Lecture 34

November 28, 2005

1 Review

As a continuation of our discussion last time, in this lecture we look into the age-old problem: when is a formula valid? What is true? This problem may look philosophical in nature, but actually occurs in many places in Computer Science, e.g. when we want to prove something about a program. We previously showed that validity is undecidable, but recursively enumerable.

Recall that validity is an example of what we call a **decision problem**: Given a first order sentence φ, is φ *valid*? (i.e. is it true that $\models \varphi$?)

The sentence φ can in general have an arbitrary structure. In order to handle this problem, in last lecture we introduced some transformations to the formula such that certain properties are preserved:

- *Elimination of* $\approx$ - preserves satisfiability
- *Prenex Normal Form* - preserves equivalence
- *Skolemization* - preserves satisfiability

We now want to consider the more general case of a structure. This is called a **Herbrand** structure. In such a structure, we include all the terms as elements of the domain. Specifically, we define:

$$A_H = (G_H, f_1^A, \ldots, f_n^A) \text{ where } f_i^A(\text{"}t\text{"}) = \text{"}f_i(t)\text{"}$$

In this kind of structure:

- Every term belongs to the domain
- The functions absorb the complexity of the existential quantifiers (through Skolemization)
- There is at least one constant (which we can think of as a 0-ary function)
- D_H is the set of all ground terms

We now have the notion of satisfiability in a Herbrand structure

$A_H \models (\forall x_1)\dots(\forall x_n)\theta$ iff for all ground terms $t_1,\dots,t_n$ we have that $A_H\langle x_1 \mapsto t_1,\dots,x_n \mapsto t_n\rangle \models \theta$.

With respect to the latter there is also the following lemma:

Lemma 1. *$A_H\langle x_1 \mapsto t_1,\dots,x_n \mapsto t_n\rangle \models \theta$ iff $A_H \models \theta[x_1 \mapsto t_1,\dots,x_n \mapsto t_n]$ where in the right side we see that the formula has no free variables.*

An example of a formula without variables can be : $\varphi = P(c, f(c), g(f(a), b))$ where a, b, and c are constants of the domains.

Proof. We give a proof by induction on θ. Suppose θ is atomic:

1. $A_H\langle x_1 \mapsto t_1,\dots,x_n \mapsto t_n\rangle \models P(s_1,\dots,s_k)$ iff $\langle \overline{a}(s_1),\dots,\overline{a}(s_k)\rangle \in P^A$
2. $A_H \models P(s_1,\dots,s_k)[x_1 \mapsto t_1,\dots,x_n \mapsto t_n]$ iff $\langle s_1,\dots,s_k\rangle[x_1 \mapsto t_1,\dots,x_n \mapsto t_n] \in P^A$

Now 1 and 2 are equivalent if they are identical element by element :

$$\overline{a}(s_i) = s_i[x_1 \mapsto t_1,\dots,x_n \mapsto t_n]$$

To prove the latter, we have to use induction on s_i which can be a variable or a function. We will need to use the properties of the Herbrand structure. $\square$

Lemma 1 has an interesting consequence.

Corollary 1. *$A_H \models (\forall x_1)\dots(\forall x_n)\theta$ iff for all ground terms $t_1,\dots,t_n$ we have $A_H \models \theta[x_1 \mapsto t_1,\dots,x_n \mapsto t_n]$.*

This corollary describes a way by which we can actually mix semantics (on the left side) with syntax (on the right side). We have the definition:

Definition 1 (Ground Terms). $ground(\theta) = \{\theta[x_1 \mapsto t_1,\dots,x_n \mapsto t_n] | t_1,\dots,t_n \in D^H\}$

So the corollary says that : $A_H \models (\forall x_1)\dots(\forall x_n)\theta$ iff $A_H \models ground(\theta)$

The most important result concerning the Herbrand structures is the following:

Herbrand Theorem $(\forall x_1)\dots(\forall x_n)\theta$ is satisfiable iff $A_H \models (\forall x_1)\dots(\forall x_n)\theta$

A corollary of that is that $(\forall x_1)\dots(\forall x_n)\theta$ is satisfiable iff $ground(\theta)$ is satisfiable. In this way, we can completely get rid of the quantifiers and end up with a set of variable-free formulas, even though the set can be potentially infinite. It is important to remember that a Herbrand universe is finite only when all the functions are 0-ary. (Otherwise, the returning result of a function can be recursively plugged in to another or the same function to produce an infinite number of terms).

The last thing we will see, is that if we take a formula in a Herbrand universe, we can actually turn it into a propositional formula. Remember that $A_H \models P(s_1, \ldots, s_n)$ iff $\langle s_1, \ldots s_n \rangle \in P^A$. If can introduce a new proposition that talks about the predicate (which is first order fact) : $q_{P(s_1,\ldots,s_n)}$. We now define:

$$prop(\theta) = ground(\theta)[P(s_1, \ldots, s_k) \mapsto q_{P(s_1,\ldots,s_n)}$$ [1]

The important result here is that $ground(\theta)$ is satisfiable iff $prop(\theta)$ is satisfiable. We now see that all the transformation we tried to do and the introduction of the Herbrand structure have a meaning, since we can use them to transform a first order formula into a propositional formula with same satisfiability properties.

This is described by the following theorem.

Theorem $(\forall x_1) \ldots (\forall x_n)\theta$ is unsat iff a finite subset of $prop(\theta)$ is unsat

The corollary of the is that *Validity* is *semi-decidable* (this is Gödel's completeness theorem). We can practically start checking all finite subsets. The program will stop if the formula is truly unsat. Moreover, validity is not decidable (Church - Turing, 1936-37). Though, we know that φ is sat iff $\neg\varphi$ is not valid. So satisfiability is in Co-RE but not RE. [2] Another result in the area is the first-order resolution by John Robinson in 1965.

In the next lecture we talk more about incompleteness...

[1] For example if we have in the Herbrand universe the formula $P_1(c, f(c)) \wedge \neg P_2(g(f(c)), f(c))$ we get the propositional formula $q_{P_1} \wedge \neg q_{P_2}$

[2] Remember that if a problem is in Co-RE and RE it is in R