CS4004/CS4504: FORMAL VERIFICATION

Lecture 9: First Order Logic

Vasileios Koutavas

School of Computer Science and Statistics
Trinity College Dublin

TERMS

FOL reasons about the properties of terms

Terms in FOL are strings from the syntax:

$$t ::= x \mid c \mid f(t, \ldots, t)$$

A term can be:

- a variable
  - e.g.: $x, y, z, \ldots$

TERMS

FOL reasons about the properties of terms

Terms in FOL are strings from the syntax:

$$t ::= x \mid c \mid f(t, \ldots, t)$$

A term can be:

- a variable
  - e.g.: $x, y, z, \ldots$
- a constant c, AKA a nullary function (a function with zero arguments)
  - e.g.: *andy*, *mary*, ...
  - we pick constants from a set $\mathcal{F}$ of functions

TERMS

FOL reasons about the properties of terms

Terms in FOL are strings from the syntax:

$$t ::= x \mid c \mid f(t, \dots, t)$$

A term can be:

- a variable
  - e.g.: $x, y, z, \dots$
- a constant c, AKA a nullary function (a function with zero arguments)
  - e.g.: *andy*, *mary*, ...
  - we pick constants from a set $\mathcal{F}$ of functions
- an application of an n-ary ($n > 0$) function f to n terms $t_1, \dots, t_n$
  - e.g. natural numbers: $zero, succ(zero), succ(succ(zero)), succ(x), \dots$
  - we pick functions from the same set $\mathcal{F}$

FOL reasons about the properties of terms

Formulas in FOL are strings from the syntax:

$$A ::= P(t_1, \dots, t_n) \mid (\neg A) \mid (A \wedge A) \mid (A \vee A) \mid (A \rightarrow A) \mid \forall x.A \mid \exists x.A$$

A formula can be:

- an application of a predicate P with arity $n > 0$ to terms $t_1, \dots, t_n$
  - e.g.: $I(mary), Y(andy, x)$
  - we pick constants from a set $\mathcal{P}$

FOL reasons about the properties of terms

Formulas in FOL are strings from the syntax:

$$A ::= P(t_1, \ldots, t_n) \mid (\neg A) \mid (A \wedge A) \mid (A \vee A) \mid (A \rightarrow A) \mid \forall x.A \mid \exists x.A$$

A formula can be:

- an application of a predicate P with arity $n > 0$ to terms $t_1, \ldots, t_n$
  - e.g.: $I(mary), Y(andy, x)$
  - we pick constants from a set $\mathcal{P}$
- if A, B are formulas then so are $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$

FOL reasons about the properties of terms

Formulas in FOL are strings from the syntax:

$$A ::= P(t_1, \ldots, t_n) \ | \ (\neg A) \ | \ (A \wedge A) \ | \ (A \vee A) \ | \ (A \rightarrow A) \ | \ \forall x.A \ | \ \exists x.A$$

A formula can be:

- an application of a predicate P with arity $n > 0$ to terms $t_1, \ldots, t_n$
  - e.g.: $I(mary), Y(andy, x)$
  - we pick constants from a set $\mathcal{P}$
- if A, B are formulas then so are $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$
- if A is a formula and x is a variable then $\forall x.A$ and $\exists x.A$ are formulas.

$$
\begin{aligned}
t, f &\in \mathcal{F} \\
P &\in \mathcal{P} \\
t &::= x \mid c \mid f(t, \ldots, t) \\
A &::= P(t_1, \ldots, t_n) \mid (\neg A) \mid (A \wedge A) \mid (A \vee A) \mid (A \to A) \mid \forall x.A \mid \exists x.A
\end{aligned}
$$

binding priorities:

$\neg$, $\forall x$, $\exists x$ bind more tightly than
$\wedge$ and $\vee$ which bind more tightly than
$\to$ which is right-associative

FOL formulas are syntax trees where

- all the **leaves** are terms
- all **nodes above leaves** are predicates
- and all **other internal nodes** are operators

Express in FOL and write as a syntax tree the following:

"every son of my father is my brother"

"For every natural number i within the domain of array A, the value of A at i is larger than or equal to the value of A at every j less than i"

$$
\begin{aligned}
c, f &\in \mathcal{F} \\
P &\in \mathcal{P} \\
t &::= x \mid c \mid f(t, \ldots, t) \\
A &::= P(t_1, \ldots, t_n) \mid (\neg A) \mid (A \wedge A) \mid (A \vee A) \mid (A \rightarrow A) \mid \forall x.A \mid \exists x.A
\end{aligned}
$$

We can use FOL to reason about

- natural numbers: $\mathcal{F} = \{0, succ, \ldots\}$, large enough $\mathcal{P}$
- booleans: $\mathcal{F} = \{\top, \bot, \ldots\}$, large enough $\mathcal{P}$

$$
\begin{aligned}
c, f &\in \mathcal{F} \\
P &\in \mathcal{P} \\
t &::= x \mid c \mid f(t, \ldots, t) \\
A &::= P(t_1, \ldots, t_n) \mid (\neg A) \mid (A \wedge A) \mid (A \vee A) \mid (A \rightarrow A) \mid \forall x.A \mid \exists x.A
\end{aligned}
$$

We can use FOL to reason about

- natural numbers: $\mathcal{F} = \{0, succ, \ldots\}$, large enough $\mathcal{P}$
- booleans: $\mathcal{F} = \{\top, \bot, \ldots\}$, large enough $\mathcal{P}$
- propositional logic: $\mathcal{F} = \emptyset$ and $\mathcal{P} = \{p, q, r \ldots\}$

Universal ($\forall$) and existential ($\exists$) quantification allow us to express interesting properties of an infinite number of terms.

- "Every student is younger than some instructor": $\forall x.(Student(x) \rightarrow \exists y.(Instructor(y) \wedge Younger(x, y)))$
- "Not all birds can fly": $\neg\forall x.(Bird(x) \rightarrow CanFly(x))$
- "every son of my father is my brother": $\forall x.\forall y.(Son(x, y) \wedge Father(y, me) \rightarrow Brother(x, me))$

Write the following as syntax trees:

- "Every student is younger than some instructor": $\forall x.(Student(x) \rightarrow \exists y.(Instructor(y) \land Younger(x, y)))$
- "Not all birds can fly": $\neg \forall x.(Bird(x) \rightarrow CanFly(x))$
- "every son of my father is my brother": $\forall x.\forall y.(Son(x, y) \land Father(y, me) \rightarrow Brother(x, me))$

Definition

- $\forall x.A$ binds the variable x in A
  - the scope of variable x is A
  - x is bound in $\forall x.A$
  - x is free in A
- $\exists x.A$ binds the variable x in A
  - the scope of variable x is A
  - x is bound in $\exists x.A$
  - x is free in A
- any variable x which appears in a formula A and is **not bound in** A is called free in A

VARIABLE SCOPE

Definition

- $\forall x.A$ binds the variable x in A
  - the scope of variable x is A
  - x is bound in $\forall x.A$
  - x is free in A
- $\exists x.A$ binds the variable x in A
  - the scope of variable x is A
  - x is bound in $\exists x.A$
  - x is free in A
- any variable x which appears in a formula A and is **not bound in** A is called free in A

Example: find the free and bound variables

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

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

CONVENTION

Barendreght convention: To avoid confusion, **every bound variable will be distinct from any other bound variable and all the free variables.**

$$\forall x.((P(x) \to Q(y)) \wedge \exists z.(\mathrm{x}' \wedge z))$$

We will need to replace variables for actual terms.

*Substitution is defined in detail in LiCS 2.2.3 & 2.2.4. The book **does not use the Barendreght convention** thus substitution $A[t/x]$ is more complicated to avoid binders in A binding free variables in t.

SUBSTITUTION

We will need to replace variables for actual terms.

We will only replace **free variables**

[*] Substitution is defined in detail in LiCS 2.2.3 & 2.2.4. The book **does not use the Barendreght convention** thus substitution $A[t/x]$ is more complicated to avoid binders in A binding free variables in t.

We will need to replace variables for actual terms.

We will only replace **free variables**

Definition

$A[t/x]$ is defined to be the formula we get by replacing all **free occurrences** of x in A with t.

*Substitution is defined in detail in LiCS 2.2.3 & 2.2.4. The book **does not use the Barendreght convention** thus substitution $A[t/x]$ is more complicated to avoid binders in A binding free variables in t.

We will need to replace variables for actual terms.

We will only replace **free variables**

Definition

$A[t/x]$ is defined to be the formula we get by replacing all **free occurrences** of x in A with t.

Example: what is $A[john/y]$ and $A[Y(john, x)/y]$ when A is:

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

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

$$\forall x.((P(x) \rightarrow Q(y)) \wedge \exists z.(x \wedge z))$$

(These formulas do not respect the Barendreght convention.)

*Substitution is defined in detail in LiCS 2.2.3 & 2.2.4. The book **does not use the Barendreght convention** thus substitution $A[t/x]$ is more complicated to avoid binders in A binding free variables in t.

We will need to replace variables for actual terms.

We will only replace **free variables**

Definition

$A[t/x]$ is defined to be the formula we get by replacing all **free occurrences** of x in A with t.

Example: what is $A[john/y]$ and $A[Y(john, x)/y]$ when A is:

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

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

$$\forall x.((P(x) \to Q(y)) \wedge \exists z.(x \wedge z))$$

(These formulas do not respect the Barendreght convention.)

Using the Barendreght convention there is no danger of **binding** any variables of $Y(john, x)$ when we substitute $A[Y(john, x)/y]$. *

---

*Substitution is defined in detail in LiCS 2.2.3 & 2.2.4. The book **does not use the Barendreght convention** thus substitution $A[t/x]$ is more complicated to avoid binders in A binding free variables in t.

FOL Proof Theory: natural deduction

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: $A_1, \ldots A_n \vdash B$

PROPOSITIONAL RULES

All propositional logic rules are rules of FOL:

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

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

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

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

† Only in classical FOL

EQUALITY RULES

We will work with sets of predicates $\mathcal{P}$ which contain 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: $t_1 = t_2$.
- We will have the following rules (axioms) for equality:

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

EQUALITY RULES

We will work with sets of predicates $\mathcal{P}$ which contain 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: $t_1 = t_2$.
- → We will have the following rules (axioms) for equality:

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

- → 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 $\mathcal{F} = \{0, 1, 2, \ldots, +\}$ where $+$ is an infix binary 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:

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