CS 357: Advanced Topics in Formal Methods
Fall 2019

Lecture 9

Aleksandar Zeljić
(materials by Clark Barrett)
Stanford University

Theories

We define a *theory* as a set of first-order sentences *closed under logical implication*.

Thus, T is a theory iff T is a set of sentences and if $T \models \sigma$, then $\sigma \in T$ for every sentence σ.

Examples

- For a given signature, the smallest possible theory consists of exactly the valid sentences over that signature.
- The largest theory for a given signature is the set of all sentences. It is the only unsatisfiable theory. Why?

Theories

For a class $\mathcal{K}$ of models over a given signature Σ, define the *theory of* $\mathcal{K}$ as

$$Th\,\mathcal{K} = \{\sigma \mid \sigma \textit{ is a } \Sigma\textit{-sentence which is true in every model in } \mathcal{K}\}.$$

Theorem

$Th\,\mathcal{K}$ is indeed a theory.

Proof

Suppose $Th\,\mathcal{K} \models \sigma$. We know that $\models_M Th\,\mathcal{K}$ for each M in $\mathcal{K}$. It follows that $\models_M \sigma$ for each M in $\mathcal{K}$, and thus $\sigma \in Th\,\mathcal{K}$.

□

Suppose Γ is a set of sentences.

Define the set $Cn\ \Gamma$ of *consequences* of Γ to be $\{\sigma \mid \Gamma \models \sigma\}$.

Then $Cn\ \Gamma = Th\,Mod\ \Gamma$.

Theories

A theory T is *complete* iff for every sentence σ, either $\sigma \in T$ or $(\neg\sigma) \in T$.

Note that if M is a model, then $Th\ \{M\}$ is complete. In fact, for a class $\mathcal{K}$ of models, $Th\,\mathcal{K}$ is complete iff any two members of $\mathcal{K}$ are elementarily equivalent.

A theory T is *axiomatizable* iff there is a decidable set Γ of sentences such that $T = Cn\ \Gamma$.

A theory T is *finitely axiomatizable* iff $T = Cn\ \Gamma$ for some finite set Γ of sentences.

Theorem

If $Cn\ \Gamma$ is finitely axiomatizable, then there is a finite $\Gamma_0 \subseteq \Gamma$ such that $Cn\ \Gamma_0 = Cn\ \Gamma$.

Proof

If $Cn\ \Gamma$ is finitely axiomatizable, then for some sentence τ, $Cn\ \Gamma = Cn\ \tau$. Clearly, $\Gamma \models \tau$. By compactness, we have that there exists $\Gamma_0 \subseteq \Gamma$ such that $\Gamma_0 \models \tau$. Thus, $Cn\ \tau \subseteq Cn\ \Gamma_0 \subseteq Cn\ \Gamma$, and since $Cn\ \Gamma = Cn\ \tau$, it follows that $Cn\ \Gamma_0 = Cn\ \Gamma$.

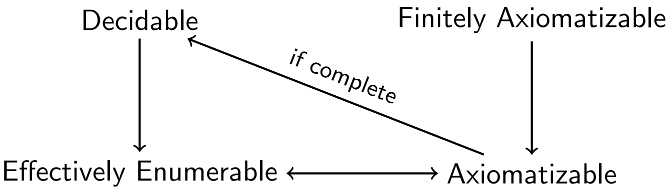
□

Theories

Using the above terminology, we can restate our earlier results as follows:

- An axiomatizable theory (in a reasonable language) is effectively enumerable.
- A complete axiomatizable theory (in a reasonable language) is decidable.

Our results about theories can be summarized in the following diagram.



Los-Vaught Test

For a theory T and a cardinal λ, say that T is *λ-categorical* iff all models of T having cardinality λ are isomorphic.

Theorem

Let T be a theory in a countable language such that

- T is λ-categorical for some infinite cardinal λ.
- All models of T are infinite.

Then T is complete.

Proof

It suffices to show that for any two models M and M' of T, $M \equiv M'$. Since M and M' are infinite, there exist (by **LST**) elementarily equivalent models of cardinality λ. But these models must be isomorphic, and by the homomorphism theorem, isomorphic models are elementarily equivalent.

□

Validity and Satisfiability Modulo Theories

Given a Σ-theory T, a Σ-formula ϕ is

1. *T-valid* if $\models_M \phi[s]$ for all models M of T and all variable assignments s.
2. *T-satisfiable* if there exists some model M of T and variable assignment s such that $\models_M \phi[s]$.
3. *T-unsatisfiable* if $\not\models_M \phi[s]$ for all models M of T and all variable assignments s.

The *validity problem* for T is the problem of deciding, for each Σ-formula ϕ, whether ϕ is T-valid.

The *satisfiability problem* for T is the problem of deciding, for each Σ-formula ϕ, whether ϕ is T-satisfiable.

Similarly, one can define the *quantifier-free validity problem* and the *quantifier-free satisfiability problem* for a Σ-theory T by restricting the formula ϕ to be quantifier-free.

Validity and Satisfiability Modulo Theories

A decision problem is *decidable* if there exists an effective procedure which always terminates with an answer for any given instance of the problem.

For example, the validity problem for a Σ-theory T is decidable if there exists an effective procedure for determining whether $T \models \phi$ for every Σ-formula ϕ.

Note that validity problems can always be reduced to satisfiability problems:

> ϕ *is* T*-valid iff* $\neg\phi$ *is* T*-unsatisfiable.*

We will consider a few examples of theories which are of particular interest in verification applications.

The Theory $T_{\mathcal{E}}$ of Equality

The theory $T_{\mathcal{E}}$ of equality is the theory $Cn\ \emptyset$.

Note that the exact set of sentences in $T_{\mathcal{E}}$ depends on the signature in question.

The theory does not restrict the possible values of symbols in any way. For this reason, it is sometimes called the theory of *equality with uninterpreted functions (EUF)*.

The satisfiability problem for $T_{\mathcal{E}}$ is just the satisfiability problem for first order logic, which is undecidable.

The satisfiability problem for conjunctions of literals in $T_{\mathcal{E}}$ is decidable in polynomial time using *congruence closure*.

The Theory $T_{\mathcal{Z}}$ of Integers

Let $\Sigma_{\mathcal{Z}}$ be the signature $(0, 1, +, -, \leq)$.

Let $\mathcal{A}_{\mathcal{Z}}$ be the standard model of the integers with domain $\mathcal{Z}$.

Then $T_{\mathcal{Z}}$ is defined to be $Th\,\mathcal{A}_{\mathcal{Z}}$.

As showed by Presburger in 1929, the validity problem for $T_{\mathcal{Z}}$ is decidable, but its complexity is triply-exponential.

The quantifier-free satisfiability problem for $T_{\mathcal{Z}}$ is "only" NP-complete.

Let $\Sigma_{\mathcal{Z}}^{\times}$ be the same as $\Sigma_{\mathcal{Z}}$ with the addition of the symbol $\times$ for multiplication, and define $\mathcal{A}_{\mathcal{Z}}^{\times}$ and $T_{\mathcal{Z}}^{\times}$ in the obvious way.

The satisfiability problem for $T_{\mathcal{Z}}^{\times}$ is undecidable (a consequence of Gödel's incompleteness theorem).

In fact, even the quantifier-free satisfiability problem for $T_{\mathcal{Z}}^{\times}$ is undecidable.

The Theory $T_{\mathcal{R}}$ of Reals

Let $\Sigma_{\mathcal{R}}$ be the signature $(0, 1, +, -, \leq)$.

Let $\mathcal{A}_{\mathcal{R}}$ be the standard model of the reals with domain $\mathcal{R}$.

Then $T_{\mathcal{R}}$ is defined to be $Th\,\mathcal{A}_{\mathcal{R}}$.

The satisfiability problem for $T_{\mathcal{R}}$ is decidable, but the complexity is doubly-exponential.

The quantifier-free satisfiability problem for conjunctions of literals (atomic formulas or their negations) in $T_{\mathcal{R}}$ is solvable in polynomial time, though exponential methods (like Simplex or Fourier-Motzkin) often perform better in practice.

Let $\Sigma_{\mathcal{R}}^{\times}$ be the same as $\Sigma_{\mathcal{R}}$ with the addition of the symbol $\times$ for multiplication, and define $\mathcal{A}_{\mathcal{R}}^{\times}$ and $T_{\mathcal{R}}^{\times}$ in the obvious way.

In contrast to the theory of integers, the satisfiability problem for $T_{\mathcal{R}}^{\times}$ is decidable.

The Theory $T_{\mathcal{A}}$ of Arrays

Let $\Sigma_{\mathcal{A}}$ be the signature $(read, write)$.

Let $\Lambda_{\mathcal{A}}$ be the following axioms:

$$\forall a \, \forall i \, \forall v \, (read(write(a, i, v), i) = v)$$
$$\forall a \, \forall i \, \forall j \, \forall v \, (i \neq j \rightarrow read(write(a, i, v), j) = read(a, j))$$
$$\forall a \, \forall b \, ((\forall i \, (read(a, i) = read(b, i))) \rightarrow a = b)$$

Then $T_{\mathcal{A}} = Cn \ \Lambda_{\mathcal{A}}$.

The satisfiability problem for $T_{\mathcal{A}}$ is undecidable, but the quantifier-free satisfiability problem for $T_{\mathcal{A}}$ is decidable (the problem is NP-complete).

Theories of Inductive Data Types

An *inductive data type* (IDT) defines one or more *constructors*, and possibly also *selectors* and *testers*.

Example: *list* **of** *int*

- Constructors: $cons : (int, list) \rightarrow list$, $null : list$
- Selectors: $car : list \rightarrow int$, $cdr : list \rightarrow list$
- Testers: is_cons, is_null

The *first order theory* of a inductive data type associates a function symbol with each constructor and selector and a predicate symbol with each tester.

Example: $\forall\, x : list.\ (x = null \vee \exists\, y : int, z : list.\ x = cons(y, z))$

For IDTs with a single constructor, a conjunction of literals is decidable in polynomial time.

For more general IDTs, the problem is NP-complete, but reasonbly efficient algorithms exist in practice.

Other Interesting Theories

Some other interesting theories include:

- Theory of bit-vectors
- Fragments of set theory
- Theory of floating-point arithmetic
- Theory of strings

SMT-LIB standard supports many different theories:
`http://smtlib.cs.uiowa.edu/logics.shtml`