Lecture 19

Categoricity and Second Order Predicate Logic

March 12, 1998
Lecturer: Richard Ladner
Notes: Nicholas Bone

In this lecture we will introduce two new concepts and briefly review the relationship between complexity and logic. We begin with a theorem.

Theorem 19.1: Let Γ be a complete, recursively ennumerable theory. Then Γ is decidable.

Proof: If Γ is inconsistent then it must contain everything (because it is a theory), and thus it is decidable. If Γ is consistent then $\forall \alpha, \alpha \in \Gamma \Leftrightarrow \neg\alpha \notin \Gamma$. Thus, any Turing machine that enumerates Γ will eventually enumerates either α or $\neg\alpha$, and this gives us a decision procedure for Γ. $\square$

19.1. Categoricity

Definition: A consistent theory Γ is λ-categorical if and only if all models of Γ of cardinality λ are isomorphic.

Theorem 19.2: Let Γ be a consistent λ-categorical theory (for some infinite λ) with no finite model. Then Γ is complete.

Proof: In order to prove this theorem we need another theorem called the "upward Lowenheim-Skolem theorem." It states that if Γ is a theory with an infinite model then it has a model of cardinality λ. Naturally, we are assuming that Γ only uses countably many symbols. Consider the sentences

$$\Delta = \Gamma \cup \{c_x \neq c_y : x \neq y \text{ and } x, y \in C\}$$

where C is a set of cardinality λ. Every finite subset of Δ is satisfiable because Γ has an infinite model that can be extended to include interpretations for any finite subset of the new constant symbols. By the compactness theorem Δ has a model. Now, use the Herbrand construction to build a model of Δ. The number of terms used in the construction has cardinality λ. Furthermore, the number of equivalence classes of terms in the model has the same cardinality because the equivalence class of each c_x is distinct from all the others. Thus, the Herbrand model has cardinality λ.

Now to show the Γ is complete, let α be a sentence. Let $\mathcal{M}$ be *the* model of Γ of cardinality λ. Either α is true or false in $\mathcal{M}$. Without loss of generality assume $\mathcal{M} \models \alpha$. We will now show that $\alpha \in \Gamma$. Suppose not. Then there is a model $\mathcal{M}'$ of $\Gamma \cup \{\neg\alpha\}$. $\mathcal{M}'$ is not finite by the hypothesis of the theorem. Thus, $\Gamma \cup \{\neg\alpha\}$ must have a model of cardinality λ by the upward Lowenheim-Skolem theorem. That model is isomorphic to $\mathcal{M}$. Thus, $\mathcal{M} \models \neg\alpha$, a contradiction. $\square$

19.1.1. Dense Linear Order without endpoints (DLO)

$CN(DLO) = Th(\mathcal{Q}, <)$ is recursively enumerable, and $\aleph_0$-categorical (from homework 3)**. There are various methods of proving this.

(**Footnote: $\aleph_0 = |\mathcal{N}|$ is the "smallest" infinity. $\aleph_1$ is defined as the "next smallest", and so on. The Continuum Hypothesis states that $\aleph_1 = 2^{\aleph_0}$. This is unprovable from any standard axioms of set theory.)

19.1.2. Algebraically closed fields of characteristic zero

The theory of algebraically closed fields is $2^{\aleph_0}$-categorical ($2^{\aleph_0} = |\mathcal{R}|$). In general, any algebraically closed field of characteristic zero may be described by three sets of axioms: the field axioms, the closure axioms, and the axioms that define the characteristic. We call these axioms ACF.

The Field Axioms: The classic field axioms hold for the rationals, reals, complex numbers, integers mod a prime, and many other important mathematical structures.

1. $\forall x(x + 0 = x \wedge 0 + x = x)$ (additive identity)
2. $\forall x \forall y(x + y = x \Rightarrow y = 0)$ (0 is unique)
3. $\forall x \exists y(x + y = 0 \wedge y + x = 0)$ (additive inverse)
4. $\forall x \forall y \forall z((x + y = 0 \wedge x + z = 0) \Rightarrow y = z)$ (inverse is unique)
5. $\forall x(1 \neq 0 \wedge x * 1 = x \wedge 1 * x = x)$ (multiplicative identity)
6. $\forall x \forall y(x * y = x \Rightarrow (y = 1 \vee x = 0))$ (1 is unique)
7. $\forall x \forall y(x * y = 0 \Rightarrow (x = 0 \vee y = 0))$ (no zero divisors)
8. $\forall x \exists y(x = 0 \vee (x * y = 1 \wedge y * x = 1))$ (multiplicative inverse)
9. $\forall x \forall y \forall z((x * y = 1 \wedge x * z = 1) \Rightarrow y = z)$ (inverse is unique)

Axioms 1-4 describe a group, 1-6 a ring with unit, 1-7 an integral domain, and the nine together describe a field.

The Closure Axioms: A field is algebraically closed if and only if it contains the roots of all its polynomials. The closure axioms are the following countable set:

1. $\forall y_0 \forall y_1 \exists x(y_0 + y_1 * x = 0)$
2. $\forall y_0 \forall y_1 \forall y_2 \exists x(y_0 + y_1 * x + y_2 * x * x = 0)$
3. $\forall y_0 \forall y_1 \forall y_2 \forall y_3 \exists x(y_0 + y_1 * x + y_2 * x * x + y_3 * x * x * x = 0)$
4. $\ldots$

Characteristic Zero: If there is a finite positive integer p such that $\overbrace{1+1+\cdots+1}^{p}=0$ and for all $0<p'<p$ $\overbrace{1+1+\cdots+1}^{p'}\neq 0$, then we say the field has characteristic p. If there is no such p the field is of characteristic 0. (Note that the only finite fields are of characteristic that is a prime power. We can define this as follows:

1. $1+1\neq 0$
2. $1+1+1\neq 0$
3. $1+1+1+1+1\neq 0$
4. ... etcetera.

It can be shown that every model of ACF of cardinality is isomorphic to $(\mathcal{C},+,*,0,1)$ where $\mathcal{C}$ is the complex numbers. So that $CN(ACF)$ is $2^{\aleph_0}$-categorical. $CN(ACF)$ has no finite models because of the "characteristic zero" axioms. Thus by theorem 19.2 $CN(ACF)$ is complete and equal to $Th((\mathcal{C},+,*,0,1))$. Finally ACF is recursively enumerable and so is $CN(ACF)$. Hence, by theorem 19.1 $CN(ACF)$ is decidable. Hence $Th((\mathcal{C},+,*,0,1))$ is decidable. This is an interesting proof because it gives no idea of the complexity of any algorithm to decide $Th((\mathcal{C},+,*,0,1))$.

Corollary 19.3: There is no way to define $\mathcal{Z}$ (the integers) in $Th((\mathcal{C},+,*,0,1))$.

Proof: Suppose that we could define $\mathcal{Z}$ in $Th((\mathcal{C},+,*,0,1))$. Then $Th((\mathcal{Z},+,*,0,1))$ would be reducible to $Th((\mathcal{C},+,*,0,1))$, but this is impossible because $Th((\mathcal{Z},+,*,0,1))$ is undecidable. □

19.1.3. Real ordered fields

Consider $Th((\mathcal{R},+,*,<,0,1))$. This is not categorical for any λ. However, it is decidable. Decision procedures can be arrived at using a variety of techniques including elimination of quantifiers and Ehrenfeucht games.

Note: $Th(\mathcal{C},+,*,0,1)$ has a countable model call the algebraic numbers. The algebraic numbers are formed my including all the roots to polynomials over the rationals and closing under addition, substraction, multiplication, and division. The algebraic numbers do not contain *trancendental numbers*, such as e and π.

19.2. Second Order Predicate Logic

Second order predicate logic is stronger than first order predicate logic in that we can quantify over sets, relations, and functions as well as the elements in the universe. First a definition:

$CN_2(\Gamma)$ = the second order consequences of Γ.

Note that $CN_2(\emptyset)$ (the second order validities) is not recursively enumerable. In fact, $CN_2(\emptyset)$ is *non-arithmetic*, which means that it cannot be reduced to any member of the infinite chain:

$$\phi_0 <_T \phi_1 <_T \phi_2 <_T \cdots,$$

where $\phi_0 = \emptyset$ and $\phi_{i+1} = K^{\phi_i}$.

Define $S1S = Th_2^m(\mathcal{N}, s, 0)$ = the monadic second order theory of successor. That is, we allow quantification over sets. Note that this is essentially the same as quantifying over unary relations, because any set A may be defined by the relation $R_A(x) \Leftrightarrow x \in A$. The following is an example of a valid formula in $S1S$:

$$\forall X \forall y \forall z ((0 \in X \wedge (y \in X \Leftrightarrow s(y) \notin X)) \Rightarrow (z \in X \Leftrightarrow s(s(z)) \in X))$$

Theorem 19.4: $S1S$ is decidable.

This result was proved in 1960 by Büchi using a reduction to the emptiness problem for ω-automata (automata on infinite strings).

Theorem 19.5: $S1S$ is *non-elementary.* That is, $S1S \notin \mathrm{SPACE}(2^{2^{\cdot^{\cdot^{\cdot^{2^n}}}}})$ for any finite stack of 2's.

This result was proved in 1975 by Albert Meyer.

19.3. Summary of Complexity of Logical Theories

We conclude the lecture with a brief review of the complexity of logical problems.

	Prop. Logic	Modal Logic	Temp. Logic	Knowledge & Time	1^{st} order Logic	2^{nd} order Logic
NA				$\vert$	$Th(\mathcal{N},+,*)$	validities
RE				$\vert$	validities	$\vert$
NE				$\vert$	$\vert$	$S1S$, $S2S$
2-EXP			CTL^*	$\vert$	$Th(\mathcal{N},+)$	
EXP		common-knowledge	CTL	$\vert$	$Th(\mathcal{R},+)$	
PSPACE	QBF	K-modal, 2-knowledge	LTL		$Th(=)$, $Th(<)$, $Th(s)$	
NP	$PROP$	1-knowledge				
P	$HORN$					

Complexity classes are shown on the vertical axis (NA = non-arithmetic, RE = recursively enumerable, NE = non-elementary). Logic systems are shown on the horizontal axis. A vertical line (|) represents the existence of natural problems in that logic system and complexity class that we wish to leave nameless.

As can be seen, very few logical theories have worst case complexity even in NP and many are not even arithmetic. This appears to put a crimp on trying to directly uses classical logic as a basis for automatic verification of programs. Nonetheless, there are fragments of varies theories that appear to be effective tools in verification. Certainly, model checking has been proven to a success in hardware verification.

Hopefully, this course has provided insight into the power and complexity of logic.