Lecture 24 November 18, 2010

Semantics of Evidence for First-Order Logic and Integer Arithmetic.

Smullyan gives us Tarski's truth semantics for First-Order Logic. There is another semantics that justifies the computational content we are finding in proofs as in our interpretation of some proof expressions as computable functions. I call this a semantics of evidence. It assigns meaning to formulas and to proof expressions.

Meaning of formulas is given using these operations.

Given sets A and B, let

$A \times B$ be the set of ordered pairs $\langle a,b \rangle$ for $a \in A$, $b \in B$, the product.

$A + B$ be the set of elements $inl(a)$, $inr(b)$ for $a \in A$, $b \in B$, the disjoint union.

$A \to B$ the functions $\lambda(x.\, exp)$ such that for $a \in A$, $exp(a)$ belongs to B, the functions from A to B.

If $B(x)$ is a set for each $a \in A$, then let

$\prod_{x \in A} B(x)$ denote the functions from a into the union of all $B(a)$ for $a \in A$ such that $f(a) \in B(a)$.

$$\sum_{x \in A} B(x) = \{ \langle a,b \rangle \mid a \in A \text{ and } b \in B(a) \}$$

Lecture 24 continued 2

Let $\mathcal{M}$ be a model (interpretation) for first-order formulas of a given signature $\mathcal{I}$, i.e. choise of predicates $P_1^{n_1}, P_2^{n_2}, \ldots, P_k^{n_k}$ with arities n_i.

Given a first-order formula A with signature $\mathcal{I}$, define $\mathcal{M}[\![A]\!](s)$ as the evidence for formula A in model $\mathcal{M}$ with state s ($s(x)$ gives the value in the model of variable x in state s).

<u>Evidence Semantics</u>

1. $\mathcal{M}[\![false]\!](s) = \phi$ the empty set
2. $\mathcal{M}[\![P^n(t_1, \ldots, t_n)]\!](s) = \{true\}$ iff $\mathcal{M} \models_s P(t_1, \ldots, t_n)$ for P^n an atomic relation in the signature $\mathcal{I}$. otherwise it is the empty set ϕ.
3. $\mathcal{M}[\![A \& B]\!](s) = \mathcal{M}[\![A]\!](s) \times \mathcal{M}[\![B]\!](s)$
4. $\mathcal{M}[\![A \vee B]\!](s) = \mathcal{M}[\![A]\!](s) + \mathcal{M}[\![B]\!](s)$
5. $\mathcal{M}[\![A \Rightarrow B]\!](s) = \mathcal{M}[\![A]\!](s) \to \mathcal{M}[\![B]\!](s)$
6. $\mathcal{M}[\![\forall x. B]\!](s) = \prod_{y \in M} \mathcal{M}[\![B]\!]\, s[x := y]$ where M is the universe of the model $\mathcal{M}$
7. $\mathcal{M}[\![\exists x. B]\!](s) = \sum_{y \in M} \mathcal{M}[\![B]\!]\, s[x := y]$

Lecture 24 continued 3

We can prove using set theory and the axiom of choice that a formula A is satisfiable in a model $\mathcal{M}$ and state s if and only if $\mathcal{M}[A](s)$ is non-empty, i.e.

$$\mathcal{M} \models_s A \text{ iff there is an } a \in \mathcal{M}[A](s).$$

It is easy to see that the proof expressions we provided with the rules can be seen as expressions that denote evidence for the formulas they prove. The evidence for atomic formulas is either the empty set or the set $\{true\}$.

To provide an evidence semantics for arithmetic, say Peano Arithmetic for simplicity, we need to see the proof expression for Standard Induction. We treat it as the following rule

$$H, x : \mathbb{N} \vdash P(x) \text{ by } ind(x;\ \_\_\_\_;\ u, i.\ \_\_\_\_\_\_)$$

$$\text{" \quad " \quad "} \vdash P(0) \text{ by } b$$

$$H, u : \mathbb{N}, 0 < u, P(u-1) \vdash P(u) \text{ by } p(u,i)$$

The computation rule for $ind(x; p_0; u, i.\, p(u,i))$ is

$$ind(0; p_0; \_\_) = p_0$$

$$ind(n+1; p_0; u, i.\, p(u,i)) = p(n, ind(n; p_0; u, i.\, p(u,i)))$$

Note, this is just primitive recursion.