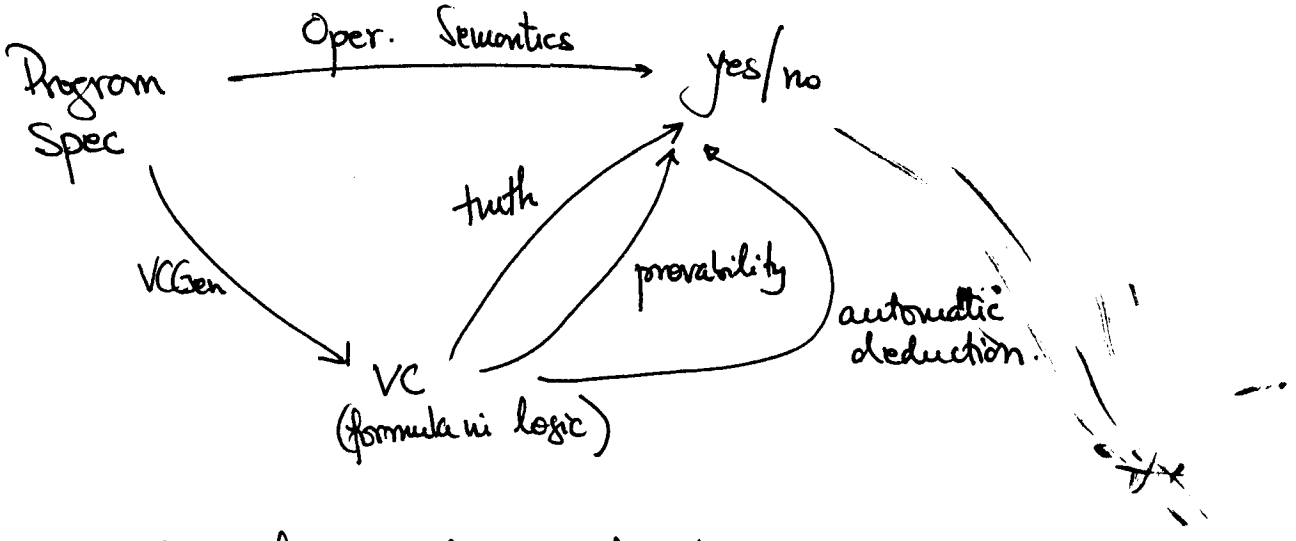
LECTURE 6: FIRST-ORDER LOGIC AND THEORIES

- Where are we?



- What is the form of verification conditions?

$$G ::= \text{true} \mid G_1 \wedge G_2 \mid H \Rightarrow G \mid \forall x.\, G$$

$$H ::= \text{true} \mid L \wedge H \qquad \text{(sequence of literals)}$$

$$L ::= p(E_1, \ldots, E_k) \qquad p \text{ - predicate symbol}$$

$$E ::= f(E_1, \ldots, E_k) \mid n \qquad f \text{ - function symbol}$$

- Recall the semantics. (truth of VC)
  - quantification over $\mathbb{Z}$ (or some universe)
  - each predicate symbol has a semantics.

    $[\![p]\!] \in \mathcal{P}(\mathbb{Z}^k)$
  - each function symbol denotes a (total) function

    $[\![f]\!] \in \mathbb{Z}^k \to \mathbb{Z}$

$\Vdash$ true always

$\Vdash G_1 \wedge G_2$ iff $\Vdash G_1$ and $\Vdash G_2$

$\Vdash H \Rightarrow G$ iff whenever $\Vdash H$ then $\Vdash G$

$\Vdash \forall x.\, G$ iff for all $n \in \mathbb{Z}$ $\Vdash G[n/x]$

- note that $\Vdash G$ is defined only on closed Gs

$\Vdash p(E_1, \ldots, E_k)$ iff $([\![E_1]\!], \ldots, [\![E_k]\!]) \in [\![p]\!]$

$[\![f(E_1, \ldots, E_k)]\!] = [\![f]\!]([\![E_1]\!], \ldots, [\![E_k]\!])$

A Deductive System for VC

$H \vdash G$

$$\frac{H \vdash G_1 \quad H \vdash G_2}{H \vdash G_1 \wedge G_2} \qquad \frac{H \wedge H' \vdash G}{H \vdash H' \Rightarrow G} \qquad \frac{H \vdash G[a/x]}{H \vdash \forall x.\, G}$$

a is a fresh logical parameter

$$\frac{}{H \vdash \text{true}} \qquad \frac{H \wedge \neg L \text{ is unsatisfiable}}{H \vdash L}$$

- soundness of deductive systems → yes
- completeness → almost (will discuss that later in course)

A proof procedure

- define Unsat $(L_1, \ldots, L_k)$ → returns true if $L_1, \ldots, L_k$ are unsatisfiable.
  - there is no substitution of logical parameters with integers that makes all L_i true
  - Unsat is a satisfiability procedure
- we define prove : $H \times G \to$ bool

$$\text{prove}(H, \text{true}) = \text{true}$$
$$\text{prove}(H, G_1 \wedge G_2) = \text{prove}(H, G_1) \text{ andalso } \text{prove}(H, G_2)$$
$$\text{prove}(H, H' \Rightarrow G) = \text{prove}(H \wedge H', G)$$
$$\text{prove}(H, \forall x.G) = \text{prove}(H, G[a/x]) \quad a \text{ is fresh}$$
$$\text{prove}(H, L) = \text{Unsat}(H \wedge \neg L)$$

- proof by inversion
- complete for this fragment in intuitionistic setting

Soundness of theorem prover

- assume soundness of satisfiability procedure
  if Unsat($L_1, \ldots, \neg L_k$) then [redacted]
  $\vdash \forall a_1 \ldots a_n \models L_1 \wedge \ldots \wedge L_{k-1} \Rightarrow L_k$
- statement
  - let H, G
  - let $a_1, \ldots, a_k$ the parameters in them

  prove(H, G) then $\vdash \forall a_1 \ldots a_n . H \Rightarrow G$
- easy proof by induction on the computation of prove

Intuition behind prove

- the logical connectives are used in a superficial way in VC
  - $\wedge$ to construct sets of (sub) goals
  - $\forall$ to mark use of fresh variables
  - $\Rightarrow$ to collect assumptions (locally)
- the only "deep" facts are in the literals
- the hard work in proving is in Unsat

Theories

- a set of function and predicate symbols
- a semantic for each function and predicate symbol
  - semantically defined theory
- a set of axioms (formulas in first-order predicate logic involving the symbols of the theory)
  - axiomatically defined theory

Examples

AX: $\{=, \leq\}$

- $\forall x \forall y \quad x \leq y \wedge y \leq x \Rightarrow x = y$
- $\forall x \forall y \forall z \quad x \leq y \wedge y \leq z \Rightarrow x \leq z$
- $\forall x \forall y \quad x \leq y \vee y \leq x$

- theory of ~~total~~ orders

SEM: $\{\mathbb{N}, +, \leq, /\!/\}$ with $[\![n]\!] = n$

$[\![+]\!] = \lambda n_1 n_2 .\ n_1 + n_2$

- theory of integers with addition
- or, Presburger arithmetic

- Decision problem
  - decide whether a sentence in a theory is true
  - the sentence can include any logical connectives and quantifiers

e.g. $\forall x \not\in. \; x > 0 \Rightarrow (\exists y. \; x = y + 1)$

  - a sentence in Presburger arithmetic

- Decision problem for quantifier-free formula can be reduced to the satisfiability problem

- Satisfiability problem
  - decide whether a <u>conjunction</u> of <u>literals</u> in a theory is satisfiable

through negation + CNF

Examples of theories

- **Equality with uninterpreted functions**
  - Symbols $f, g, \ldots$ $=$

$$\frac{}{E = E} \qquad \frac{E_2 = E_1}{E_1 = E_2} \qquad \frac{E_1 = E_2 \quad E_2 = E_3}{E_1 = E_3}$$

$$\frac{E_1 = E_2}{f(E_1) = f(E_2)} \text{ congruence}$$

  - example

$$g(g(g(x))) = x \wedge$$
$$g(g(g(g(g(x))))) = x \wedge$$
$$g(x) \neq x$$

is unsatisfiable

- **Real numbers under addition**
  - Symbols $\geq, =, +,$ int. literals

example

$$y > 2x + 1 \wedge y + x > 1 \wedge y < 0$$ is unsat

  - decidable, even in polynomial time
- **natural numbers under addition** (Presburger)
  - also decidable

- theory of list structures

  cons , car , cdr , atom , nil

$$car(x) = car(y) \wedge cdr(x) = cdr(y) \Rightarrow x = y$$

- axioms
  - atom(nil)

$$car(cons(x,y)) = x$$

$$cdr(cons(x,y)) = y$$

$$atom(x) \Rightarrow x \neq cons(y,z)$$

- arrays

$$sel(upd(x,y,z),y) = z$$

$$y \neq y' \Rightarrow sel(upd(x,y,z),y') = sel(x,y')$$

- example

$$upd(x,y,sel(x,y)) = x$$