Announcements

- HW1 out tomorrow
  (Due Oct 11)
LAST CLASS

• Another proof system for propositional logic: PK
  Soundness of PK
  Completeness of PK

• Propositional Compactness Theorem

Pages 9–17 of Lecture Notes
Today

• Propositional Compactness Theorem (Finish)

• First Order Logic
  Language/Syntax
  Semantics: Models

(pages 18-27 of course notes)
**Definition** Let $\Phi$ be a set of sequents, $S$ a sequent. A $\text{PK} - \Phi$ proof of $S$ is a $\text{PK}$-proof of $S$ from $\Phi$ and axioms of $\text{PK}$. (also written as $\Phi \vdash S$)

**Theorem** Let $\Phi$ be a set of (possibly infinite) sequents. Then $\Phi = S \iff S$ has a (finite) $\text{PK} - \Phi$ proof

$\Phi = S \iff \Phi \vdash S$
Propositional Compactness

**Theorem** (Form 2, see notes for 2 other equivalent forms)

Let $\Phi$ be a set of (possibly infinite) formulas $\Phi \models A$ iff $A$ is a logical consequence of a finite subset of $\Phi$

We'll assume this for now and prove it after proof of 3 equivalent forms of compactness as homework
Proof (Derivational Soundness/Completeness)

By compactness, it suffices to prove the case where $\Phi$ is finite.

- Let $\Phi = \{ S_1, \ldots, S_k \}$, and suppose $\Gamma \Rightarrow \Delta$ is a logical consequence of $\{ S_1, \ldots, S_k \}$. Thus
  
  $$(\ast) \quad \Gamma, A_{S_1}, \ldots, A_{S_k} \Rightarrow \Delta \quad \text{is valid}$$

- Thus by PK completeness, $(\ast)$ has a PK proof.

  Derive $\Gamma \Rightarrow \Delta$ from $(\ast)$ and $\Rightarrow A_{S_1}, \ldots, A_{S_k}$.
Derive $\Gamma \Rightarrow \Delta$ from $\{ \rightarrow A_{s_1}, \rightarrow A_{s_2}, \rightarrow A_{s_3}, (*) \}$
Proof (Propositional Compactness)

Suppose \( \Phi \models A \). Then \( \Phi, \neg A \) is unsatisfiable.

Show: If \( \psi \) is UNSAT, then some finite subset of \( \psi \) is UNSAT (Form 1)

Pf sketch: Assume the set of underlying atoms in \( \psi \) is countable: \( P_1, P_2, \ldots \).

- Make decision tree that queries \( P_i \) at layer 1, then \( P_j \) at layer 2, etc.
• Each path in $T$ corresponds to a complete truth assignment

• Prune $T$ to $T'$:
  
  For every node $v$ of $T$, remove subtree rooted below $v$ if partial truth assignment from root to $v$ falsifies some formula $f \in \Psi$. Label $v$ by $f$

• Every path in $T'$ is finite (since $\Psi$ unsat, so $\forall$ truth ass to all vars, some $f \in \Psi$ is falsified, and each $f \in \Psi$ is finite)

• By König's Lemma, $T'$ is finite
König's Lemma. If $T'$ is a rooted binary tree, where every branch/path of $T$ is finite, then $T'$ is finite.

Thus, the formulas $\psi' \subseteq \psi$ labelling the leaves of $T'$ form a finite subset of $\varnothing \psi$, and thus $\psi'$ is unsat + finite subset of $\psi$. 

FIRST ORDER LOGIC

Underlying language $L$ specified by:

1. A set of $n$-ary function symbols (i.e., $f, g, h, +, \cdot$)
   - 0-ary function symbols are called constants

2. A set of $n$-ary predicate symbols (i.e., $P, Q, R, <, \leq$)

Plus:
- Variables: $x, y, z, \ldots a, b, c, \ldots$
- $\neg, \vee, \wedge, \exists, \forall$
- Parentheses ($, )$

Built in symbols
Example 1 $L_A$ (language of arithmetic)

$L_A = \{ 0, s, +, \cdot ; = \}$

- function symbols
- relation symbols

0 constant (0-ary function symbol)

s unary function symbol

+, \cdot binary function symbols

= binary predicate symbol
Terms over $\mathcal{L}$

(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 \( \mathcal{L} \)

(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, 1, s, f, +, •)

\[
\begin{align*}
\text{0-ary} &: 0, s, f, +, \cdot \\
\text{Unary} &: f(0), f(s(x)), f(y) \\
\text{Binary} &: t + f(y, z), t \\
\end{align*}
\]
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 $
eg A$, $(A \land B)$, $(A \lor B)$, $A \land A$, $\exists x A$.
Example: Propositional formulas are FO Formulas

$\mathcal{L}^{\text{prop}}$:

1. No function symbols
2. 0-ary predicate symbols $P_1, P_2, \ldots$ (are propositional atoms)

Plus $\land, \lor, \neg, (),$,

Since there are no function symbols, and all predicate symbols have 0-arity, propositional formulas have no variables, terms, or $\forall, \exists$. 
Example: FO Formulas over \( \mathbb{Z}_A \)

1. Existence of infinitely many primes

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

1. Existence of infinitely many primes

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

\[ y \text{ is prime} : \forall z, z' (z, z' \geq 2 \Rightarrow z \cdot z' \neq y) \]
Example: FO Formulas over \( \mathbb{A} \)

1. Existence of infinitely many primes

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

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

   \( \left( \forall z \forall z' \left( \left( z \neq 0 \vee z' \neq 0 \right) \land \left( z = 2 \lor z' = 2 \right) \Rightarrow (z \cdot z' = y) \right) \right) \)

   \( \Rightarrow (y = \gamma) \)

   \( A \rightarrow B \) abbreviates \( \neg A \lor B \)
Example: FO Formulas over $\mathbb{Z}_A$

1. Existence of infinitely many primes

<table>
<thead>
<tr>
<th>want to say: $\forall x \exists y$ ($y &gt; x$ and $y$ is prime)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$y$ is prime: $\forall z, z'$ ($z, z' \geq 2 \Rightarrow z \cdot z' \neq y$)</td>
</tr>
<tr>
<td>(**) $\forall z, z'$ ($z, z' \geq 2 \Rightarrow z \cdot z' \neq y$)</td>
</tr>
<tr>
<td>(**) $\forall z \forall z'$ ($z, z' \geq 2 \Rightarrow z \cdot z' \neq y$)</td>
</tr>
<tr>
<td>(**) $y &gt; x$ : $\exists y$ such that $y = x + w$ (where $w = y$)</td>
</tr>
</tbody>
</table>
Example: FO Formulas over $\mathcal{L}_A$

1. Existence of infinitely many primes

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

A: $\forall z, z' \left( z, z' \geq 2 \implies z \cdot z' \neq y \right)$

$\forall z \forall z' \left( \neg (z = 0) \land \neg (z = 50) \land \neg (z' = 0) \land \neg (z' = 50) \right) \implies \neg (z \cdot z' = y)$

B: $\neg (x = y) \land \exists w \left( x + w = y \right)$

Whole thing: $\forall x \exists y \left( \star \right) \land \left( \star \star \right)$
Example: FO Formulas over $\mathbb{Z}_A$

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: Fo Formulas in LaTeX

(3) Fermat’s Last Theorem

\[ \forall n \geq 3 \forall a, b, c (n > 2 \implies a^n + b^n \neq c^n) \]
Fermat's Last Theorem

$$A^n + B^n = C^n$$

any integer for which $$n$$ is an integer greater than 2.

ancient Greek text

3rd century AD

example: For in
Example: FO Formulas in

Fermat's Last Theorem

Conjectured by Fermat in 1637

in margin of his copy of

Arithmetica

\[ a^n + b^n = c^n \]

Conjectured by Fermat in 1637 in margin of his copy of Arithmetica.
Example: Fo Formulas in LaTeX

3 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 $\forall x \exists \exists x \beta$, or $\exists x \beta$ (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 Ł -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 $Ł$, an associated function $f^M : M^n \to M$

3. For each $n$-ary relation symbol $P$ in $Ł$, an associated relation $P^M \subseteq M^n$

* Equality predicate $=$ is always true equality relation on $M$. $M = \mathbb{N} \iff \{ (i, i) \mid i \in \mathbb{N} \}$
Example

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

1. \( \mathbb{N} \): standard model of \( L_A \)

\[ M = \mathbb{N} \]

\[ \overline{0} = 0 \in \mathbb{N} \]

\( +, \cdot, s \) are usual plus, times, successor functions

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

\[ \forall x \forall z ( \exists \ z' ( x = z' + z \land (0 = z' \lor \exists z'' ( s2 + z'' = x )) ) \]

Says: \( \forall x \forall z \text{ if } x > z \text{ then } x \text{ can be written as } z + 1 + (\text{some other } z'') \in \mathbb{N} \)
Example

\[ L_A = \{0, s, t, * \} = 3 \]

1. \( M = \mathbb{N} \), \( 0 = 0 \in \mathbb{N} \)
   
   \( s: \) successor, i.e. \( s(2) = 3, \ldots \)
   
   \( t: \) plus, i.e. \( t(0, i) = i, \quad t(2, 3) = 5, \ldots \)
   
   \( \times: \) times

2. \( M = \{ \blacklozenge, \bullet, \ast \} \)
   
   \( 0 = \blacklozenge \)

\[ s(\blacklozenge) = \bullet \]
\[ s(\bullet) = \blacklozenge \]
\[ s(\ast) = \ast \]
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 $M, s$

(a) $^m_x [c] = s(x)$ for all variables $x$

(b) $(t_1, \ldots, t_n)^m [c] = f^m (t_1^m [c], \ldots, t_n^m [c])$

Example 6: $x_1 \rightarrow 5$ $x_2 \rightarrow 7$

$s(x_1 + x_2) [c] = 13$
Evaluation of formulas over \( M, \alpha \)

Let \( A \) be an \( L \)-formula. \( M \models A[\alpha] \)

\[ (M \text{ satisfies } A \text{ under } \alpha) \iff \]

(a) \( M \models \text{Pt}_i \ldots \text{Pt}_n[\alpha] \iff \langle t^m_1[\alpha], \ldots, t^m_n[\alpha] \rangle \in \text{P}^m \)

(b) \( M \models (s = t)[\alpha] \iff s^m[\alpha] = t^m[\alpha] \)

(c) \( M \models \neg A[\alpha] \iff \text{not } M \models A[\alpha] \)

(d) \( M \models (A \lor B)[\alpha] \iff M \models A[\alpha] \text{ or } M \models B[\alpha] \)

(e) \( M \models (A \land B)[\alpha] \iff M \models A[\alpha] \text{ and } M \models B[\alpha] \)

(f) \( M \models \forall x A[\alpha] \iff \forall m \in M \; M \models A[\alpha(\beta X)] \)

(g) \( M \models \exists x A[\alpha] \iff \exists m \in M \; M \models A[\alpha(\alpha X)] \)
For $x$, $y$, $z$.

Evaluate $\exists x \ (x + x = 550 + x) \ [\%]$

For $b = 0, 1, 2, \ldots$

Evaluate $(x + x + 550 + x) \ [\%] \ [\%]$
Example $\mathcal{L} = \{ ; R, = \}$

$M = (\mathbb{N}, \leq, =)$

$R_M(m, n) \text{ if } m \leq n$

Then

$M \models \forall x \exists y R(x, y)$

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

$satisfiable$ by $M$

but $\exists y \forall x R(x, y)$ is also $satisfiable$
**IMPORTANT DEFINITIONS**

Let $A$ be a f.o. formula over $X$.

1. $A$ is satisfiable iff there exists a model $M$ and an object assignment $\sigma$ such that $M \models A[\sigma]$.

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

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

4. $\models A$ (A is valid) iff $\forall M, \sigma$ $M \models A[\sigma]$.
④ $A \iff B$ (A and B are logically equivalent)

\[ A \models B \text{ and } B \models A \]
Examples

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

2. \(\forall x (A_x \lor B_x) \vdash \forall x A_x \lor \forall x B_x\)

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

Earlier formula $A$:

$$
\forall x \forall z \exists z' \forall (z = z' \land (x = x')) \supset
\exists z'' (yx'' + z'' = x))
$$

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

- true when $M = \mathbb{N}$ so $A$ is satisfiable
- false when $M = (M = \{0, 1, 2\}$ so

$$
\begin{align*}
&50 = 1 \\
&51 = 2 \\
&52 = 0 \\
&\text{all others} \\
&x+y = 0
\end{align*}
$$
Example

\[ \forall x \forall y \left( f(x) = f(y) \right) \]

\[ \Rightarrow \quad x = y \]

\[ M = \{0, 1, 2\} \]

\[ f(x) = 0 \quad \forall x \in \{0, 1, 2\} \]

\[ \forall x \forall y \quad f(x) = f(y) = 0 \]

But

\[ g(x) = 1 \]
\[ g(y) = 2 \]
Example

\[ \forall x \forall y \ (f(x) = f(y)) \quad ? \]
\[ x = y \quad \text{No} \]

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

\[ \text{On:} \quad f(0) = 0 \]
\[ f(1) = 0 \]

Then \( M = \forall x \forall y \ (f(x) = f(y)) \)

but \( M \not\models x = y \) (since \( 0 \neq 1 \))
Substitution

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

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

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

For readability, we will write

$t = t \textsc{ss0} x$ as $\textsc{ss0} + x$
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 $s$

\[ (t(s/x))^M[G] = t^M[G(s^{M[G][x]}/x)] \]

Lemma

Substitute $x$ for $s$ to get $t'$
then evaluate $t'$ under $M,s$

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:  
\[ A : \forall y \, (x = y + y) \]
\[ A(\frac{x+y}{x}) : \forall y \, (x + y = y + y) \]

Defn term \( t \) is \underline{freely substitutable} for \( x \) in \( A \) iff there is no subformula in \( A \) of the form \( \forall y B \) or \( \exists y B \) where \( y \) occurs in \( t \)
**Substitution Theorem**

If \( t \) is freely substitutable for \( x \) in \( A \) then \( \forall M A \in_6 \)

\[ M \models A(t/x)[6] \text{ iff } M \models A[6 \left( \frac{\text{tm}[6]}{x} \right)] \]
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

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

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

\[ A_s : A_1 \wedge A_2 \wedge \ldots \wedge A_k \rightarrow B_1 \vee \ldots \vee B_e \]
Lines are again sequents

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

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

$\exists$-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

\[
\begin{align*}
\text{Pa} \Rightarrow \text{Pa} \\
\text{Pa, Qa} \Rightarrow \text{Pa} & \Rightarrow \text{Pa, Qa} \\
\text{Pa} \land \text{Qa} \Rightarrow \text{Pa} \\
\text{Pa} \land \text{Qa} \Rightarrow \exists x P_x & \Rightarrow \exists x (P_x \land Q_x) \\
\exists (P_x \land Q_x) & \Rightarrow \exists x P_x \\
\exists x (P_x \land Q_x) & \Rightarrow \exists x P_x \land \exists x Q_x
\end{align*}
\]
**Soundness**

**Definition:** A first order sequent $A_1, \ldots, A_k \rightarrow B_1, \ldots, B_e$ is valid if and only if its associated formula $(A_1 \land \ldots \land A_k) \rightarrow (B_1 \lor \ldots \lor B_e)$ 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 $\Gamma = B_1 \ldots B_k$
$\Delta = C_1 \ldots C_{k'}$

$A_s: B_1 \land \ldots \land B_k \supset (\exists v \ldots \exists C_{k'} \land A(a))$

$A_{s'}: B_1 \land \ldots \land B_k \supset (\exists v \ldots \exists C_{k'} \land \forall x A(x))$

Note: $a$ cannot occur in lower sequent and thus $a$ can't occur in any $B_i$, $C_i$. 

$\Gamma \rightarrow \Delta, A(x)$

$\Gamma \rightarrow \Delta, \forall x A(x)$
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
Soundness (Proof): By induction on the number of sequents in proof

Example: \exists \text{Left}

Assume: \phi(b), \phi \Rightarrow \Delta \text{ has an LK proof and is valid}

Show: \exists x \phi(x), \phi \Rightarrow \Delta \text{ also valid}

By defn. \phi(b) \lor \overline{\phi}, \ldots \lor \overline{\phi} \lor \Delta \lor \ldots \lor \Delta_k \text{ is valid}

Let \mathcal{M} be any structure, \mathcal{G} any object assignment.

Show: \mathcal{M} \models \neg \exists x \phi(x) \lor \overline{\phi}, \ldots \lor \overline{\phi} \lor \Delta \lor \ldots \lor \Delta_k [6] \hspace{1cm} (\ast)

Case 1: \mathcal{M} \models \overline{\phi}, \ldots \lor \overline{\phi}, \ldots \lor \Delta \lor \ldots \lor \Delta_k [6]. \text{ Then (\ast) holds}

Case 2: Case 1 does not hold.
**Soundness (Proof):** By induction on the number of sequents in proof

**Example:** \( \exists \text{Left} \)

**Assume:** \( \forall (b), \Gamma \Rightarrow \Delta \) has an LK proof and is valid

**Show:** \( \exists x \forall (x), \rho \Rightarrow \Delta \) also valid

By defn \( \forall (b) \forall \pi, \nu \Rightarrow \forall \nu \Delta, \nu \Rightarrow \Delta_k \) is valid

Let \( M \) be any structure, \( \rho \) any object assignment.

**Show:** \( M \models \exists x \forall (x) \forall \pi, \nu \Rightarrow \forall \nu \Delta, \nu \Rightarrow \Delta_k \) \[6\] \( \ast \)

**Case 1** \( M \models \forall \pi, \nu \Rightarrow \forall \nu \Delta, \nu \Rightarrow \Delta_k \) \[6\] \( \ast \)

Then \( \ast \) holds

**Case 2** Case 1 does not hold.

Since \( b \) does not occur in \( \Gamma \) or \( \Delta \),

\( M \models \forall \pi, \nu \Rightarrow \forall \nu \Delta, \nu \Rightarrow \Delta_k \) \[6 \{ \ast \} \] for all \( m \in M \)

Since \( \forall (b), \Gamma \Rightarrow \Delta \) is valid, \( M \models \forall (b) \) \[6 \{ \ast \} \] \( \forall m \in M \)

Thus \( M \models \exists x \forall (x) \) \[6\], \( \ast \) thus \( \exists x \forall (x), \Gamma \Rightarrow \Delta \) is valid.