Mathematical Logic 2016

Lecture 19: Logical theories

Instructor: Ashutosh Gupta

TIFR, India

Compile date: 2016-10-20

Where are we and where are we going?

We have seen

- FOL syntax and semantics
- various proof methods
- practical aspects of FOL theorem proving

We will see

- logical theories

Decidablity and Complexity

- FOL validity is undecidable
- We restrict the problem in two ways
  - Theories : limits on the space of models
  - Logics/Fragments : limits on the structure of formulas

Topic 19.1

Theories

Definabiblity of a class of models

Definition 19.1

For a set Σ of sentences in signature $\mathbf{S}$, *let* $\mathcal{M} = Mod(\Sigma)$ *be a class of models, which is defined as follows.*

$$\mathcal{M} = Mod(\Sigma) = \{m | \text{ for all } F \in \Sigma.\ m \models F\}$$

Theories

Definition 19.2

A theory $\mathcal{T}$ is a set of sentences closed under implication, i.e.,

$$\text{if } \mathcal{T} \models F \text{ then } F \in \mathcal{T}$$

Definition 19.3

For a set $\mathcal{M}$ of models for signature $\mathbf{S}$, let $Th(\mathcal{M})$ be the set of $\mathbf{S}$-sentences that are true in every model in Σ,i.e.,

$$Th(\mathcal{M}) = \{F | \text{ for all } m \in \mathcal{M}.\ m \models F\}$$

Theorem 19.1

$Th(\mathcal{M})$ is a theory

Proof.

Consider $Th(\mathcal{M}) \models F$. Therefore, F is true in every model in $\mathcal{M}$.
Therefore,$F \in Th(\mathcal{M})$. □

Consequences

Definition 19.4

For a set Σ of clauses, let $Cn(\Sigma)$ be the set of consequences of Σ, i.e.,

$$Cn(\Sigma) = Th(Mod(\Sigma)).$$

Exercise 19.1

Show for a theory $\mathcal{T}$, $\mathcal{T} = Cn(\mathcal{T})$.

Example 19.1

Let $\mathbf{S} = (\{:: /2, head/1, tail/1\}, \{atom/1\})$
Let Σ consists of

1. $\forall x, y.\ head(x :: y) \approx x$
2. $\forall x, y.\ tail(x :: y) \approx y$
3. $\forall x.\ atom(x) \vee head(x) :: tail(x) \approx x$
4. $\forall x, y.\ \neg atom(x :: y)$

$\mathcal{T}_{list} = Th(Mod(\Sigma))$ is the set of valid formulas over lists.
These formulas may not be true on non-list models.

Complete theory

Definition 19.5

A theory $\mathcal{T}$ is complete if for every sentence F, either $F \in \mathcal{T}$ or $\neg F \in \mathcal{T}$.

Exercise 19.2

If $Mod(\mathcal{T})$ is singleton then $\mathcal{T}$ is complete

Theorem 19.2

If for each $m_1, m_2 \in Mod(\mathcal{T})$ and sentence F,

$$m_1 \models F \text{ iff } m_2 \models F$$

then $\mathcal{T}$ is complete.

Proof.

If F is true in one model in $Mod(\mathcal{T})$ then F is true in all models.
Therefore, F is complete. □

Axiomatizable

Definition 19.6

A theory $\mathcal{T}$ is axiomatizable if there is a decidable set Σ s.t. $\mathcal{T} = Cn(\Sigma)$.

Definition 19.7

A theory $\mathcal{T}$ is finitely axiomatizable if there is a finite set Σ s.t. $\mathcal{T} = Cn(\Sigma)$.

Theorem 19.3

If $Cn(\Sigma)$ is finitely axiomatizable, then there is a finite $\Sigma_0 \subseteq \Sigma$ s.t. $Cn(\Sigma_0) = Cn(\Sigma)$.

Proof.

Let Σ' be a finite axiomatization of $Cn(\Sigma)$.
Therefore, $\Sigma \models \Sigma'$.
Due to compactness, there is a finite Σ_0 s.t. $\Sigma_0 \models \Sigma'$.
Therefore, $Cn(\Sigma') \subseteq Cn(\Sigma_0) \subseteq Cn(\Sigma)$.
Therefore, $Cn(\Sigma_0) = Cn(\Sigma)$. □

$\mathcal{T}$-satisfiability,validity

Definition 19.8

A formula F $\mathcal{T}$-satisfiable if there is model m s.t. $m \models \mathcal{T} \cup \{F\}$.
$\mathcal{T}$-satisfiability is usually written as $m \models_{\mathcal{T}} F$.

Definition 19.9

A formula F is $\mathcal{T}$-valid if $\mathcal{T} \models F$.
$\mathcal{T}$-validity is usually written as $\models_{\mathcal{T}} F$.

Topic 19.2

Decidability

Decidable theories

Definition 19.10

Let $\mathcal{T} = Th(Mod(\Sigma))$. $\mathcal{T}$ is decidable if there is an algorithm that, for each closed first-order formula F, can decide (in finite time) whether $F \in \mathcal{T}$ or not.

Definition 19.11 (Equivalent to 19.10)

There is an algorithm which, for every closed first-order formula F, can decide (in finite time) whether $\Sigma \Rightarrow F$ or not.

Axiomatizable vs. Decidable

We assume that theories consists of countably many symbols.

Theorem 19.4

a. An axiomatizable theory $\mathcal{T}$ is effectively enumerable.
b. A complete axiomatizable theory is decidable.

Proof.

a. Let decidable set Σ' s.t. $Cn(\Sigma') = \mathcal{T}$.
Therefore for each $F \in \mathcal{T}$, there is finite subset Σ_0 s.t. $\Sigma_0 \models F$.

We enumerate all proofs and if $\Sigma_0 \models F$ has a proof then eventually the enumeration will return true.

b. Since for each **S**-formula F, either F or $\neg F$ is in Σ.
The above enumeration will eventually generate proof for F or $\neg F$.
Therefore, complete axiomatizable theory is decidable. □

Complexity of decidability

In the previous proof, we enumerate all proofs to look for members of the theory.

However, a given theory have axioms that are structured in a way such that we can search for the proof more efficiently.

Such dedicated procedures are called decision procedures.

We often show decidability of a theory by providing a decision procedure.

(We can also show it by showing completeness, which can be shown by proving that all countable models are isomorphic and there are no finite models. We will skip this approach in this lecture).

Example decidable and undecidable theories

Example 19.2

Two arithmetics over natural numbers.

Decidable — *Presburger [3EXPTIME]*

$$\forall x \neg(x + 1 \approx 0)$$

$$\forall x \forall y(x + 1 \approx y + 1 \Rightarrow x \approx y)$$

$$F(0) \wedge (\forall x(F(x) \Rightarrow F(x + 1)) \Rightarrow \forall x F(x))$$

$$\forall x(x + 0 \approx x)$$

$$\forall x \forall y(x + (y + 1) \approx (x + y) + 1)$$

$$\forall x, y(x \cdot 0 \approx 0)$$

$$\forall(x \cdot (y + 1) \approx x \cdot y + x)$$

Peano — *Undecidable*

The third axiom is a schema.(It will be explained shortly!)

Exercise 19.3

Prove commutativity of $+$ in Presburger arithmetic.

Topic 19.3

Theory Examples

Defining theory

A theory may be expressed in two ways.

1. By giving a set Σ of axioms
2. By giving a set $\mathcal{M}$ of acceptable models

There are theories that can not be expressed by one of the above two ways.

For example,

- Number theory can only be defined using the model. There is no complete axiomatization. (Due to Gödel's incompleteness theorem)
- Set theory has no "natural model". We understand set theory via its axioms.

Theory of equality $\mathcal{T}_E$

We have treated equality as part of FOL syntax and added special proof rules for it.

We can also treat equality as yet another predicate.

We can encode the behavior of equality as the set of following axioms.

1. $\forall x.x \approx x$
2. $\forall x, y.x \approx y \Rightarrow y \approx x$
3. $\forall x, y, z.\ x \approx y \wedge y \approx z \Rightarrow x \approx z$
4. for each $f/n \in \mathbf{F}$
   $\forall x_1, .., x_n, y_1, .., y_n.\ x_1 \approx y_1 \wedge .. \wedge x_n \approx y_n \Rightarrow f(x_1, .., x_n) \approx f(y_1, .., y_n)$
5. for each $P/n \in \mathbf{R}$
   $\forall x_1, .., x_n, y_1, .., y_n.\ x_1 \approx y_1 \wedge .. \wedge x_n \approx y_n P(x_1, .., x_n) \Rightarrow P(y_1, .., y_n)$

The last two axioms are called schema, because they define a set of axioms using a pattern.

Number theory $m_{\mathbb{N}}$

Number theory has signature $\mathbf{S} = (\{0/0, s/1, +/2, \cdot/2, e/2\}, \{< /2\})$

Number theory is defined by the standard model.

We may use same symbols for both function symbols and their models.

$$m_{\mathbb{N}} = (\mathbb{N}; 0, s, +, \cdot, e, <)$$

There is no axiomatization of the theory. (Due to Gödel's incompleteness)

But, we may consider a sub-theories of $m_{\mathbb{N}}$ that have axiomatization.
For example,

1. $m_s = (\mathbb{N}; 0, s)$
2. $m_< = (\mathbb{N}; 0, s, <)$
3. $m_+ = (\mathbb{N}; 0, s, +, <)$

Let us consider m_s for now.

m_s is axiomatizable

Let $\mathbf{S} = (\{0/0, s/1\}, \emptyset)$

Consider the following axiomatization Σ_s of m_s

1. $\forall x.\ s(x) \not\approx 0$
2. $\forall x, y.\ s(x) \approx s(y) \Rightarrow x \approx y$
3. $\forall x.\ x \not\approx 0 \Rightarrow \exists y.\ x \approx s(y)$
4. $\forall x.\ \underbrace{S(..S(}_{n>0} x)..) \not\approx x$

Clearly, $\mathcal{T}_s = Cn(\Sigma_s) \subseteq Th(m_s)$

Theorem 19.5

$\mathcal{T}_s = Th(m_s)$.

Proof sketch.

There is an algorithm that obtains an equivalent quantifier free formula for a given formula using axioms of Σ_s.

Proving validity of quantifier free $\mathbf{S}$-formula is simplification in proportional logic. Therefore, the equality holds. □

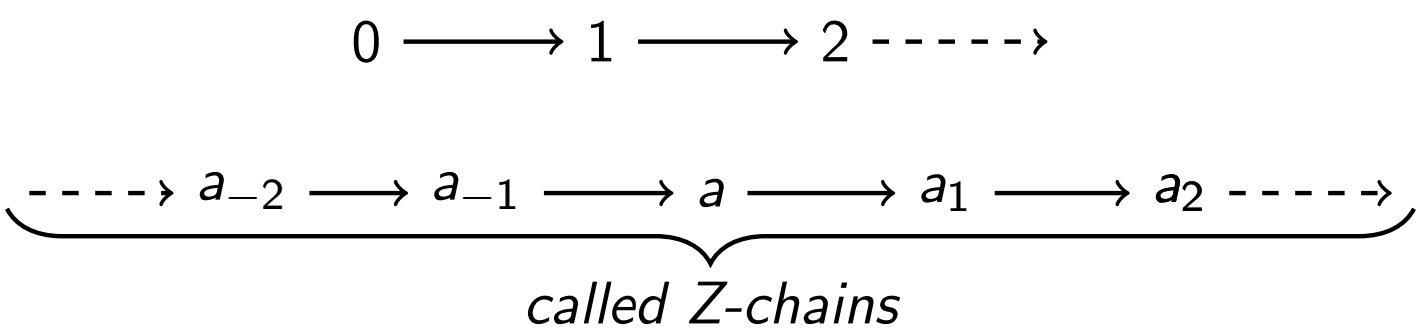
Non standard models for $\mathcal{T}_s$

The previous theorem does not say that $Mod(\mathcal{T}_s) = \{m_s\}$.

In fact, there are many models in $Mod(\mathcal{T}_s)$.

Example 19.3

Consider the following model



A model in $Mod(\mathcal{T}_s)$ may have any number of Z-chains.
There are no axioms in S-sentence that excludes Z-chains.

Exercise 19.4

Can we extend language of **S** *such that we can express exclusion of Z-chains?*

Theory of rational numbers $\mathcal{T}_{\mathbb{Q}}$

Signature $\mathbf{S} = (\{0/0, 1/1, +/2, -/1, \}, \{\geq /2\})$ (no multiplication.)

A axiomatization of $\mathcal{T}_{\mathbb{Q}}$ is

1. $\forall x, y, z.\ (x + y) + z \approx x + (y + z)$
2. $\forall x, y.\ x + y \approx y + x$
3. $\forall x.\ x + 0 \approx x$
4. $\forall x.\ x + (-x) \approx 0$
5. $1 \geq 0$
6. $1 \not\approx 0$
7. $\forall x, y.\ x \geq y \wedge y \geq x \Rightarrow x \approx y$
8. $\forall x, y, z.\ x \geq y \wedge y \geq z \Rightarrow x \approx z$
9. $\forall x, y.\ x \geq y \vee y \geq x$
10. $\forall x, y, z.\ x \geq y \Rightarrow x + z \geq y + z$
11. For every n, $\forall x, y, z.\ x = \underbrace{y + \ldots + y}_{n}$

The above theory is decidable.

Topic 19.4

Fragments/Logics

Fragments

We may restrict F syntactically to achieve decidablity or reduction in complexity.

Definition 19.12

Let $\mathcal{T} = Th(Mod(\Sigma))$ and $\mathcal{L}$ be a class of FO Σ-formulas. The class $\mathcal{L}$ for $\mathcal{T}$ is decidable if there is an algorithm that, for each closed first-order formula $F \in \mathcal{L}$, can decide (in finite time) whether $F \in \mathcal{T}$ or not.

Example 19.4 (Horn clauses and integer difference logic)

$\mathcal{L} = \{\forall x A_1(x) \wedge \cdots \wedge A_n(x) \Rightarrow B(x) | A_i \text{ and } B \text{ are atomic}\}$

Example 19.5 (Horn clauses and integer difference logic)

$\mathcal{L}$ = linear arithmetic formulas that contain atoms with only two variables and with opposite signs [quadratic complexity].

Quantifier free fragments

Quantifier-free fragment(QF) has free variables that are assumed to be existentially quantified.(unlike FOL clauses!!)

Often, the quantifier free fragment of theories have efficient decision procedures.

Example 19.6

The following is a QF formula in the theory of equality

$$f(x) \approx y \wedge (x \approx g(a, z) \vee h(x) \approx g(b))$$

QF of $\mathcal{T}$ of equality has an efficient decision procedure.
Otherwise, the theory is undecidable.

Example of logics

- theory of equality and uninterpreted function symbols (QF_EUF)
- theory of linear rational arithmetic (QF_LRA)
- theory of uninterpreted function and linear integer arithmetic (QF_UFLIA)

Topic 19.5

SMTLIB

Visit SMTLIB

http://smtlib.cs.uiowa.edu/

Topic 19.6

Problems

Axioms for predicates

Exercise 19.5

a. Write axioms for odd numbers in first order logic

b. Write axioms for even numbers in first order logic

c. Write axioms for divisibility in first order logic

d. Using the axioms write a resolution proof for the following statement

Between any two prime numbers greater than 2, there is an even number.

End of Lecture 19