CS4004/CS4504: FORMAL VERIFICATION

Lecture 10: First Order Logic

Vasileios Koutavas

School of Computer Science and Statistics
Trinity College Dublin

Last lecture

SYMBOLIC PROOFS IN FOL

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:

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

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

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

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

*Only in classical FOL

EQUALITY RULES

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: $t_1 = t_2$.

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

EQUALITY RULES

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: $t_1 = t_2$.

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

- Equality as we know it is **symmetric** and **transitive**. Prove † the following **derivable rules** (theorems):

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

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

†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:

$$t_1 = t_2 \vdash (t + t_2) = (t + t_1)$$

EXAMPLE

Assume a FOL over natural numbers. Prove:

$$[x+1=1+x],\ [(x+1)>1 \to x>0] \vdash (1+x)>1 \to (x>0)$$

TODAY: $\forall$ AND $\exists$

Elimination rule:

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

UNIVERSAL QUANTIFICATION

Elimination rule:

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

- 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.)

EXAMPLE

Prove:

$$P(t),\ [\forall x(P(x) \to \neg Q(x))] \ \vdash \ \neg Q(t)$$

Introduction rule:

$$\dfrac{\boxed{\begin{array}{l} x_0 \\ \quad\quad \cdots \\ \quad A[x_0/x] \end{array}}}{\forall x.A}\ \forall i$$

- 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 $\mathcal{P}$:

$$[\forall x.(P(x) \to Q(x))],\ [\forall x.P(x)] \ \vdash \ \forall x.Q(x)$$

Introduction rule:

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

→ Pick an convenient t and prove $A[t/x]$.

EXISTENTIAL QUANTIFICATION

Elimination rule:

$$\dfrac{\exists x.A \qquad \boxed{\begin{array}{lcr} x_0 & & A[x_0/x] \\ & \cdots & \\ & C & \end{array}}}{C}\ \exists e$$

- 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

EXAMPLE

Prove

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

$$\frac{\forall x.A}{A[t/x]}\ \forall e \qquad \frac{\boxed{\begin{array}{l} x_0 \\ \quad \cdots \\ \quad A[x_0/x] \end{array}}}{\forall x.A}\ \forall i \qquad \frac{A[t/x]}{\exists x.A}\ \exists i \qquad \frac{\exists x.A \qquad \boxed{\begin{array}{lr} x_0 & A[x_0/x] \\ \multicolumn{2}{c}{\cdots} \\ \multicolumn{2}{c}{C} \end{array}}}{C}\ \exists e$$

Prove

$$\forall x.(P(x) \to Q(x)),\quad \exists x.P(x) \quad \vdash \quad \exists x.Q(x)$$

$$\frac{\forall x.A}{A[t/x]}\ \forall e \qquad \frac{\boxed{\begin{array}{l} x_0 \\ \quad\cdots \\ \quad A[x_0/x] \end{array}}}{\forall x.A}\ \forall i \qquad \frac{A[t/x]}{\exists x.A}\ \exists i \qquad \frac{\exists x.A \qquad \boxed{\begin{array}{lr} x_0 & A[x_0/x] \\ \multicolumn{2}{c}{\cdots} \\ \multicolumn{2}{c}{C} \end{array}}}{C}\ \exists e$$

all FOL rules

FIRST ORDER LOGIC RULES (1/2)

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

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

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

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

‡Only in classical FOL

FIRST ORDER LOGIC RULES (2/2)

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

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

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

$$\frac{A[t/x]}{\exists x.A} \exists i \qquad \frac{\exists x.A \qquad \boxed{\begin{array}{lr} x_0 & A[x_0/x] \\ \multicolumn{2}{c}{\cdots} \\ \multicolumn{2}{c}{C} \end{array}}}{C} \exists e$$

EXAMPLE

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**: $\dfrac{}{x < x + 1}$ <+1

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

"Any natural number is smaller than some number"

EXAMPLE

"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."

$$\forall x.(Q(x) \to R(x)), \;\; \exists y.(P(y) \wedge Q(y)) \vdash \exists x.(P(x) \wedge R(x))$$

Prove the following lemmas

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

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

let x not appear free in B. Then

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

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

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

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

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

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

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

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

EVEN MORE EQUIVALENCES

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

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

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

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