Predicate logic: Semantics

CS242 Formal Specification and Verification

University of Warwick

Autumn term 2006

Models

Let $\mathcal{F}$ be a set of function symbols and $\mathcal{P}$ a set of predicate symbols. A *model* $\mathcal{M}$ of the pair $(\mathcal{F}, \mathcal{P})$ consists of the following:

1. a non-empty set A, the *universe of concrete values*;
2. for each $f \in \mathcal{F}$ with n arguments, a concrete function

$$f^{\mathcal{M}} : A^n \to A$$

3. for each $P \in \mathcal{P}$ with n arguments, a subset

$$P^{\mathcal{M}} \subseteq A^n$$

Environments

An *environment* is a function

$$I : \mathrm{var} \to A$$

Let I be an environment for a universe of concrete values A, and let $a \in A$. We denote by $I[x \mapsto a]$ the following environment:

$$I[x \mapsto a](y) = \begin{cases} a, & \text{if } y = x \\ I(y), & \text{if } y \neq x \end{cases}$$

Satisfaction

Given a model $\mathcal{M}$ for a pair $(\mathcal{F}, \mathcal{P})$, an environment l for the universe of concrete values A of $\mathcal{M}$, and a formula ϕ over $(\mathcal{F}, \mathcal{P})$,

$$\mathcal{M} \models_l \phi$$

says that ϕ computes to $\mathtt{T}$ in the model $\mathcal{M}$ with respect to l.

For any term t, let

$$t^{\mathcal{M},l}$$

be the value of t obtained by interpreting any function symbol $f \in \mathcal{F}$ by $f^{\mathcal{M}}$, and any variable x by $l(x)$.

We define $\mathcal{M} \models_I \phi$ by structural induction on ϕ:

P: $\mathcal{M} \models_I P(t_1, t_2, \ldots, t_n)$ iff

$$(t_1^{\mathcal{M},I}, t_2^{\mathcal{M},I}, \ldots, t_n^{\mathcal{M},I}) \in P^{\mathcal{M}}$$

$\forall x$: $\mathcal{M} \models_I \forall x\, \psi$ iff $\mathcal{M} \models_{I[x \mapsto a]} \psi$ for all $a \in A$.

$\exists x$: $\mathcal{M} \models_I \exists x\, \psi$ iff $\mathcal{M} \models_{I[x \mapsto a]} \psi$ for some $a \in A$.

$\neg$: $\mathcal{M} \models_I \neg\psi$ iff not $\mathcal{M} \models_I \psi$.

$\vee$: $\mathcal{M} \models_I \psi_1 \vee \psi_2$ iff $\mathcal{M} \models_I \psi_1$ or $\mathcal{M} \models_I \psi_2$.

$\wedge$: $\mathcal{M} \models_I \psi_1 \wedge \psi_2$ iff $\mathcal{M} \models_I \psi_1$ and $\mathcal{M} \models_I \psi_2$.

$\rightarrow$: $\mathcal{M} \models_I \psi_1 \rightarrow \psi_2$ iff $\mathcal{M} \models_I \psi_2$ whenever $\mathcal{M} \models_I \psi_1$.

Semantic entailment

$$\phi_1, \phi_2, \ldots, \phi_n \models \psi$$

denotes that, whenever $\mathcal{M} \models_l \phi_i$ for all i, then $\mathcal{M} \models_l \psi$, *for all* models $\mathcal{M}$ and environments l.

Some examples:

$$\forall x(P(x) \rightarrow Q(x)) \models \exists x\, P(x) \rightarrow \exists x\, Q(x)$$

$$\exists x\, P(x), \forall x(P(x) \rightarrow Q(x)) \models \forall y\, Q(y)$$

Semantics of equality

If $= \in \mathcal{P}$, $=^{\mathcal{M}}$ must be actual equality on the universe of concrete values A:

$$=^{\mathcal{M}} = \{(a, a) \mid a \in A\}$$