Lecture 13

The Herbrand Universe Construction

February 19, 1998
Lecturer: Richard Ladner
Notes: Marc T. Friedman

13.1. The Theorem and its Implications

Theorem 13.1: Given Γ, a recursively enumerable set of first-order sentences, we construct a set H_Γ of *propositional* formulas which is satisfiable if and only if Γ is. This effective construction builds a Turing machine generating H_Γ given one generating Γ. Furthermore, if Γ is satisfiable, then H_Γ will completely describe a countable model for Γ, which can easily be extracted from a model for H_Γ.

This theorem has a number of remarkable consequences.

- **Compactness.** Γ is satisfiable if and only if all of its finite subsets are. This is often stated in the contrapositive: if Γ is unsatisfiable, so is some finite subset of Γ. This follows from the Herbrand universe construction by virtue of the fact that any unsatisfiable subset of H_Γ is constructed (by a process described below) from a finite subset of Γ, and there is a compactness theorem for propositional logic.
- **Lowenheim-Skolem Theorem.** If Γ is satisfiable, then it is so in a countable (possibly finite) model. In some sense, this exposes a weakness of first-order logic in that it cannot express any property of uncountable sets that distinguish them from countable ones. For instance, the first-order theory of real numbers $Th(\Re) = (\Re, +, *, <, 0, 1)$ has a countable "non-standard" model, model. For example the first-order theory cannot talk about arbitrary functions. Talking about functions is vital for discussions about derivatives and integrals.
- **Completeness.** if Γ is recursively enumerable so is $CN(\Gamma)$. The more familiar statement is that if $\Gamma \models \alpha$ then $\Gamma \vdash \alpha$. The more familiar statement follows from the fact that the Herbrand universe construction defines a proof system for first-order logic by the observation that $\Gamma \cup \{\neg\alpha\}$ is not satisfiable if and only if $\Gamma \models \alpha$. If $\Gamma \cup \{\neg\alpha\}$ is not satisfiable then there is a finite subset of H_Γ that is not satisfiable. Such a finite subset can be found as part of the construction of H_Γ.

13.2. The construction

Given Γ, a countable set of first-order sentences.

- Construct P_Γ, the *prenex* form of sentences in Γ. Rename away any variables whose scopes overlap, and move the quantifiers forward. For instance, change

$$\forall x \forall y (R(x, y) \wedge \exists y P(y))$$

to

$$\forall x \forall y \exists z (R(x, y) \wedge P(z)).$$

P_Γ is satisfiable if and only if Γ is, by the same model.

- Construct S_Γ, the *Skolemization* of P_Γ, to eliminate existential quantifiers while introducing new function symbols. For instance, if α is some formula with free variables x_1, x_2, x_3, x_4, to convert the sentence

$$\forall x_1 \exists x_2 \forall x_3 \exists x_4 \alpha(x_1, x_2, x_3, x_4)$$

introduce two new functions $f()$ and $g()$, resulting in

$$\forall x_1 \forall x_3 \alpha(x_1, f(x_1), x_3, g(x_1, x_3)).$$

S_Γ is satisfiable if and only if P_Γ is, since any model of P_Γ will have an object assigned to each universally quantified variable which depends only on the preceding quantified variables, which assures us that functions f and g exist. On the other hand, if you can find such functions, then the existentially quantified variables clearly exist.

- Add the axioms of equality to S_Γ to construct E_Γ. These rules completely characterize the behavior of equality as an equivalence relation on, and how it interacts with function and relation symbols:[1]

  1. $\forall x(x = x)$
  2. $\forall x \forall y(x = y \Rightarrow y = x)$
  3. $\forall x \forall y \forall z(x = y \wedge y = z \Rightarrow x = z)$
  4. Relations respect equality. Adopt the shorthand $\bar{x}$ for the vector of variables $x_1, x_2, \ldots, x_k$.

$$\forall \bar{x} \forall \bar{y}(\bar{y} = \bar{x} \Rightarrow (R(\bar{x}) \equiv R(\bar{y}))$$

In other words, given equal parameters, the boolean value R returns must be the same.

[1]Throughout these notes, the equals sign will be used for many different things. It should be clear enough from context whether we intend the equals sign in the formal first-order language, equality of objects, or equality in the presentation metalanguage. Boolean equivalence is distinct, however.

5. Functions respect equality.

$$\forall \bar{x} \forall \bar{y} (\bar{y} = \bar{x} \Rightarrow (f(\bar{x}) = f(\bar{y}))$$

That is, given equal arguments, the objects f refers to must be the identical object in the universe.

E_Γ is satisfiable whenever S_Γ is, since it merely states that equality is interpreted correctly. Note that there are no existential quantifiers in the equality axioms.

- Construct H_Γ, the instances of Γ, from E_Γ. In essence we replace universal quantification with enumeration. First introduce one constant symbol, c. Then T_Γ is the set of all terms constructed from c and the function symbols, *e.g.*

$$T_\Gamma = \{c, f(c), f(f(c)), g(c, c), g(c, f(c)), \ldots\}.$$

Now

$$H_\Gamma = \{\alpha(t_1, \ldots, t_k) | \forall x_1 \forall x_2 \ldots \forall x_k \alpha(x_1, x_2, \ldots, x_k) \in E_\Gamma \text{ and } t_i \in T_\Gamma .\}$$

H_Γ contains relations and functions and c, but no quantifiers. So think of each relation such as $R(g(c, f(c)), c)$ or $f(c) = f(f(c))$ as a distinct proposition.

13.3. Correctness.

Claim: H_Γ is satisfiable *as a propositional formula* if and only if E_Γ is satisfiable as a set of first order sentences.

First a few words of explanation. A term or relation is *ground* if it has no variables. The propositions in H_Γ are ground relations, or propositions, like $R(g(c, f(c)), c)$ or $f(c) = f(f(c))$. Each is a sentence which is either true or false. We can enumerate the ground relations, and associate with each a boolean variable, such as $v_{R(g(c,f(c)),c)}$. Then H_Γ can be viewed as boolean propositional formula on these new boolean variables.

Proof: Assume E_Γ is satisfiable, so there is a model $\mathcal{M} \models E_\Gamma$. Choose $c^{\mathcal{M}} \in \mathcal{U}^{\mathcal{M}}$. Now all $t \in T_\Gamma$ are interpreted as an element $t^{\mathcal{M}} \in \mathcal{U}^{\mathcal{M}}$ recursively. For example:

$$f(f(c))^{\mathcal{M}} = f^{\mathcal{M}}(f^{\mathcal{M}}(c^{\mathcal{M}})).$$

Now we define an assignment σ from the propositional variables of H_Γ into $\{T, F\}$:

$$\sigma(R(t_1, t_2)) = R^{\mathcal{M}}(t_1^{\mathcal{M}}, t_2^{\mathcal{M}})$$

$$\sigma(t_1 = t_2) = t_1^{\mathcal{M}} = t_2^{\mathcal{M}}\ ^2$$

Now we claim that for all ground quantifier-free sentences α,

$$\mathcal{M}, c = c^{\mathcal{M}} \models \alpha \Leftrightarrow \sigma \models \alpha. \tag{13.1}$$

Note that we write $\mathcal{M}, c = c^{\mathcal{M}}$ because the model $\mathcal{M}$ does not contain an interpretation for the symbol c. Thus, the notation simply extends the model $\mathcal{M}$ to include an interpretation for c. The equivalence (13.1) transparently true by induction on the structure of α and the definition of σ.

To finish this direction let $\alpha(t_1, t_2, \ldots, t_k) \in H_\Gamma$. We have the follow sequence of consequences:

$\mathcal{M} \models \forall x_1 \forall x_2 \ldots \forall x_k \alpha(x_1, x_2, ..., x_k)$ because $\forall x_1 \forall x_2 \ldots \forall x_k \alpha(x_1, x_2, ..., x_k) \in E_\Gamma$
$\mathcal{M}, c = c^{\mathcal{M}} \models \alpha(t_1, t_2, \ldots, t_k)$ because the formula is universal
$\sigma \models \alpha(t_1, t_2, \ldots, t_k)$ by the equivalence (13.1).

To prove the other direction, let $\sigma \models H_\Gamma$. Now, we define an equivalence relation $\sim$ on terms in T_Γ. $t_1 \sim t_2$ if $\sigma(t_1 = t_2) = T$. The equality axioms 1-3 are used to show that $\sim$ is an equivalence relation Also define $[t] = \{t' | t \sim t'\}$. Then we define the model $\mathcal{M} = (\mathcal{U}^{\mathcal{M}}, I^{\mathcal{M}})$ where the language of $\mathcal{M}$ contains all the symbols of E_Γ and c. The universe contains the equivalence classes over terms:

$$\mathcal{U}^{\mathcal{M}} = \{[t] | t \in T_\Gamma\}.$$

The relations are well-defined on equivalence classes, by the fourth axiom of equality:

$$R^{\mathcal{M}}([t_1], [t_2], \ldots, [t_k]) = \sigma(R(t_1, t_2, \ldots, t_k)).$$

The functions are well-defined on equivalence classes by the fifth axiom of equality:

$$f^{\mathcal{M}}([t_1], [t_2], \ldots, [t_k]) = [f(t_1, t_2, \ldots, t_k)].$$

Then we claim that for all quantifier-free ground formulas α,

$$\mathcal{M} \models \alpha \Leftrightarrow \sigma \models \alpha. \tag{13.2}$$

This proof is also a mechanical structural induction. Note further that this model contains an interpretation of the constant c, since α may contains c's. To obtain a model for E_Γ we remove

[2]Note the particularly perverse abuse of equals signs. The first is a symbol in the formula, the second is part of the metalanguage defining σ, and the third is equality in the universe.

the interpretation for the symbol c to yield a model $\mathcal{M}'$. Let $\forall x_1 \forall x_2 \ldots \forall x_k \alpha(x_1, x_2, ..., x_k)$ be a sentence in E_Γ. We have the following sequence of consequences:

$\sigma \models \alpha(t_1, t_2, \ldots, t_k)$ for all $t_1, t_2, \ldots, t_k \in T_\Gamma$ because $\alpha(t_1, t_2, \ldots, t_k) \models H_\Gamma$
$\mathcal{M} \models \alpha(t_1, t_2, \ldots, t_k)$ for all $t_1, t_2, \ldots, t_k \in T_\Gamma$ by equivalence (13.2)
$\mathcal{M}, x_1 = [t_1], \ldots, x_k = [t_k] \models \alpha(x_1, x_2, ..., x_k)$ for all $[t_1], [t_2], \ldots, [t_k] \in \mathcal{U}^{\mathcal{M}}$ by the semantics
$\mathcal{M} \models \forall x_1 \forall x_2 \ldots \forall x_k \alpha(x_1, x_2, ..., x_k)$ by the semantics
$\mathcal{M}' \models \forall x_1 \forall x_2 \ldots \forall x_k \alpha(x_1, x_2, ..., x_k)$ because $\forall x_1 \forall x_2 \ldots \forall x_k \alpha(x_1, x_2, ..., x_k)$ does not contain c.

Note further that by eliminating the interpretations for the symbols introduced by skolemization and the symbol c, $\mathcal{M}$ contains a model for the original Γ. This model is countable because there are only countably many terms in T_Γ.

Claim: The construction is effective. If Γ is recursively enumerable then H_Γ is recursively enumerable.

If Γ is recursively enumerable then you can generate its elements in sequence. As you generate them, maintain (perhaps each on a separate tape) a counter n of elements of Γ, the set of function symbols F, the set of relation symbols R, and the set E_Γ. Each time you generate a new sentence of Γ, update the lists. Add to E_Γ the prenex, Skolemized version of the sentence, and any equality axioms for the new function and relation symbols in it. On another tape, build T_Γ in lexicographic order, but only up to those terms of length n. When a new function symbol arises, extend T_Γ to include the terms of length n that contain the new symbol. On the last tape, maintain the elements of H_Γ of length $\leq n$ from E_Γ and T_Γ. You may have to extend these periodically to include formulas with a new symbol that arises from the generation of Γ. $\square$