CS438/2404

Lecture 3

- HW1: DUE THIS FRIDAY!
- OFFICE HOURS TODAY 5-6 and Wednesday
- HW2: OUT THIS FRIDAY, DUE OCT 18

Submit PDF to: noahfleming@cs.toronto.edu by deadline
OR: submit hardcopy at beginning of tutorial
TODAY

• First Order Logic
  Language/Syntax
  Semantics: Models

• Sound & Complete Proof Systems for FO Logic
  LK (extension of sequent calculus PK)
  FO Resolution (extension of Resolution)
FIRST ORDER LOGIC

Underlying language \( L \) specified by:

1. \( \forall n \in \mathbb{N} \) a set of \( n \)-ary function symbols (i.e., \( \cdot, f, g, h, +, \cdot \))

   0-ary function symbols are called constants

2. \( \forall n \in \mathbb{N} \) a set of \( n \)-ary predicate symbols (i.e., \( P, Q, R, <, \leq \))

Plus:
- Variables: \( x, y, z, \ldots a, b, c, \ldots \) \{ Built in symbols \}
- \( \neg, \lor, \land, \forall, \exists, \forall \)
- Parenthesis (, )
**Example** \( L_A \) (language of arithmetic)

\[ L_A = \{ 0, s, +, \cdot; = \} \]

- **function symbols**: 0, s, +, \cdot
- **relation symbols**: =

- 0 constant (0-ary function symbol)
- s unary function symbol
- +, \cdot binary function symbols
- = binary predicate symbol
Terms over $L$

(1) Every variable is a term

(2) If $f$ is an $n$-ary function symbol, and $t_1, \ldots, t_n$ terms, then $f(t_1, \ldots, t_n)$ is a term
Terms over $L$

1. Every variable is a term.
2. If $f$ is an $n$-ary function symbol, and $t_1, \ldots, t_n$ terms, then $f(t_1, \ldots, t_n)$ is a term.

Examples of terms ($0, s, f, +, *$)

- $0, s, f, +, *$
- $f(s(s, s)), + f(y, z), * + a b s$
- $f(s(s, s)), + f(y, z), * + a b s$
**FIRST ORDER FORMULAS OVER \( L \)**

(1) \( P t_1 \ldots t_n \) is an atomic \( L \)-formula, where \( P \) is an \( n \)-ary predicate in \( L \), and \( t_1 \ldots t_n \) are terms over \( L \).

(2) If \( A, B \) are \( L \)-formulas, so are

\( \neg A \), \( (A \land B) \), \( (A \lor B) \), \( \forall x A \), \( \exists x A \).
Example: FO Formulas over $\mathcal{L}_A$

1) Existence of infinitely many primes

$$\forall x \exists y \ (y > x \text{ and } y \text{ is prime})$$
Example: FO Formulas over $\mathcal{L}_A$

1. Existence of infinitely many primes

Want to say: $\forall x \exists y \ (y > x \text{ and } y \text{ is prime})$

$y \text{ is prime} : \forall z, z' \ (z, z' \geq 2 \implies z \cdot z' \neq y)$
Example: FO Formulas over $\mathbb{Z}_A$

1. Existence of infinitely many primes

want to say: $\forall x \exists y \ (y > x \text{ and } y \text{ is prime})$

$y \text{ is prime} : \forall z, z' \ (z, z' > 2 \implies z \cdot z' \neq y)$

$(\star) \left[ \forall z \forall z' \left( (0 \leq z') \wedge (0 < z) \wedge (z \neq z') \wedge (0 < z') \right) \right] \implies \not \exists y$
Example: FO Formulas over \( \mathcal{L}_A \)

1. Existence of infinitely many primes

want to say: \( \forall x \exists y \ (y > x \text{ and } y \text{ is prime}) \)

\( y \text{ is prime} : \forall z, z' \ (z, z' \geq 2 \Rightarrow z \cdot z' \neq y) \)

\[ (*) \left[ \forall z \forall z' \ (z, z' \geq 2 \Rightarrow z \cdot z' \neq y) \right] \]

\[ (*) (*) \left[ y > x : \forall z, z' \ (z, z' \geq 2 \Rightarrow z \cdot z' \neq y) \right] \]
The existence of infinitely many primes:

Let $x$ be a prime number. Then there exists a prime number $y$ such that $y > x$.

This can be formulated as:

$$\exists x \forall y (y > x \land y \text{ is prime})$$

Example: For formulas over $\forall$
Example: FO Formulas over $\mathcal{L}_A$

2 Twin Prime Conjecture

There exists infinitely many pairs of numbers, $(x, x')$ such that $x' = x + 2$ and both $x$ and $x'$ are prime.
Example: 50 Formulas in $L_{\mathcal{A}}$

(3) Fermat's Last Theorem

$$\forall n \geq 3 \forall a, b, c \ (n > 2 \Rightarrow a^n + b^n \neq c^n)$$
Example: If \( a \), \( b \), \( c \) are positive integers such that

\[ a^3 + b^3 = c^3, \]

then it is impossible to have

\[ A_n = 3 A_{a, b, c}. \]

Fermat’s Last Theorem

Ancient Greek text, 3rd century AD
Fermat's Last Theorem

Example: Fo Formulas in

$V_2 \neq 3$

conjectured by Fermat 1637

in margin of his copy of

Arithmetic
Fermat's Last Theorem

Fermat's equation:

$$x^n + y^n = z^n$$

This equation has no solutions in integers for $n \geq 3$.

Finally proven by Andrew Wiles.
Example: Fo Formulas in LaTeX

3 Fermat’s Last Theorem (actually Andrew Wiles’ theorem)

\[ \forall n \geq 3 \ ( \forall a, b, c \ a^n + b^n \neq c^n ) \]

Problem: How to say \( a^n \)?

(we’ll see later how to do this!)
FREE/BOUND VARIABLES

• An occurrence of $x$ in $A$ is bound if $x$ is in a subformula of $A$ of the form $\forall xB$, or $\exists xB$ (otherwise $x$ is free in $A$)

  Example: $\exists y (x = y + y)$
  $P \land \forall x (\neg (x + 5x = x))$

• A formula/term is closed if it contains no free variables

• A closed formula is called a sentence
SEMANTICS OF FO LOGIC

An \( \mathcal{L} \)-structure \( M \) (or model) consists of:

1. A nonempty set \( M \) called the universe (variables range over \( M \))

2. For every \( n \)-ary function symbol \( f \) in \( \mathcal{L} \), an associated function \( f^M : M^n \rightarrow M \)

3. For each \( n \)-ary relation symbol \( P \) in \( \mathcal{L} \), an associated relation \( P^M \subseteq M^n \)

* Equality predicate \( = \) is always true equality relation on \( M \).
Example

\[ L_A = \{ 0, s, +, \cdot, \} \]

0. \underline{IN}: standard model of \( L_A \)

\[ M = \mathbb{N} \]
\[ 0 = 0 \in \mathbb{N} \]
\([+, \cdot, s]\) are usual plus, times, successor functions

Jumping ahead a bit: Evaluation of a formula in \( \mathbb{N} \)

\[ \forall x \forall z ( \exists \bar{z} \forall \bar{z} \bar{z} = x + z) \rightarrow \exists \bar{z}'' ( \bar{z}'' + \bar{z}'' = x ) \]
Example

\[ L_A = \{0, s, t, \cdot, i\} = \{0, 1, 2, 3\} \]

1. \[ M = \mathbb{N} \quad \text{O} = 0 \in \mathbb{N} \]
   - \( s \): successor. i.e., \( s(0) = 1 \), \( s(1) = 2 \), etc.
   - \( t \): plus. i.e., \( t(0) = 1 \), \( t(2, 3) = 5 \), etc.
   - \( \cdot \): times

2. \[ M = \{\text{□}, \text{●}, \text{★}\} \quad \text{O} = \text{□} \]

\[ s(\text{□}) = \text{●} \]
\[ s(\text{●}) = \text{★} \]
\[ s(\text{★}) = \text{★} \]
How to evaluate formulas that contain free variables?

**Defn** An object assignment $\sigma$ for a model $M$ is a mapping from variables to $M$. 
Definition: Evaluation of terms/formulas on $M, s$

Let $M$ be an $L$-structure, $s$ an object assignment for $M$.

Evaluation of terms over $M, s$:

1. $x^M \in M$ is $s(x)$ for all variables $x$.
2. $(f t_1 \ldots t_n)^M \in_M [s] = f^M(t_1^M[s], \ldots, t_n^M[s])$.
Evaluation of formulas over $\mathcal{M}, \sigma$

Let $A$ be an $\mathcal{L}$-formula. $\mathcal{M} \models A[\sigma]$

(M satisfies $A$ under $\sigma$) iff

(a) $\mathcal{M} \models \Pi t_1, \ldots, t_n[\sigma]$ iff $\langle t_1^\mathcal{M}[\sigma], \ldots, t_n^\mathcal{M}[\sigma] \rangle \in P^\mathcal{M}$

(b) $\mathcal{M} \models (s = t)[\sigma]$ iff $s^\mathcal{M}[\sigma] = t^\mathcal{M}[\sigma]$

(c) $\mathcal{M} \models \neg A[\sigma]$ iff not $\mathcal{M} \models A[\sigma]$

(d) $\mathcal{M} \models (A \lor B)[\sigma]$ iff $\mathcal{M} \models A[\sigma]$ or $\mathcal{M} \models B[\sigma]$

(e) $\mathcal{M} \models (A \land B)[\sigma]$ iff $\mathcal{M} \models A[\sigma]$ and $\mathcal{M} \models B[\sigma]$

(f) $\mathcal{M} \models \forall x A[\sigma]$ iff $\forall m \in M \mathcal{M} \models A[\sigma(\sigma x)]$

(g) $\mathcal{M} \models \exists x A[\sigma]$ iff $\exists m \in M \mathcal{M} \models A[\sigma(\sigma x)]$
Example \( \mathcal{L} = \{ ; \, \wedge, = \} \)

\[ M = ( \mathbb{N}^\ast; \leq, = ) \]

\[ R^M(m,n) \text{ iff } m \leq n \]

Then

\[ M \models \forall x \exists y \, R(x, y) \]

\[ M \not\models \exists y \, \forall x \, R(x, y) \]

\[ \text{satisfiable by } M \]

\[ \exists y \, \forall x \, R(x, y) \]

is also satisfiable.
**IMPORTANT DEFINITIONS**

0. A is **satisfiable** if there exists a model $M$ and an object assignment $g$ such that $M \models A[g]$.

2. A set of formulas $\Phi$ is **satisfiable** if $\exists M, g$ such that $M \models \Phi[g]$ [for all $A \in \Phi$].

3. $\Phi \models A$ (A is a logical consequence of $\Phi$) if $\forall M, g$ if $M \models \Phi[g]$ then $M \models A[g]$.

$\Delta A$ (A is valid) if $\forall M, g$ $M \models A[g]$. 
4. $A \iff B$ (A and B are logically equivalent)
   iff $\forall M \forall \phi M \models A$ iff $M \models B$
Examples

1. \((\forall x P_x \lor \forall x Q_x) \Longleftrightarrow \forall x (P_x \lor Q_x)\)

2. \(\forall x (A_x \lor B_x) \not\Longleftrightarrow \forall x A_x \lor \forall x B_x\)

\(\mathcal{L} = \{\emptyset, P, Q, A, B\}\)
Example

Earlier formula \( A : \)

\[
\forall x \forall z \exists z' \ 
\left( x = z' + z \land (z' = 0 \lor z' = -x) \right) \supset
\exists z'' \left( sz + z'' = x \right)
\]

says for every \( x,z \) if \( x \geq z \) then
we can write \( x \) as \((z+1)+z''\) for some \( z'' \)

- true when \( M = \emptyset \) so \( A \) is satisfiable
- false when \( M = \left( M = \{0,1,2\} \right. \left. \left. \begin{array}{c}
0+0 = 0 \\
1+0 = 1 \\
2+0 = 2 \\
\forall \text{ all others}
\end{array}
\right) \right) \)

\[
\begin{align*}
x &= 2 \\
z &= 0 \\
z' &= 2
\end{align*}
\]
Example

\[ \forall x \forall y \ (f(x) = f(y)) \implies x = y \]

No

Let \( M = [0, 1] \)

\( M: \quad f(0) = 0 \)
\( f(1) = 0 \)

Then \( M = \forall x \forall y \ (f(x) = f(y)) \)
but \( M \not\subseteq x = y \) (since \( 0 \not= 1 \))
Substitution

Let $s, t$ be $L$-terms.

$t(s/x)$: substitute $x$ everywhere by $s$

$A(s/x)$: substitute all free occurrences of $x$ in $A$ by $s$

$t = \text{\texttt{+ s s o} x}

\text{\texttt{t(+) y z)}: + ss o + y z

\text{\texttt{s s o} + (y +)}
Substitution

Let $s, t$ be $L$-terms.

$t(s/x)$: substitute $x$ everywhere by $s$

$A(s/x)$: substitute all free occurrences of $x$ in $A$ by $s$

Lemma: $(t(s/x))^M[G] = t^M[G(x \stackrel{s^M[G]}{\mapsto} x)]$

- substitute $x$ for $s$
- obtain new object assignment $G'$ where $G'(x) = s^M$
- then evaluate $t$ under $M, G'$
- then evaluate $t'$ under $M, G'$

substitute $x$ for $s$

obtain new object assignment $G'$ where $G'(x) = s^M$

Then evaluate $t$ under $M, G'$
Substitution Cont’d

Need to be more careful when making substitutions into formulas

Example: $A : \forall y \varphi (x = y + y)$

$A(\frac{x+y}{x}) : \forall y \varphi (x + y = y + y)$

Defn term $t$ is freely substitutable for $x$ in $A$ iff there is no subformula in $A$ of the form $\forall y \varphi B$ or $\exists y \varphi B$ where $y$ occurs in $t$
Substitution Theorem

If \( t \) is freely substitutable for \( x \) in \( A \) then \( \forall M \forall a \)

\[ M \models A(t/x)[a] \text{ iff } M \models A[a](t^m/x) \]
Easy way to avoid this problem (of making a “bad” substitution):

2 types of variables
free variables $a, b, c, \ldots$
bound variables $x, y, z, \ldots$

**Proper formula**: every free variable occurrence is of type free, and every bound variable occurrence is of type bound

**Proper term**: no variables of type bound
Lines are again sequents

\[ A_1, \ldots, A_k \rightarrow B_1, \ldots, B_e \] 

where each \( A_i \), \( B_j \) is a proper \( L \)-formula

\[ A_s : A_1 \land A_2 \land \ldots \land A_k \rightarrow B_1 \lor \ldots \lor B_e \]
First order sequent calculus LK

Lines are again sequents

\[ A_1, \ldots, A_k \rightarrow B_1, \ldots, B_L \]

where each \( A_i \), \( B_j \) is a proper \( L \)-formula.

Rules

Old rules of PK

Plus new rules for \( \forall, \exists \)

like a large AND

Large OR
New Logical Rules for $\forall, \exists$

**$\forall$-left**

\[
\frac{A(t), \Gamma \Rightarrow \Delta}{\forall x \ A(x), \Gamma \Rightarrow \Delta}
\]

**$\forall$-right**

\[
\frac{\Gamma \Rightarrow \Delta, \ A(b)}{\Gamma \Rightarrow \Delta, \ \forall x \ A(x)}
\]

**$\exists$-left**

\[
\frac{A(b), \Gamma \Rightarrow \Delta}{\exists x \ A(x), \Gamma \Rightarrow \Delta}
\]

**$\exists$-right**

\[
\frac{\Gamma \Rightarrow \Delta, \ A(t)}{\Gamma \Rightarrow \Delta, \ \exists x \ A(x)}
\]

* $A, t$ are proper
* $b$ is a free variable not appearing in lower sequent of rule
Example of an LK proof

\[
\begin{align*}
\text{Pa} & \Rightarrow \text{Pa} \\
\text{Pa, Qa} & \Rightarrow \text{Pa} \\
\text{Pa} \land \text{Qa} & \Rightarrow \text{Pa} \\
\text{Pa} \land \text{Qa} & \Rightarrow \exists x \ P x \\
\exists (P x \land Q x) & \Rightarrow \exists x \ P x \\
\exists (P x \land Q x) & \Rightarrow \exists x \ P x \land \exists x \ Q x
\end{align*}
\]
**SOUNDNESS**

**Defn** A first order sequent \( A_1, \ldots, A_k \to B_1, \ldots, B_e \) is valid if and only if its associated formula \((A_1 \land \ldots \land A_k) \to (B_1 \lor \ldots \lor B_e)\) is valid.

**Soundness Theorem for LK** Every sequent provable in LK is valid.
Proof of Lemma

Go through each rule.

Example: $\forall$-right rule

Let $\Gamma' = B_1 \ldots B_e$
$\Delta = C_1 \ldots C_{l'}$

$A : B_1 \land \ldots \land B_e \Rightarrow \exists v \ldots \exists C_{l'} \land A(x)$

$A_L : B_1 \land \ldots \land B_e \Rightarrow \exists v \ldots \exists C_{l'} \land A(x)$

Note: $A$ cannot occur in lower sequent $\Gamma' \Rightarrow \Delta$, thus $A$ cannot occur in any sequent $\Gamma' \Rightarrow \Delta$.
Theorem (LK Soundness)

Every sequent provable in LK is valid

Proof by induction on the number of sequents in proof.

Axiom $A \rightarrow A$ is valid

Induction step: use previous soundness lemma.