CS4004/CS4504: FORMAL VERIFICATION

Lecture 10: First Order Logic

Vasileios Koutavas

School of Computer Science and Statistics
Trinity College Dublin
LAST LECTURE
As in propositional logic, in FOL:

→ We will use **natural deduction rules** to define the axioms of the logic.

→ We will symbolically prove the validity of **sequents**: $A_1, \ldots, A_n \vdash B$
All propositional logic rules are rules of FOL:

\[
\begin{align*}
\frac{A_1}{A_1 \land A_2} & \quad \land i \\
\frac{A_1 \land A_2}{A_1} & \quad \land e_1 \\
\frac{A_1 \land A_2}{A_2} & \quad \land e_2
\end{align*}
\]

\[
\begin{align*}
\frac{A_1}{A_1 \lor A_2} & \quad \lor i_1 \\
\frac{A_2}{A_1 \lor A_2} & \quad \lor i_2 \\
\frac{A_1 \lor A_2}{B} & \quad \lor e
\end{align*}
\]

\[
\begin{align*}
\frac{A \quad \ldots \quad B}{A \rightarrow B} & \quad \rightarrow i \\
\frac{A \quad \ldots \quad B}{A \rightarrow B} & \quad \rightarrow e
\end{align*}
\]

\[
\begin{align*}
\frac{A \quad \ldots \quad \bot}{\neg A} & \quad \neg i \\
\frac{\bot}{\neg A} & \quad \neg e
\end{align*}
\]

\[
\begin{align*}
\frac{\bot}{\bot} & \quad \bot e \\
\frac{\neg A}{A} & \quad \neg e^*
\end{align*}
\]

*Only in classical FOL*
We often work with a set of predicates \( \mathcal{P} \) which contains at least one special binary predicate: \textit{equality}.

→ That is equality \textit{between terms}. (there is no equality between predicates)

→ \textbf{Notation:} We will write this predicate in infix notation: \( t_1 = t_2 \).

\[
\begin{align*}
&\quad \\ &t = t \quad \text{(reflexivity)} \\
\end{align*}
\]

\[
\begin{align*}
&\quad \\ &t_1 = t_2 \quad A[t_1/x] \\
&\phantom{t_1} = e \\
&\phantom{A[t_1/x]} A[t_2/x]
\end{align*}
\]

† Proofs are the same as before with small extensions (stay tuned).
We often work with a set of predicates $\mathcal{P}$ which contains at least one special binary predicate: equality.

→ That is equality **between terms.** (there is no equality between predicates)

→ **Notation:** We will write this predicate in infix notation: $t_1 = t_2$.

\[
\begin{align*}
\frac{}{t = t} & \quad = i \quad \text{(reflexivity)} \\
\frac{t_1 = t_2}{A[t_1/x]} & \quad = e \\
\end{align*}
\]

→ Equality as we know it is **symmetric** and **transitive.** Prove $^\dagger$ the following **derivable rules** (theorems):

\[
\begin{align*}
\frac{t_1 = t_2}{t_2 = t_1} & \quad = \text{sym} \\
\frac{t_1 = t_2}{t_1 = t_3} & \quad = \text{trans}
\end{align*}
\]

i.e., prove the FOL sequents $(t_1 = t_2 \vdash t_2 = t_1)$ and $(t_1 = t_2, \ t_2 = t_3 \vdash t_2 = t_1)$

$^\dagger$Proofs are the same as before with small extensions (stay tuned).
Assume the set of natural numbers $\mathcal{F} = \{0, +1\}$ where $+1$ is a postfix unary function. Assume the usual arithmetic predicates over natural numbers $\mathcal{P} = \{=, <, >, \leq, \geq, \ldots\}$.

Prove:

\[ t_1 = t_2 \vdash (t + t_2) = (t + t_1) \]
Assume a FOL over natural numbers. Prove:

\[ x + 1 = 1 + x, \quad (x + 1) > 1 \rightarrow x > 0 \quad \vdash \quad (1 + x) > 1 \rightarrow (x > 0) \]
TODAY: ∀ AND ∈
Universal quantification

Elimination rule:

\[
\forall x. A \quad \frac{}{\forall e \quad A[t/x]}
\]
Universal quantification

Elimination rule:

\[ \forall x. A \quad \forall e \]

\[ \frac{\forall x. A}{A[t/x]} \]

→ Remember that substitution should not capture variables of the substitutee term. Suppose we work with natural numbers and have in our assumptions:

\[ \forall x. \exists y. x < y \]

If substitution allowed to capture variables then by applying \( \forall e \) we could replace \( x \) with \( y \) and get \( \exists y. y < y \), which would be a contradiction in a sound system about arithmetic.

→ Barendreght convention doesn’t let us use the same symbol for a “free” \( y \) and a “bound” \( y \). (there are other ways to deal with this, besides the B.Conv.)
Prove:

\[ P(t), \ [\forall x (P(x) \rightarrow \neg Q(x))] \vdash \neg Q(t) \]
Introduction rule:

$x_0$

\[ \ldots \]

\[ A[x_0/x] \]

\[ \forall x. A \]

\[ \forall i \]

→ The box stipulates the existence of a **dummy variable** $x_0$
→ $x_0$ should be **fresh**: doesn’t appear elsewhere in the proof.
→ $x_0$ represents an **arbitrary term**
→ Thus, to prove $\forall x. A$ we need to prove $A[x_0/x]$ for an arbitrary term $x_0$
Prove in FOL over some $\mathcal{F}$ and $\mathcal{P}$:

$$\forall x. (P(x) \rightarrow Q(x)), \forall x. P(x) \vdash \forall x. Q(x)$$
Introduction rule:

\[
\frac{A[t/x]}{\exists x.A} \exists i
\]

→ Pick an convenient \( t \) and prove \( A[t/x] \).
Existential quantification

Elimination rule:

\[ \exists x. A \quad \frac{x_0}{C} \quad A[x_0/x] \]

- Pick a fresh \( x_0 \) and prove \( A[x_0/x] \).
- \( x_0 \) should be **fresh**: doesn't appear elsewhere in the proof.
- \( x_0 \) represents an **unknown term**
Prove

∀x.A ⊢ ∃x.A

∀x.A ⊢ ∀e

A[t/x]

A[x_0/x]

∀x.A

∀i

∃x.A ⊢ ∃e

A[t/x]

C

∀x.A

∃i

∃x.A

C

∃e
Prove

\( \forall x. (P(x) \rightarrow Q(x)), \ \exists x. P(x) \vdash \exists x. Q(x) \)
all FOL rules
FIRST ORDER LOGIC RULES (1/2)

\[
\begin{align*}
\frac{A_1 \quad A_2}{A_1 \land A_2} & \land i \\
\frac{A_1 \land A_2}{A_1} & \land e_1 \\
\frac{A_1 \land A_2}{A_2} & \land e_2 \\
\frac{A_1}{A_1 \lor A_2} & \lor i_1 \\
\frac{A_2}{A_1 \lor A_2} & \lor i_2 \\
\frac{A_1 \lor A_2}{B} & \lor e \\
\frac{A \quad A \rightarrow B}{A \rightarrow B} & \rightarrow i \\
\frac{A \rightarrow B}{B} & \rightarrow e \\
\frac{A \quad \bot}{\bot} & \neg e \\
\frac{\bot}{\neg A} & \neg i \\
\frac{\neg A}{A} & \neg e^+ \\
\end{align*}
\]

\[\text{Only in classical FOL}\]

17
FIRST ORDER LOGIC RULES (2/2)

\[
\begin{align*}
\text{reflexivity} & : t = t \\
\text{symmetry} & : t_1 = t_2 \quad t_2 = t_1 \\
\text{universal quantifier} & : \forall x.A \quad \forall e \quad A[t/x] \\
\text{existential quantifier} & : \exists x.A \quad \exists e \quad A[t/x]
\end{align*}
\]
Assume the set of natural numbers $\mathcal{F} = \{0, +1\}$ where $+1$ is a postfix unary function. Assume the usual arithmetic predicates over natural numbers $\mathcal{P} = \{=, <, >, \leq, \geq, \ldots\}$.

Assume the **axiom:** 

\[
\begin{align*}
x &< x + 1 \\
\end{align*}
\]

Express and prove in FOL over $\mathcal{F}$ and $\mathcal{P}$:

“Any natural number is smaller than some number”
“If all quakers are reformists and if there is a protestant who is also a quaker, then there must be a protestant who is also a reformist.”

$$\forall x. (Q(x) \rightarrow R(x)), \exists y. (P(y) \land Q(y)) \vdash \exists x. (P(x) \land R(x))$$
Prove the following lemmas

\[ \neg \forall x. A \vdash \exists x. \neg A \]

\[ \neg \exists x. A \vdash \forall x. \neg A \]
let $x$ not appear free in $B$. Then

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

$$(\forall x. A) \lor B \vdash \forall x. (A \lor B)$$

$$(\exists x. A) \land B \vdash \exists x. (A \land B)$$

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

$$\forall x. (A \rightarrow B) \vdash (\exists x. A) \rightarrow B$$

$$\forall x. (B \rightarrow A) \vdash B \rightarrow (\forall x. A)$$

$$\exists x. (A \rightarrow B) \vdash (\forall x. A) \rightarrow B$$

$$\exists x. (B \rightarrow A) \vdash B \rightarrow (\exists x. A)$$
(∀x.A) ∧ (∀x.B) ⊢ ∀x.(A ∧ B)

(∃x.A) ∨ (∃x.B) ⊢ ∃x.(A ∨ B)

∀x.∀y.A ⊢ ∀y.∀x.A

∃x.∃y.A ⊢ ∃y.∃x.A