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 $\mathcal{L}$ specified by:

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

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

Built in symbols

Example $\mathcal{L}_A$ (language of arithmetic)

$$\mathcal{L}_A = \{ \underbrace{0, s, +, \cdot}_{\text{function symbols}} ; \underbrace{=}_{\text{relation symbols}} \}$$

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 $t_1, \dots, t_n$ terms, then $f t_1 \dots t_n$ is a term

Examples of terms $(0, s, f, +, \cdot)$

0-ary   unary   binary

$f0sss0$, $+xfyz$, $\cdot + ab\, ss0$

$f(0sss, 0)$ $x + f(y, z)$ $(a+b) * ss0$

FIRST ORDER FORMULAS OVER $\mathcal{L}$

(1) $Pt_1 .. t_n$ is an atomic $\mathcal{L}$-formula, where
P is an n-ary predicate in $\mathcal{L}$, and
$t_1 .. t_n$ are terms over $\mathcal{L}$

(2) If A, B are $\mathcal{L}$-formulas, so are
$\neg A$, $(A \wedge B)$, $(A \vee B)$, $\forall x A$, $\exists x A$

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: $\forall x \; \exists y \; (y > x$ and y is prime$)$

y is prime : $\forall z, z' \; (z, z' \geq 2 \Rightarrow z \cdot z' \neq y)$

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

① Existence of infinitely many primes

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

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

(*) $$\forall z \forall z' \Big(\big(\neg(z=0) \wedge \neg(z=S0) \wedge \neg(z'=0) \wedge \neg(z'=S0) \big) \rightarrow \neg(z \cdot z' = y) \Big)$$

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

① Existence of infinitely many primes

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

y is prime : $\forall z, z' \; (z, z' \geq 2 \Rightarrow z \cdot z' \neq y)$

(*) $\left[\forall z \forall z' \left(\left(\neg(z = 0) \wedge \neg(z = S0) \wedge \neg(z' = 0) \wedge \neg(z' = S0) \right) \rightarrow \neg(z \cdot z' = y) \right) \right.$

(**) $\left[y > x : \; \neg(x = y) \wedge \exists w \, (x + w = y) \right.$

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

① Existence of infinitely many primes

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

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

(*) $\forall z \forall z' \big((\neg(z=0) \wedge \neg(z=S0) \wedge \neg(z'=0) \wedge \neg(z'=S0)) \rightarrow \neg(z \cdot z' = y) \big)$

(**) $y > x$: $\neg(x=y) \wedge \exists w\,(x+w=y)$

Whole thing: $\forall x \exists y\, (*) \wedge (**)$

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: FO Formulas in $\mathcal{L}_A$

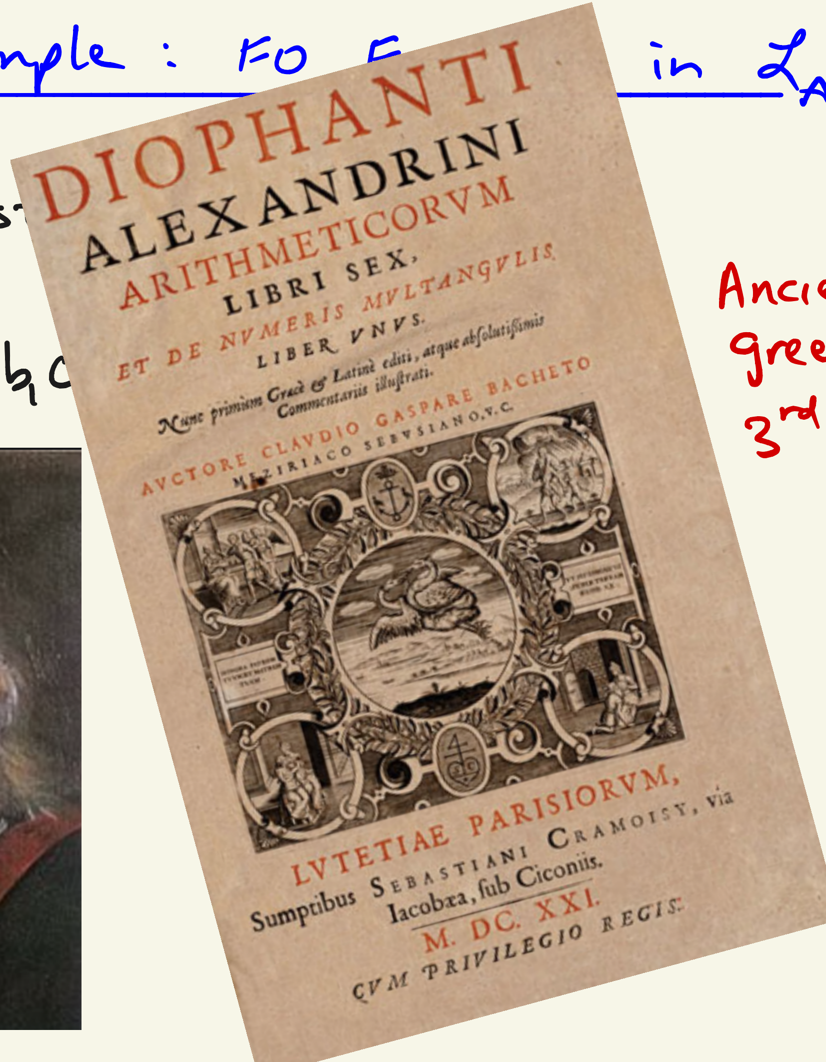
③ Fermat's Last Theorem

$$\forall n \geq 3\ \forall a, b, c\ (n > 2 \rightarrow a^n + b^n \neq c^n)$$

Example : FO F ... in $\mathcal{L}_A$

(3) Fermat's Las

$\forall n \geq 3 \; \forall a, b, c$



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis
Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.

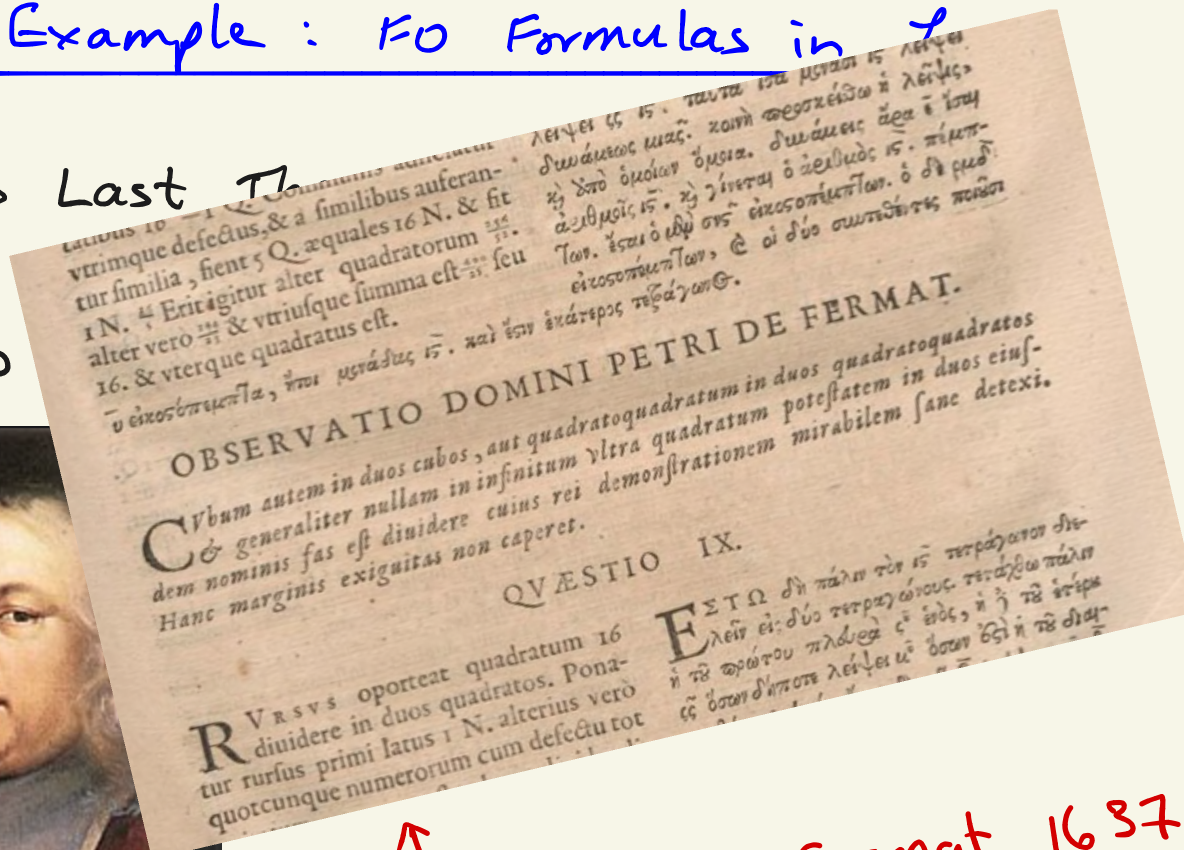
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Ancient greek text, 3^{rd} century AD

Example : FO Formulas in $\mathcal{L}$

③ Fermat's Last Th

$\forall n \geq 3$



latibus 16 — 1 Q. Communis adiiciatur utrimque defectus, & a similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter vero $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

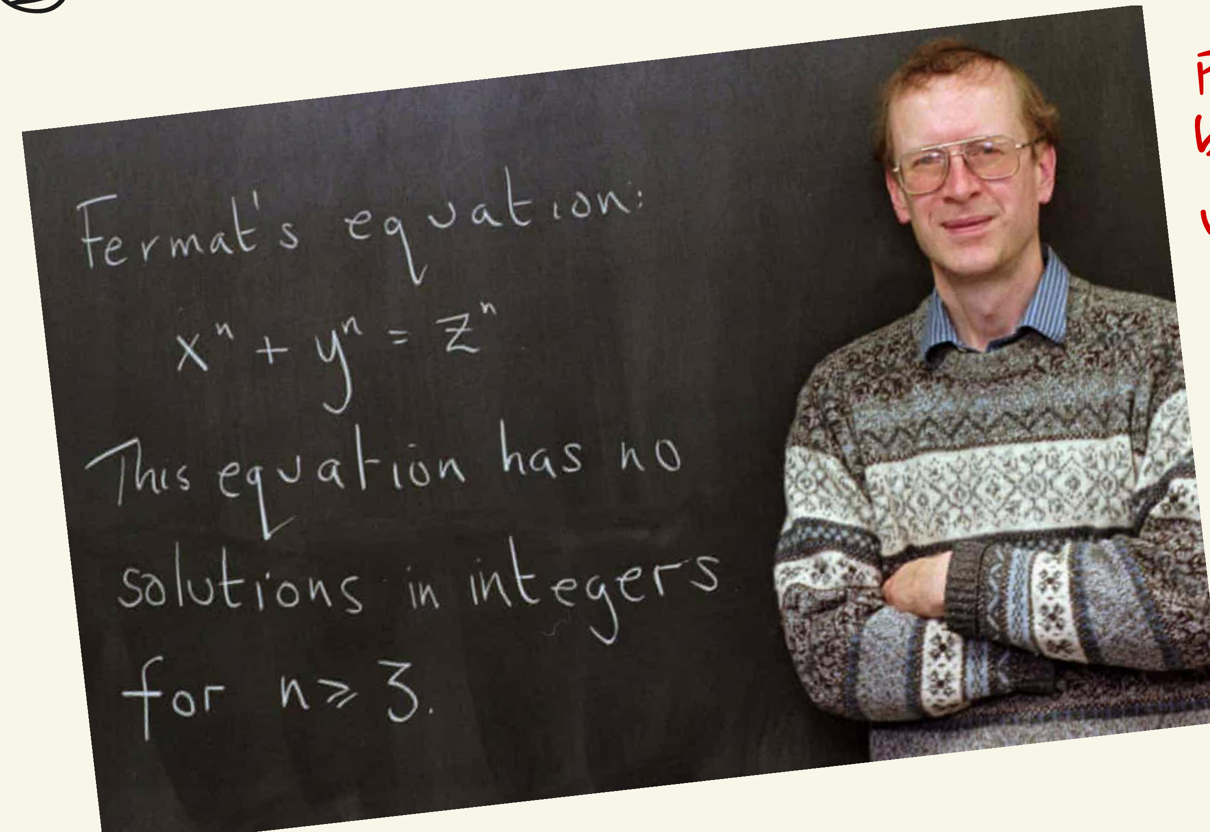
QVÆSTIO IX.

Rvrsvs oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot

conjectured by Fermat 1637 in margin of his copy of Arithmetica

Example: FO Formulas in $\mathcal{L}_A$

③ Fermat's Last Theorem



Finally proven by Andrew Wiles

Example : FO Formulas in $\mathcal{L}_A$

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

$$\forall n \geq 3 \; (\forall a, b, c \quad a^n + b^n \neq c^n)$$

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 $\forall x B$, or $\exists x B$ (otherwise x is free in A)

<u>Example</u> $\exists y(x = y + y)$

$$Px \wedge \forall x(\neg(x + Sx = x))$$

- 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 $\mathfrak{M}$ (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 $f^{\mathfrak{M}} : M^n \to M$

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

* Equality predicate '=' is always true equality relation on M.

Example

$\mathcal{L}_A = \{0, S, +, \cdot, =\}$

1. $\mathbb{N}$: standard model of $\mathcal{L}_A$

$M = \mathbb{N}$

$0 = 0 \in \mathbb{N}$

$+, \cdot, S$ are usual plus, times, successor functions

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

$$\forall x \, \forall z \; \big(\exists z' \, (\neg(z' = 0) \wedge z + z' = x) \rightarrow \exists z'' \, (Sz + z'' = x) \big)$$

Example

$\mathcal{L}_A = \{0, s, +, \cdot\, ; =\}$

① $\mathcal{M} = \underline{\mathbb{N}}$,

$0 = 0 \in \mathbb{N}$

s: successor. ie. $s(2)=3$, ...

$+$: plus. ie, $+(0,i) = i$, $+(2,3)=5$, etc

$\cdot$: times

② $M = \{$ ■, ●, ★ $\}$ $0 =$ ■

s(■) = ●
s(●) = ■
s(★) = ★

+	■	●	★
■	●	●	★
●	●	●	★
★	★	★	★

•	■	●	★
■	■	★	●
●	■	■	★
★	★	★	■

How to evaluate formulas that contain free variables?

Defn An object assignment σ for a model $\mathfrak{M}$ is a mapping from variables to M

Definition: Evaluation of terms/formulas over $\mathfrak{M}, \sigma$

Let $\mathfrak{M}$ be an $\mathcal{L}$-structure,
σ an object assignment for $\mathfrak{M}$

Evaluation of terms over $\mathfrak{M}, \sigma$

(a) $x^{\mathfrak{M}}[\sigma]$ is $\sigma(x)$ for all variables x

(b) $(f t_1 \ldots t_n)^{\mathfrak{M}}[\sigma] = f^{\mathfrak{M}}(t_1^{\mathfrak{M}}[\sigma], \ldots, t_n^{\mathfrak{M}}[\sigma])$

Evaluation of formulas over $\mathfrak{M}, \sigma$

Let A be an $\mathcal{L}$-formula. $\mathfrak{M} \models A[\sigma]$ ($\mathfrak{M}$ satisfies A under σ) iff

(a) $\mathfrak{M} \models Pt_1 \ldots t_n[\sigma]$ iff $\langle t_1^{\mathfrak{M}}[\sigma], \ldots, t_n^{\mathfrak{M}}[\sigma] \rangle \in P^{\mathfrak{M}}$

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

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

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

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

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

(g) $\mathfrak{M} \models \exists x A[\sigma]$ iff $\exists m \in M$ $\mathfrak{M} \models A[\sigma(m/x)]$

Example

$\mathcal{L} = \{ ; R, = \}$

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

$R^{\mathfrak{M}}(m,n)$ iff $m \leq n$

Then $\mathfrak{M} \overset{?}{\models} \forall x \exists y R(x,y)$ yes

satisfiable by $\mathfrak{M}$

$\mathfrak{M} \overset{?}{\models} \exists y \forall x R(x,y)$ No

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

IMPORTANT DEFINITIONS

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

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

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

$\models A$ (A is valid) iff $\forall \mathfrak{M}, \sigma$ $\mathfrak{M} \models A[\sigma]$

④ $A \Leftrightarrow B$ (A and B are logically equivalent)

iff $\forall \mathfrak{M} \, \forall \sigma \quad \mathfrak{M} \models A[\sigma]$ iff $\mathfrak{M} \models B[\sigma]$

Examples

(1) $\underbrace{(\forall x\, Px \vee \forall x.Qx)}_{t} \overset{?}{\vDash} \underbrace{\forall x(Px \vee Qx)}$ Yes

(2) $\underbrace{\forall x(Ax \vee Bx)} \overset{?}{\vDash} \forall x\, Ax \vee \forall x\, Bx$ NO

$\mathcal{L} = \{;\ P, Q, A, B\}$

or

Example

Earlier formula A:

$$\forall x \forall z \; (\exists z' (\neg(z'=0) \wedge z+z'=x) \supset \exists z'' (sz + z'' = x))$$

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

- true when $\mathcal{M} = \underline{\mathbb{N}}$ so A is satisfiable
- false when $\mathcal{M} = \left(M = \{0,1,2\} \quad \begin{matrix} s0=1 \\ s1=2 \\ s2=0 \end{matrix} \quad \begin{matrix} 0+2=2 \\ \text{all others} \\ x+y=0 \end{matrix} \right)$

$x=2 \quad z=0 \quad z'=2$

Example

$$\forall x \forall y\, (fx = fy) \overset{?}{\underset{\text{No}}{\models}} x = y$$

Let $M = \{0, 1\}$

$\mathfrak{M}$: $f(0) = 0$

$f(1) = 0$

then $\mathfrak{M} \models \forall x \forall y\, (fx = fy)$

but $\mathfrak{M} \not\models x = y$ (since $0 \neq 1$)

Substitution

Let s, t be $\mathcal{L}$-terms.

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

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

$t = + SS0\, x$ $\longleftarrow$ $SS0 + x$

$t\left(\frac{+yz}{x}\right)$: $+ SS0 \; +yz$

$SS0 + (y+z)$

Substitution

Let s, t be $\mathcal{L}$-terms.

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

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

Lemma $$\left(t(s/x)\right)^{\mathcal{M}}[\sigma] = t^{\mathcal{M}}\left[\sigma\left(\frac{s^{\mathcal{M}}[\sigma]}{x}\right)\right]$$

substitute x for s to get t' then evaluate t' under $\mathcal{M}, \sigma$

obtain new object assignment σ' where $\sigma'(x) = s^{\mathcal{M}}$ then evaluate t under $\mathcal{M}, \sigma'$

Substitution Cont'd

Need to be more careful when making substitutions into formulas

<u>Example</u>: $A : \forall y \neg (x = y + y)$

$$A\left(\frac{x+y}{x}\right) : \forall y \neg (x + y = y + y)$$

<u>Defn</u> term t is <u>freely substitutable</u> 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 $\forall \mathfrak{M}\ \forall \sigma$

$$\mathfrak{M} \models A(t/x)[\sigma] \text{ iff } \mathfrak{M} \models A\left[\sigma\left(t^{\mathfrak{M}}[\sigma]/x\right)\right]$$

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 & every bound variable occurrence of type bound

Proper term: No variables of type bound

FIRST ORDER SEQUENT CALCULUS LK

Lines are again sequents

$$\left.A_1, \ldots, A_k \rightarrow B_1, \ldots, B_\ell\right\} S$$

where each A_i, B_j is a proper $\mathcal{L}$-formula

$$A_S : \quad A_1 \wedge A_2 \wedge \ldots \wedge A_k \supset B_1 \vee \ldots \vee B_\ell$$

FIRST ORDER SEQUENT CALCULUS LK

Lines are again sequents

$$A_1, \dots, A_k \to B_1, \dots, B_\ell$$

where each A_i, B_j is a proper $\mathcal{L}$-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 $\quad \dfrac{A(t), \Gamma \to \Delta}{\forall x\, A(x), \Gamma \to \Delta}$ $\qquad$ $\forall$-Right $\quad \dfrac{\Gamma \to \Delta, A(b)}{\Gamma \to \Delta, \forall x\, A(x)}$

$\exists$-left $\quad \dfrac{A(b), \Gamma \to \Delta}{\exists x\, A(x), \Gamma \to \Delta}$ $\qquad$ $\exists$-right $\quad \dfrac{\Gamma \to \Delta, A(t)}{\Gamma \to \Delta, \exists x\, A(x)}$

* A, t are proper
* b is a free variable Not appearing in lower sequent of rule

Example of an LK proof

$$
\begin{prooftree}
\AxiomC{$Pa \to Pa$}
\UnaryInfC{$Pa, Qa \to Pa$}
\UnaryInfC{$Pa \wedge Qa \to Pa$}
\LeftLabel{$\exists$-rt}
\UnaryInfC{$Pa \wedge Qa \to \exists x Px$}
\LeftLabel{$\exists$-left}
\UnaryInfC{$\exists x (Px \wedge Qx) \to \exists x Px$}
\AxiomC{$Qa \to Qa$}
\UnaryInfC{$Pa, Qa \to Qa$}
\UnaryInfC{$Pa \wedge Qa \to Qa$}
\RightLabel{$\exists$-rt}
\UnaryInfC{$Pa \wedge Qa \to \exists x Qx$}
\RightLabel{$\exists$-left}
\UnaryInfC{$\exists x (Px \wedge Qx) \to \exists x Qx$}
\LeftLabel{$\wedge$-rt}
\BinaryInfC{$\exists x (Px \wedge Qx) \to \exists x Px \wedge \exists x Qx$}
\end{prooftree}
$$

SOUNDNESS

Defn A first order sequent $A_1, \ldots, A_k \rightarrow B_1, \ldots, B_\ell$ is valid if and only if its associated formula $(A_1 \wedge \ldots \wedge A_k) \supset (B_1 \vee \ldots \vee B_\ell)$ is valid.

Soundness Theorem for LK Every sequent provable in LK is valid

Proof of Lemma

go through each rule

Example: $\forall$-right rule

$$\frac{\Gamma \to \Delta, A(a)}{\Gamma \to \Delta, \forall x\, A(x)} \qquad \leftarrow A_u$$

Note: a cannot occur in lower sequent & thus a can't occur in any B_i, C_j

Let $\Gamma = B_1 \ldots B_\ell$

$\Delta = C_1 \ldots C_{\ell'}$

A : $B_1 \wedge \ldots \wedge B_\ell \supset C_1 \vee \ldots \vee C_{\ell'} \vee A(a)$

A_L : $B_1 \wedge \ldots \wedge B_\ell \supset C_1 \vee \ldots \vee C_{\ell'} \vee \forall A(x)$

Theorem (LK Soundness)

Every sequent provable in LK is valid

Pf by induction on the number of sequents in proof.

Axiom $A \to A$ is valid

Induction step : use previous soundness lemma