CS20a: Models (Nov 14, 2002)

- Alternative models
  - *Primitive recursive functions*
  - *Partial recursive functions*
  - *Recursion theorem*
  - *Rice's theorem*
- Lambda Calculus
  - *Recursion theorem*
  - *Rice's theorem*
- Arithmetic
  - *Recursion theorem*
  - *Godel's incompleteness theorem (aka Rice's theorem)*

Arithmetic

- Let’s do the same for arithmetic
- Arithmetic is:
  - *Operators: +, -, *, /, …*
  - *First-order logic*
- First, let’s define logic

Defining logics

- A logic is defined in three parts
  - *Syntax*
  - *Define what is "true"*
  - *Define derivation procedures*

Defining the syntax

Start with a countable set of propositional letters $P, Q, R, \ldots$
Define the propositions inductively:

- $\top$ (true) is a proposition
- $\bot$ (false) is a proposition
- Any propositional letter is a proposition
- If A is a proposition, so it $\neg A$ (negation)
- If A and B are propositions, so are
  - $A \wedge B$ (conjunction)
  - $A \vee B$ (disjunction)
  - $A \Rightarrow B$ (implication)

Standard syntax definition

Propositions:

$$
\begin{array}{lcl}
e & ::= & \top \mid \bot \\
& \mid & P, Q, R, \ldots \\
& \mid & \neg e \\
& \mid & e \wedge e \\
& \mid & e \vee e \\
& \mid & e \Rightarrow e
\end{array}
$$

Semantics

- The semantics of constants: $\top = 1, \bot = 0$
- The semantics of a propositional letter is its truth value.
- The semantics of a compound proposition is determined by truth tables.

A	B	$A \lor B$
0	0	0
0	1	1
1	0	1
1	1	1

A	B	$A \land B$
0	0	0
0	1	0
1	0	0
1	1	1

A	B	$A \land B$
0	0	1
0	1	1
1	0	0
1	1	1

Extending the truth assignment

A	B	C	$A \wedge B$	$(A \wedge B) \Rightarrow C$
0	0	0	0	1
0	0	1	0	1
0	1	0	0	1
0	1	1	0	1
1	0	0	0	1
1	0	1	0	1
1	1	0	1	0
1	1	1	1	1

Some definitions

- A *truth assignment* $\mathcal{A}$ assigns a value to each propositional letter A a unique truth value $\mathcal{A}(A) \in \{0, 1\}$
- A *truth valuation* $\mathcal{V}$ assigns a truth value to each proposition (it can be constructed from a $\mathcal{A}$ by following the truth tables).
- A proposition α is *satisfiable* if there is a truth valuation $\mathcal{V}(\alpha) = 1$
- A proposition α is *true* (a tautology) if it is true in all valuations.

A proof (Pierce's Law)

A	B	$A \Rightarrow B$	$(A \Rightarrow B) \Rightarrow A$	$((A \Rightarrow B) \Rightarrow A) \Rightarrow A$
0	0	1	0	1
0	1	1	0	1
1	0	0	1	1
1	1	1	1	1

Derivations

- Truth tables are hard to use
- We want a mechanical method for proving propositions
- Use sequents and truth judgments

Sequents

- A *sequent* has the form $\Gamma \vdash \Delta$
- Δ is a list of propositions $\alpha_1, \ldots, \alpha_n$
- Γ is a *context* containing a list of propositions $\beta_1, \ldots, \beta_n$
- We can extend valuations to sequents, to get the folowing semantics:
  - A sequent $\beta_1, \ldots, \beta_n \vdash \alpha_1, \ldots, \alpha_n$ is true if some α_i is true whenever $\beta_1, \ldots, \beta_n$ are all true.

Derivations

- There are two kinds of inference rules
  - *Introduction* rules operate on the right of the turnstile
  - *Elimination* rules operate on the left of the turnstile
- The base axiom

$$\frac{}{\Gamma_1, \alpha, \Gamma_2 \vdash \Delta_1, \alpha, \Delta_2}\ \text{axiom}$$

Introduction rules, part I

$$\frac{}{\Gamma \vdash \Delta_1, \top, \Delta_2} \text{ true intro}$$

$$\frac{\Gamma \vdash \Delta_1, \alpha, \Delta_2 \quad \Gamma \vdash \Delta_1, \beta, \Delta_2}{\Gamma \vdash \Delta_1, \alpha \wedge \beta, \Delta_2} \text{ and intro}$$

$$\frac{\Gamma \vdash \Delta_1, \alpha, \beta, \Delta_2}{\Gamma \vdash \Delta_1, \alpha \vee \beta, \Delta_2} \text{ or intro}$$

Introduction rules, part II

$$\frac{\Gamma, \alpha \vdash \Delta_1, \beta, \Delta_2}{\Gamma \vdash \Delta_1, \alpha \Rightarrow \beta, \Delta_2} \text{ implies intro}$$

$$\frac{\Gamma, \alpha \vdash \Delta_1, \Delta_2}{\Gamma \vdash \Delta_1, \neg\alpha, \Delta_2} \text{ not intro}$$

Elimination rules

$$\frac{}{\Gamma_1, \bot, \Gamma_2 \vdash \Delta} \text{ false elim}$$

$$\frac{\Gamma_1, \alpha, \beta, \Gamma_2 \vdash \Delta}{\Gamma_1, \alpha \wedge \beta, \Gamma_2 \vdash \Delta} \text{ and elim}$$

$$\frac{\Gamma_1, \alpha, \Gamma_2 \vdash \Delta \quad \Gamma_1, \beta, \Gamma_2 \vdash \Delta}{\Gamma_1, \alpha \vee \beta, \Gamma_2 \vdash \Delta} \text{ or elim}$$

$$\frac{\Gamma_1, \beta, \Gamma_2 \vdash \Delta \quad \Gamma_1, \Gamma_2 \vdash \alpha, \Delta}{\Gamma_1, \alpha \Rightarrow \beta, \Gamma_2 \vdash \Delta} \text{ implies elim}$$

Rule table

$$\frac{}{\Gamma \vdash \Delta_1, \top, \Delta_2} \qquad \frac{}{\Gamma_1, \bot, \Gamma_2 \vdash \Delta}$$

$$\frac{\Gamma \vdash \Delta_1, \alpha, \Delta_2 \quad \Gamma \vdash \Delta_1, \beta, \Delta_2}{\Gamma \vdash \Delta_1, \alpha \wedge \beta, \Delta_2} \qquad \frac{\Gamma_1, \alpha, \beta, \Gamma_2 \vdash \Delta}{\Gamma_1, \alpha \wedge \beta, \Gamma_2 \vdash \Delta}$$

$$\frac{\Gamma \vdash \Delta_1, \alpha, \beta, \Delta_2}{\Gamma \vdash \Delta_1, \alpha \vee \beta, \Delta_2} \qquad \frac{\Gamma_1, \alpha, \Gamma_2 \vdash \Delta \quad \Gamma_1, \beta, \Gamma_2 \vdash \Delta}{\Gamma_1, \alpha \vee \beta, \Gamma_2 \vdash \Delta}$$

$$\frac{\Gamma, \alpha \vdash \Delta_1, \beta, \Delta_2}{\Gamma \vdash \Delta_1, \alpha \Rightarrow \beta, \Delta_2} \qquad \frac{\Gamma_1, \beta, \Gamma_2 \vdash \Delta \quad \Gamma_1, \Gamma_2 \vdash \alpha, \Delta}{\Gamma_1, \alpha \Rightarrow \beta, \Gamma_2 \vdash \Delta}$$

Proving the law of excluded middle

- Every proposition is either true or false

$$\dfrac{\dfrac{\overline{A \vdash A}\;3}{\vdash A, \neg A}\;2}{\vdash A \vee \neg A}\;1$$

Pierce's law

$$
\cfrac{\cfrac{\cfrac{}{A \vdash B, A}\;4}{\vdash A \Rightarrow B, A}\;3 \qquad \cfrac{}{A \vdash A}\;5}{\cfrac{(A \Rightarrow B) \Rightarrow A \vdash A}{\vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A}\;1}\;2
$$

Currying

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A, B \vdash A}\;5 \qquad \dfrac{}{A, B \vdash B}\;6}{A, B \vdash A \wedge B}\;4 \qquad \dfrac{}{C, A, B \vdash C}\;6}{(A \wedge B) \Rightarrow C, A, B \vdash C}\;3}{(A \wedge B) \Rightarrow C \vdash A \Rightarrow B \Rightarrow C}\;2}{\vdash ((A \wedge B) \Rightarrow C) \Rightarrow (A \Rightarrow (B \Rightarrow C))}\;1$$

First-order logic

- Add *atomic formulas* $f(a_1, \ldots, a_n)$ of various ar-itites.

- Add *atomic predicates* $P(a_1, \ldots, a_m)$ is various ar-ities.

$$
\begin{array}{rcl}
a & ::= & f(a_1, \ldots, a_n) \\
e & ::= & \top \mid \bot \\
& | & P(a_1, \ldots, a_m) \\
& | & \neg e \\
& | & e \wedge e \\
& | & e \vee e \\
& | & e \Rightarrow e \\
& | & \forall v.e \\
& | & \exists v.e
\end{array}
$$

Some examples

- $\forall x.big(x) \Rightarrow heavy(x)$
- $\forall i.(i + 1) > i$
- $\forall i.\exists j.j > i$
- $\exists i.\forall j.j \leq i$

Adding rules for FOL

$$\frac{\Gamma \vdash \Delta_1, P(t), \Delta_2}{\Gamma \vdash \Delta_1, \exists v.P(v), \Delta_2} \text{ exists intro}$$

$$\frac{\Gamma \vdash \Delta_1, P(c), \Delta_2 \quad (\text{new } c)}{\Gamma \vdash \Delta_1, \forall v.P(v), \Delta_2} \text{ all intro}$$

$$\frac{\Gamma_1, P(c), \Gamma_2 \vdash \Delta \quad (\text{new } c)}{\Gamma_1, \exists v.P(v), \Gamma_2 \vdash \Delta} \text{ exists elim}$$

$$\frac{\Gamma_1, \forall v.P(v), \Gamma_2, P(t) \vdash \Delta}{\Gamma_1, \forall v.P(v), \Gamma_2 \vdash \Delta} \text{ all elim}$$

A quantifier DeMorgan law

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi(c) \vdash \varphi(c)}\;6}{\forall x.\varphi(x) \vdash \varphi(c)}\;5}{\neg\varphi(c), \forall x.\varphi(x) \vdash}\;4}{\neg\varphi(c) \vdash \neg(\forall x.\varphi(x))}\;3}{\exists x.\neg\varphi(x) \vdash \neg(\forall x.\varphi(x))}\;2}{\vdash (\exists x.\neg\varphi(x)) \Rightarrow \neg(\forall x.\varphi(x))}\;1$$

Another proof

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{\varphi(c) \vdash \varphi(c)}{\varphi(c) \vdash \exists x.\varphi(x)}\;5
      \qquad
      \psi \vdash \psi
    }{(\exists x.\varphi(x)) \Rightarrow \psi, \varphi(c) \vdash \psi}\;4
  }{
    \dfrac{}{(\exists x.\varphi(x)) \Rightarrow \psi, \varphi(c) \Rightarrow \psi}\;3
  }
}{
  \dfrac{}{(\exists x.\varphi(x)) \Rightarrow \psi \vdash \forall x.\varphi(x) \Rightarrow \psi}\;2
}
$$

$$
\dfrac{(\exists x.\varphi(x)) \Rightarrow \psi \vdash \forall x.\varphi(x) \Rightarrow \psi}{\vdash ((\exists x.\varphi(x)) \Rightarrow \psi) \Rightarrow (\forall x.\varphi(x) \Rightarrow \psi)}\;1
$$

Formalizing arithmetic

The language of arithmetic:

$$
\begin{array}{rcl}
e & ::= & i \mid v \mid e + e \mid \cdots \mid e/e \\
P & ::= & e = e \mid e < e \mid \cdots \\
 & \mid & \neg P \\
 & \mid & P \wedge P \mid P \vee P \mid P \Rightarrow P \\
 & \mid & \exists v.P[v] \mid \forall v.P[v]
\end{array}
$$

Example:

$$\forall x_1.\exists x_2.\forall x_3.\exists x_4.(x_3 + x_2 \leq (1 + x_1) * x_4)$$

Indexing the arithmetic formulas

Define $\ulcorner \varphi \urcorner$ is the Gödel index of formula φ
Define the normal way:

- $\ulcorner x_i \urcorner = [0 :: i]$
- $\ulcorner e_1 + e_2 = 1 :: \ulcorner e_1 \urcorner @ \ulcorner e_2 \urcorner$
- $\ulcorner e_1 < e_2 \urcorner = 10 :: \ulcorner e_1 \urcorner @ \ulcorner e_2 \urcorner$
- $\ulcorner P_1 \wedge P_2 \urcorner = 20 :: \ulcorner P_1 \urcorner @ \ulcorner P_2 \urcorner$
- ...

Defining substitution

- Define a function $\textsc{subst}(x, y, z) = w$, where

$$\textsc{subst}(n, \ulcorner x \urcorner, \ulcorner \varphi \urcorner) = \ulcorner \varphi[n/x] \urcorner$$

- That is, $\textsc{subst}(n, \ulcorner x \urcorner, \ulcorner \varphi \urcorner)$ produces the number of a new function $\ulcorner \varphi[n/x] \urcorner$ where the constant n is substituted for x.
- Define $\textsc{subst}'(y) \equiv \textsc{subst}(y, \ulcorner x_0 \urcorner, y)$
- (Note that $\textsc{subst}$ can be defined in arithmetic)

Fixpoint theorem for arithmetic

Theorem (Fixpoint theorem)
For any formula $\psi(y)$ with free variable y, there is a sentence φ with no free variables s.t. $\varphi \Leftrightarrow \psi(\ulcorner \varphi \urcorner)$.

Fixpoint proof

- Let $\rho(y) = \psi(\text{SUBST}'(y))$
- so $\rho(x_0) = \psi(\text{SUBST}'(x_0))$
- Let $\varphi = \rho(\ulcorner\rho(x_0)\urcorner)$

$$
\begin{aligned}
\varphi &\Leftrightarrow \rho(\ulcorner\rho(x_0)\urcorner) \\
&\Leftrightarrow \psi(\text{SUBST}'(\ulcorner\rho(x_0)\urcorner)) \\
&\Leftrightarrow \psi(\text{SUBST}(\ulcorner\rho(x_0)\urcorner, \ulcorner x_0\urcorner, \ulcorner\rho(x_0)\urcorner)) \\
&\Leftrightarrow \psi(\ulcorner\rho(\ulcorner\rho(x_0)\urcorner)\urcorner) \\
&\Leftrightarrow \psi(\ulcorner\varphi\urcorner)
\end{aligned}
$$

Godel's Incompleteness Theorem

Theorem (Gödel's Incompletness theorem)
There is a formula that is not provable.
Proof

- Define a formula $\text{UNPROVABLE}(\ulcorner\varphi\urcorner)$ iff φ is not provable.
- This is a formula in arithmetic

$$\psi(y) \equiv \text{UNPROVABLE}(y) \equiv \text{UNPROVABLE}(\ulcorner\varphi_y\urcorner)$$

- Consider, for some φ, the formula

$$\varphi \Leftrightarrow \text{UNPROVABLE}(\ulcorner\varphi\urcorner)$$