# CS4004/CS4504: FORMAL VERIFICATION

Lecture 10: First Order Logic

Vasileios Koutavas



School of Computer Science and Statistics Trinity College Dublin



### SYMBOLIC PROOFS IN FOL

# As in propositional logic, in FOL:

- → We will use natural deduction rules to define the axioms of the logic.
- $\rightarrow$  We will symbolically prove the validity of sequents:  $A_1, \dots A_n \vdash B$

### PROPOSITIONAL RULES

All propositional logic rules are rules of FOL:

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

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \vee i \qquad \frac{A_1 \wedge A_2}{B} \wedge e$$

$$\frac{A}{A_1 \wedge A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \vee i_2 \qquad \frac{A_1 \wedge A_2}{B} \wedge e$$

$$\frac{A}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{B} \wedge e$$

$$\frac{A}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{B} \wedge e$$

$$\frac{A}{A_1 \wedge A_2} \wedge i \qquad \frac{A_1 \wedge A_2}{B} \wedge e$$

<sup>\*</sup>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:  $t_1 = t_2$ .

$$\frac{1}{t=t}=i$$
 (reflexivity) 
$$\frac{t_1=t_2}{A[t_1/x]}=e$$

### **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:  $t_1 = t_2$ .

$$\frac{1}{t=t} = i \quad \text{(reflexivity)} \qquad \qquad \frac{t_1 = t_2 \quad A[t_1/x]}{A[t_2/x]} = e$$

→ Equality as we know it is **symmetric** and **transitive**. Prove <sup>†</sup> the following **derivable rules** (theorems):

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

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

<sup>&</sup>lt;sup>†</sup>Proofs are the same as before with small extensions (stay tuned).

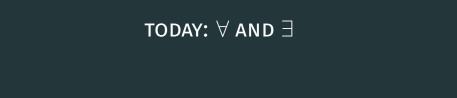
Assume the set of natural numbers  $\mathcal{F} = \{0, +1\}$  where +1 is a postfix unary function. Assume the usual arithmetic predicates over natural numbers  $\mathcal{P} = \{=, <, >, \leq, \geq, \ldots\}$ .

Prove:

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

Assume a FOL over natural numbers. Prove:

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



## **UNIVERSAL QUANTIFICATION**

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.)

Prove:

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

### UNIVERSAL QUANTIFICATION

#### Introduction rule:



- $\rightarrow$  The box stipulates the existence of a dummy variable  $x_0$
- $\rightarrow$   $x_0$  should be **fresh**: doesn't appear elsewhere in the proof.
- $\rightarrow x_0$  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  $\mathcal{P}$ :

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

### **EXISTENTIAL QUANTIFICATION**

Introduction rule:

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

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

### **EXISTENTIAL QUANTIFICATION**

### Elimination rule:



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

Prove

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

$$\frac{\forall x.A}{A[t/x]} \ \forall e \qquad \frac{\begin{bmatrix} x_0 & & & \\ & \ddots & \\ & A[x_0/x] & \\ \hline \forall x.A & \forall i & \frac{A[t/x]}{\exists x.A} \ \exists i & \frac{\exists x.A}{C} & \frac{C}{C} \end{bmatrix} \ \exists e$$

Prove

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

$$\frac{\forall x.A}{A[t/x]} \forall e \qquad \frac{\begin{bmatrix} x_0 & & & \\ & \ddots & \\ & & A[x_0/x] \end{bmatrix}}{\forall x.A} \forall i \qquad \frac{A[t/x]}{\exists x.A} \exists i \qquad \frac{\exists x.A}{C} \qquad \frac{C}{C}$$



# FIRST ORDER LOGIC RULES (1/2)

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

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \vee e_2$$

$$\frac{A_1}{A_1 \vee A_2} \vee i_1 \qquad \frac{A_2}{A_1 \vee A_2} \vee i_2 \qquad \frac{A_1 \vee A_2}{B} \vee e_2$$

$$\frac{A_1}{A_1 \vee A_2} \wedge e \qquad \frac{A_1}{A_1 \vee A_2} \wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2} \wedge e \qquad \frac{A_1 \vee A_2}{A_1 \vee A_2} \wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2} \wedge e \qquad \frac{A_1 \vee A_2}{A_1 \vee A_2} \wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2} \wedge e \qquad \frac{A_1 \vee A_2}{A_1 \vee A_2} \wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2} \wedge e \qquad \frac{A_1 \vee A_2}{A_1 \vee A_2} \wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2} \wedge e \qquad \frac{A_1 \vee A_2}{A_1 \vee A_2} \wedge e_2$$

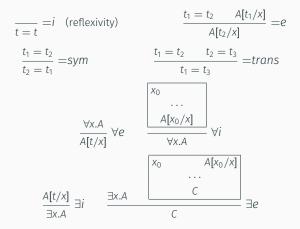
$$\frac{A_1}{A_1 \vee A_2} \wedge e \qquad \frac{A_1 \vee A_2}{A_1 \vee A_2} \wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2} \wedge e \qquad \frac{A_1 \vee A_2}{A_1 \vee A_2} \wedge e_2$$

$$\frac{A_1}{A_1 \vee A_2} \wedge e \qquad \frac{A_1 \vee A_2}{A_1 \vee A_2} \wedge e_2$$

<sup>&</sup>lt;sup>‡</sup>Only in classical FOL

# FIRST ORDER LOGIC RULES (2/2)



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

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."

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

### **EQUIVALENCES**

Prove the following lemmas

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

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

### MORE EQUIVALENCES

let x not appear free in B. Then

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

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

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

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

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

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

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

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

### **EVEN MORE EQUIVALENCES**

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