Formal Methods: “Metatheory”

4.3 First-Order Theories

Johns Hopkins University, Spring 2017

Theories

Def 4.3.1. The **deductive closure/set of logical consequences** of a set of sentences Σ is $\text{Cn}\ \Sigma =_{df} \{\tau \mid \Sigma \models \tau\}$.

Def 4.3.2. Let T be a set of sentences. T is a **theory** iff $\text{Cn}\ T = T$.

Def 4.3.3. Let $\mathcal{K}$ be a class of structures for a 1st-order language $\mathcal{L}$. Then $Th\ \mathcal{K} =_{df} \{\sigma \mid \text{for each } \mathfrak{A} \in \mathcal{K}, \models_{\mathfrak{A}} \sigma\}$.

Convention. We write $Th\ \mathfrak{A}$ for $Th\ \{\mathfrak{A}\}$.

Lemma 4.3.1. $Th\ \mathcal{K}$ is indeed a theory for any $\mathcal{K}$.

In general, there are two methods for "locating" theories.

- Take $Th\ \mathcal{K}$ for some class $\mathcal{K}$ of structures.
- List a set Σ of sentences, then take $\text{Cn}\ \Sigma$.

Arithmetic Examples

Recall the standard model of arithmetic $\mathfrak{N} = (\mathbb{N}, 0, S, +, \cdot)$, where S is the successor function on $\mathbb{N}$ and $+$ and $\cdot$ the operations of addition and multiplication respectively. Then $Th\ \mathfrak{N}$ is the set of all 1st-order arithmetic truths.

In contrast, **Peano Arithmetic (PA)** is the set of 1st-order consequences of the following axioms.

(S1) $\forall x\ 0 \neq Sx$

(S2) $\forall x \forall y (Sx = Sy \supset x = y)$

(A1) $\forall x\ x + 0 = x$

(A2) $\forall x \forall y\ x + Sy = S(x + y)$

(M1) $\forall x\ x \cdot 0 = 0$

(M2) $\forall x \forall y\ x \cdot Sy = x \cdot y + x$

(IS) For each wff $\varphi(x)$, the universal generalization of $(\varphi(0) \wedge \forall x(\varphi(x) \supset \varphi(Sx))) \supset \forall x \varphi(x)$

Arithmetic Examples (cont.)

The first six axioms are true in $\mathfrak{N}$, and (IS) just embodies the principle of mathematical induction on $\mathbb{N}$. Hence,

$$\mathsf{PA} \subseteq \mathit{Th}\,\mathfrak{N}.$$

But is the converse the case, viz., that

$$\mathit{Th}\,\mathfrak{N} \subseteq \mathsf{PA}?$$

I.e., is every arithmetic truth a theorem of PA?

This is a deep question. Before attempting to answer it, let us go over some general features of theories.

Sizes of Models

Thm 4.3.2. If T has arbitrarily large finite models, then T has an infinite model.

Proof. Suppose that T has arbitrarily large finite models. Add to T the following infinite set Λ of sentences.

$$\begin{array}{lcl}
\exists^{\geq 2} & : & \exists x_1 \exists x_2 \; x_1 \neq x_2 \\
\exists^{\geq 3} & : & \exists x_1 \exists x_2 \exists x_3 (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3) \\
\vdots & \vdots & \vdots \\
\exists^{\geq n} & : & \exists x_1 \cdots \exists x_n (x_1 \neq x_2 \wedge \cdots \wedge x_1 \neq x_n \wedge \cdots \wedge x_{n-1} \neq x_n) \\
\vdots & \vdots & \vdots
\end{array}$$

Every finite subset of $T \cup \Lambda$ is satisfiable, and so by compactness, $T \cup \Lambda$ is satisfiable. But $T \cup \Lambda$ has only infinite models, each of which is also a model of T. Therefore, T has an infinite model. ■

Löwenheim-Skolem

Thm 4.3.3 (Löwenheim-Skolem). Let T be a theory in a countable 1st-order language. If T has a model, then T has a countable model.

One method for proving the completeness theorem for countable languages also provides a proof of the Löwenheim-Skolem theorem. That method is to construct for a consistent set of sentences a model whose domain of discourse consists of equivalence classes of terms of the language (supplement by a countably infinite set of new constants, introduced to have a witness for each existential sentence). Since the set of terms is countable, so is any set of equivalence classes of terms.

An extended version of the Löwenheim-Skolem theorem states that for any infinite cardinal κ, if the cardinality of the language is κ, then if T has a model, it has a model of cardinality κ or less.

Löwenheim-Skolem-Tarski

Thm 4.3.4 (Löwenheim-Skolem-Tarski). Let T be a theory in a countable 1st-order language. If T has an infinite model, then T has a model of size κ for each infinite cardinal κ.

Proof. Add to the language κ new constants $\{c_\alpha \mid \alpha < \kappa\}$, where α ranges over ordinals. Then for every pair of distinct ordinals $\alpha, \beta < \kappa$, add to T the sentence $c_\alpha \neq c_\beta$. The resulting set T^+ of sentences is such that every finite subset of T^+ has a model. So, by compactness, T^+ has a model $\mathfrak{A}$ (which, of course, is also a model of T). But in order to satisfy T^+, $|\mathfrak{A}|$ must have cardinality $\geq \kappa$. ■

The LST Theorem can also be generalized to languages of arbitrary infinite cardinalities.

Effective Procedures

Def 4.3.4*. An **effective procedure** is a procedure that can be performed by following a finite list of instructions each of which can be properly executed by a mechanical device. In particular, following the instructions involves no intuition, creativity, guess work, oracles, or random devices.

Example. A computer program that runs without error.

Examples. The usual methods of calculating sums, differences, products, and quotients taught in elementary school.

Example. Constructing the truth table for a wff of sentential logic.

In various contexts, an effective procedure is otherwise known as an **algorithm**.

An Explicit Example of an Effective Procedure

There is a standard algorithm for computing the factorial $n!$ of any natural number n. Intuitively $n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$ with the stipulation that $0! = 1$.

1. Input n. Go to 2.
2. Set $x := 0$ and $f := 1$. Go to 3.
3. Is $x = n$? If yes output the value of f and stop. If no, go to 4.
4. Increase the value of x by 1. Change the value of f to x times the old value of f. Go to 3.

This implements the standard recursive definition of the factorial function:

$$\begin{aligned} 0! &= 1 \\ (n+1)! &= n! \cdot (n+1). \end{aligned}$$

Enumerations and Enumerability

Def. An **enumeration** of a set A is a surjective element $f \in {}^{\mathbb{N}}A$, i.e., a mapping $f : \mathbb{N} \to A$ that is onto.

Example. Let A be the set of all even numbers. Define $f : \mathbb{N} \to A$ by

$$f(n) = \begin{cases} n & \text{if } n \text{ is even} \\ 2n & \text{otherwise.} \end{cases}$$

Frequently, an enumeration is indicated by listing the values $f(n)$ in increasing order of n. In this example, the listing would be:

$$0, 2, 2, 6, 4, 10, 6, 14, 8, 18, 10, 22, 12, 26, \ldots.$$

Thus, an enumeration can be redundant, i.e., fail to be 1-1.

Proposition. Any enumerable set is countable.
Proof. Let $g : A \to \mathbb{N}$ be s.t. for each $a \in A$, $g(a)$ is the least element of $\{n \in \mathbb{N} \mid f(n) = a\}$. Then g is 1-1. ■

Effective Enumerability

Def 4.3.5*. A set is **effectively enumerable** iff there is an effective procedure for enumerating it.

Example. The set of even numbers is effectively enumerable. Consider the following algorithm.

1. Set $n := 0$. Go to 2.
2. Output n. Go to 3.
3. Double n. Go to 2.

Note that if a set is infinite and effectively enumerable, then an effective procedure for enumerating it never terminates.

Decidability

Def 4.3.6*. A **decision procedure** is an effective procedure for answering a yes-no question that terminates after some finite number of steps.

Def 4.3.7*. A set B of *natural numbers* is **decidable** iff there is a decision procedure for answering for any $n \in \mathbb{N}$ whether or not $n \in B$.

Def 4.3.8*. Similarly, a set E of *strings* of symbols over a countable vocabulary is **decidable** iff there is a decision procedure for answering for any string s whether or not $s \in E$.

Examples of decidable sets.

1. The set of primes.
2. The set of wffs of sentential logic.
3. The set of logical axioms for the Hilbert system for sentential logic.
4. The set of tautologies in sentential logic.

The Existence of Undecidable Sets

Consider:

- We have only countably many words in our (meta)language.
- So, there are only countably many sentences.
- And thus, there are only countably many finite lists of sentences.
- Hence, there are only countably many effective procedures.
- Therefore, there are only countably many decidable sets of natural numbers.
- But there are uncountably many sets of natural numbers.
- Therefore, there exists an undecidable set of natural numbers, in fact, uncountably many.

The same holds for sets of sentences in a countable language and for theories in sentential and in 1st-order logic.

Some (Interesting) Properties of Theories

Def 4.3.9. A theory T is **consistent** iff it is not the case that for some sentence σ both $\sigma \in T$ and $\neg\sigma \in T$.

Def 4.3.10*. A theory T is **axiomatizable** iff there exists a decidable set A s.t. Cn $A = T$.

Def 4.3.11. T is **finitely axiomatizable** iff there exists a sentence σ s.t. Cn $\sigma = T$.

Def 4.3.12. T is **complete** iff for every sentence σ of the language of T either $\sigma \in T$ or $\neg\sigma \in T$.

Def 4.3.13*. T is **decidable** iff T is decidable as a set of sentences.

Some General Relations

Theorem 4.3.5*. In a countable 1st-order language, if Σ is a decidable set of sentences, then Cn Σ is effectively enumerable.

Corollary*. An axiomatizable theory is effectively enumerable.

Theorem 4.3.6*. A complete axiomatizable theory is decidable.

Theorem 4.3.7* **(Craig)**. An effectively enumerable theory is axiomatizable.

Theorem 4.3.8*. A decidable theory is effectively enumerable.

Theory of DLO without Endpoints

Example 1: Theory T of Dense Linear Orderings without Endpoints. The language of T is $\mathcal{L} = \{<\}$. We can specify T with a finite set of axioms.

1. $\forall x \forall y(x < y \supset y \not< x$ (asymmetry)
2. $\forall x \forall y \forall z((x < y \wedge y < z) \supset x, z)$ (transitivity)
3. $\forall x \forall y(x < y \vee x = y \vee y < x)$ (trichotomy)
4. $\forall x \forall y(x < y \supset \exists z(x < z \wedge z < y))$ (density)
5. $\forall x \exists y \; y < x \wedge \forall x \exists y \; x < y$ (no endpoints)

Theorem 4.3.9. T is complete and hence decidable.

Corollary. $Th\ (\mathbb{Q}, <) = T = Th\ (\mathbb{R}, <)$. Thus, no 1st-order sentence can distinguish between the strict ordering of the rationals and the strict ordering of the reals.

Theory of Infinite Structures

Example 2: Theory I of Infinite Structures. The language of the theory is $\mathcal{L}_I = \emptyset$. Let

$$\mathcal{K}_{inf} = \{\mathfrak{A} : |\mathfrak{A}| \text{ is infinite}\}.$$

Then $I = Th\ K_{inf}$.

Theorem 4.3.10. I is complete, axiomatizable (by the set $\Lambda = \{\exists^{\geq 2}, \exists^{\geq 3}, \ldots\}$), and thus decidable. But I is not finitely axiomatizable.

N.B. If we add vocabulary to the language, then I is no longer complete, but it remains axiomatizable and decidable, but not finitely axiomatizable.

Theory of Equivalence Relations

Example 3: Theory E of Equivalence Relations. Let $\mathcal{L}_E = \{R\}$, where R is a dyadic (relational) predicate and let

$$\mathcal{K}_E = \{\mathfrak{A} \mid R^{\mathfrak{A}} \text{ is an equivalence relation on } |\mathfrak{A}|\}.$$

Theorem 4.3.11. *Th* $\mathcal{K}_E$ is finitely axiomatizable, incomplete, and decidable.

Gödel's 1st Incompleteness Theorem

Earlier, we asked the question whether PA $= \mathit{Th}\ \mathfrak{N}$.

Note that $\mathit{Th}\ \mathfrak{N}$ is complete, since any sentence is either true or false in $\mathfrak{N}$, and if false, then its negation is true in $\mathfrak{N}$.

So, the question is equivalent to asking whether PA is complete.

Theorem 4.3.12 (Gödel). No axiomatic extension of PA is complete.

Corollary. $\mathit{Th}\ \mathfrak{N}$ is not axiomatizable.

Proof. If it were, it would be an axiomatic extension of PA.

Corollary. $\mathit{Th}\ \mathfrak{N}$ is undecidable.

Proof. If $\mathit{Th}\ \mathfrak{N}$ were decidable, it would axiomatize itself.

Corollary. $\mathit{Th}\ \mathfrak{N}$ is not even effectively enumerable.

Proof. If it were, then by Craig's theorem it would be axiomatizable.

On Gödel's Method of Proof

Gödel proceeded by "arithmetizing" the language of PA together with the logical vocabulary.

- Assign to each symbol s a distinct number $g(s)$.
- Assign to each sequence of symbols, e.g., $s_1 s_2 s_3 s_4$ a distinct natural number $\# s_1 s_2 s_3 s_4$ by the rule

$$\# s_1 s_2 s_3 s_4 = 2^{g(s_1)+1} \cdot 3^{g(s_2)+1} \cdot 5^{g(s_3)+1} \cdot 7^{g(s_1)+1}$$

- Find a wff that is true of only those numbers that are Gödel numbers of strings that are wffs. Also find wffs that are true of only those numbers that are Gödel numbers of sentences and of axioms, respectively.
- Assign to each sequence of wffs a "super" Gödel number by the method used for assigning Gödel numbers to strings of symbols.

Gödel's Method of Proof (cont.)

- Find a wff that is true of only those numbers which are "super" Gödel numbers of sequences of wffs that are derivations from the axioms of PA.
- Find a wff $Bew(x)$ that is true of only those numbers that are Gödel numbers of sentences provable from the axioms of PA.
- Construct a sentence σ such that the sentence $\sigma \equiv \neg Bew(\ulcorner \sigma \urcorner)$ is a theorem of PA, where $\ulcorner \sigma \urcorner$ is the numeral for the Gödel number of σ.
- Hence, σ "says" of itself that it is not provable.
- If σ were false in $\mathfrak{N}$, then σ would be provable from the axioms of PA. However, the axioms of PA are all true in $\mathfrak{N}$. So σ must be true.
- But since σ is true, it is unprovable.

Church's Theorem

Recall that the set $Th\,\mathfrak{N}$ of all arithmetic truths is undecidable.

It can also be shown that if PA is consistent, then it is undecidable.

There is also a finitely axiomatizable subtheory of PA, called **Robinson's Q**, which is also undecidable (if consistent).

The undecidability of Robinson's Q gives us an easy way of proving an otherwise more difficult result:

Theorem 4.3.13 (Church)*. The set of logical truths of $\mathcal{L}_A$ is undecidable.

Proof. Suppose that the set of logical truths of $\mathcal{L}_A$ is decidable. Let σ be a sentence that axiomatizes Robinson's Q. Then for any sentence τ we can test whether or not τ is a theorem of Q by testing whether $\sigma \supset \tau$ is a logical truth.

Lesson: Unlike sentential logic, THERE IS IN GENERAL NO DECISION PROCEDURE FOR TESTING THE VALIDITY OF ARGUMENTS.

Expressing PA is Consistent

Reconsider Gödel's method of arithmetizing syntax. In particular, recall the wff $Bew(x)$ which is true of all Gödel numbers of wffs provable from the axioms of PA.

Since this wff concerned the Gödel numbers of wffs provable from PA in particular, let's index $Bew_{PA}(x)$ so as to indicate that.

Since the sentence $0 \neq S0$ is a theorem of PA, PA is inconsistent if $0 = S0$ is also a theorem.

So $Bew_{PA}(\ulcorner 0 = S0 \urcorner)$ is true iff PA is inconsistent.

Let's let the sentence Con_{PA} abbreviate $\neg Bew_{PA}(\ulcorner 0 = S0 \urcorner)$. Hence, Con_{PA} expresses the consistency of PA.

For any theory T just as expressible as and even stronger than PA, we can go through the same type of procedure to formulate a sentence Con_T expressing the consistency of T.

Gödel's 2nd Incompleteness Theorem

Theorem 4.3.14 (Gödel). PA$\nvdash$ Con_{PA} unless PA is inconsistent. Moreover, for any theory T at least as strong as PA, $T \nvdash Con_T$ unless T is inconsistent.

Query. But don't we know that PA is consistent since $\mathfrak{N}$ is a model of PA?

$\mathfrak{N}$ is a creation of our meta-theory, Z, which is stronger than PA. And hence, by Gödel's 2nd incompleteness theorem, $Z \nvdash Con_Z$ unless Z is inconsistent.

So is Z consistent?

Is PA consistent?