\neg A}{A}\ \neg\neg e$$

Prove the following using LEM

$$\neg\forall x.A \vdash \exists x.\neg A$$

$$\dfrac{}{A \vee \neg A}\ \text{LEM}$$