Logical Theories

Ashutosh Gupta

TIFR, India

Compile date: 2016-12-06

What is theory?

Theory

"Theory is a contemplative and rational type abstract ... thinking, or .... ."

- Wikipedia

Example 1.1

Scientific and economic theories

- *Newton's theory of Gravity*
- *Theory of evolution*
- *Theory of marginal utility*

Conspiracy theories

Example 1.2

- *9/11 is an inside job*
- *Trump is a Russian mole*
- $N + L = J$

They may sound silly.

However, they are still theories.

FOL has no knowledge

First-order logic(FOL) provides a grammar for rational abstract thinking.

However, FOL carries no knowledge of any subject matter.

It was not obvious. 16th century philosopher René Descartes tried to prove

$$\text{Inherent structure of logic} \Rightarrow \text{God exists.}$$

Theory crafting needs something more than logic

$$\text{Theory} = \text{Subject knowledge} + \text{FOL}$$

Now we will formally define theories in logic.

Topic 1.1

Theories

Defining theories

The subject knowledge can be expressed in the following two ways

- the set of acceptable models
- the set of valid sentences in the subject

Example 1.3

Model m with $D_m = \mathbb{N}$ is the only model we consider for the theory of natural numbers.

We can also define the theory using the set of valid sentences over natural numbers. e.g. $\forall x.\ x + 1 \not\approx 0$.

$\approx$ is equality within the logical syntax.

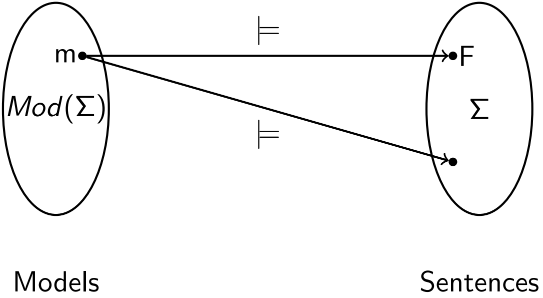
Now let us define this formally.

Definabiblity of a set of models

Definition 1.1

For a set Σ of sentences in signature **S**, *let* $Mod(\Sigma)$ *be a set of models such that*

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



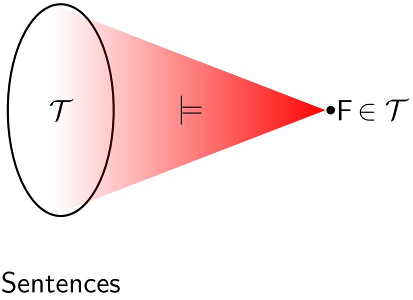
Theories

Definition 1.2

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

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

Abuse of notation, $\models$ is also used for implication

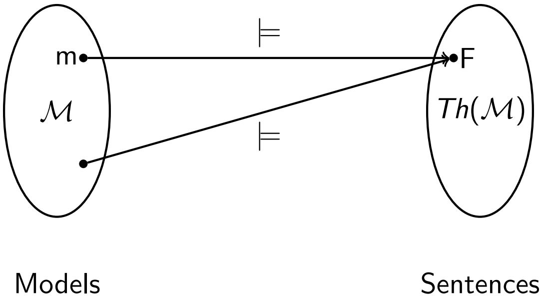


Theory of Models

Definition 1.3

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

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



Theory and models

Theorem 1.1

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

Proof.

Consider F such that $Th(\mathcal{M}) \models F$.

Therefore, F is true in every model in $\mathcal{M}$.

Therefore, $F \in Th(\mathcal{M})$.

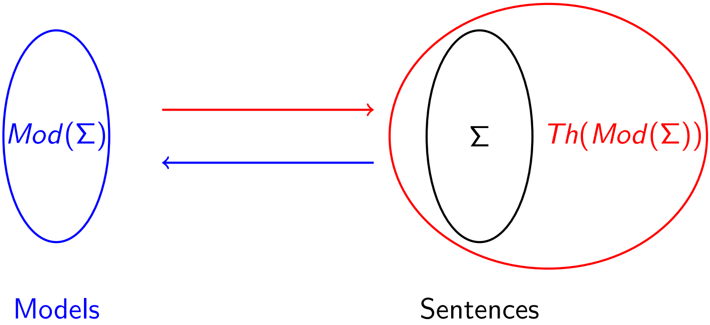
$Th(\mathcal{M})$ is closed under implication. □

Consequences

Definition 1.4

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

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



Exercise 1.1

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

Example: theory of lists

Example 1.4

Let us suppose our subject of interest is lists.

First we need to fix our signature.

We should be interested in the following functions and predicates

- :: - *constructor for extending a list*
- *head - function to pick head of a list*
- *tail - function to pick tail of a list*
- *atom - predicate that checks if something is constructed using* :: *or not*

The signature is

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

Example: theory of lists

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 sentences over lists.

The sentences in $\mathcal{T}_{list}$ may not be true on the non-list models.

Exercise 1.2

Why empty list is not explicitly encoded?

Complete theory

Definition 1.5

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

Exercise 1.3

When a theory is not complete?

Exercise 1.4

Can a theory have both F and $\neg F$ for some sentence F?

Exercise 1.5

Prove: if $Mod(\mathcal{T})$ is singleton then $\mathcal{T}$ is complete.

A condition for complete theory

Theorem 1.2

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

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

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. □

No sentence can distinguish models of $\mathcal{T}$.

Axiomatizable

Definition 1.6

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

Definition 1.7

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

Theorem 1.3

If $Cn(\Sigma)$ is finitely axiomatizable, there is a finite $\Sigma' \subseteq \Sigma$ s.t. $Cn(\Sigma') = Cn(\Sigma)$

Proof.

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

$\mathcal{T}$-satisfiability,validity

Definition 1.8

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 1.9

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

Topic 1.2

Decidability

Decidable theories

Definition 1.10

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

Definition 1.11 (Equivalent to 1.10)

There is an algorithm that, for each sentence 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 1.4

An axiomatizable theory $\mathcal{T}$ is effectively enumerable.

Proof.

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 triples (F, Σ_0, Pr) such that

- $F \in$ **S**-sentences,
- finite $\Sigma_0 \subseteq \Sigma'$, and
- Pr is a FO-proof (sequence of formulas with consequence relation).

Since the three sets are enumerable, the triple is also enumerable. If Pr is proof of $\Sigma_0 \models F$, we report F. Therefore, $\mathcal{T}$ is effectively enumerable. □

Axiomatizable vs. Decidable

Theorem 1.5

A complete axiomatizable theory is decidable.

Proof.

Since for each **S**-formula F, either F or $\neg F$ is in Σ.

The previous enumeration will eventually generate proof for F or $\neg F$.

Therefore, complete axiomatizable theory is decidable. □

Decidability via completeness

We can show decidability of a theory via completeness.

We may show completeness as follows.

- there are no finite models
- all countable models are isomorphic (No sentence can distinguish them)

In the previous proof, we enumerate all proofs to look for the members of $\mathcal{T}$.

The method does not tell us about the hardness of the decision problem.

So, we will skip this approach in this lecture.

Complexity of decidability

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.

Example decidable and undecidable theories

Example 1.5

Two arithmetics over natural numbers.

Decidable — Presburger [3EXPTIME]:

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

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

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

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

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

Undecidable — Peano (all of the above, plus):

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

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

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

Topic 1.3

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.

Example: 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.

Topic 1.4

Number theory

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 1.6

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

Proof sketch.

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

Proving the validity of quantifier free **S**-sentence is simplification in proportional logic. Therefore, the equality holds. □

Quantifer elimination in $\mathcal{T}_s$

Algorithm 1.1: Q_ELEM($\exists x.\ell_1 \wedge .. \wedge \ell_k$)

Input: ℓ_i is a literal (atom or its negation) and x occurs in ℓ_i
Output: an equivalent quantifier-free formula

if $\exists i.\ \ell_i = (s^n(x) \approx s^m(x))$ *for* $m \neq n$ *or* $\ell_i = (s^n(x) \not\approx s^n(x))$ **then**
    return $\bot$;
if $\exists i.\ \ell_i = (s^n(x) \approx s^m(u))$ *for* $u \neq x$ **then**
    // $\bowtie \in \{\approx, \not\approx\}$;
    for $\ell_j = (s^p(x) \bowtie s^q(u'))$ **do**
        $\ell'_j := (s^{m+p}(u) \bowtie s^{q+n}(u'))$
    return $s^m(u) \not\approx s^0(0) \wedge .. \wedge s^m(u) \not\approx s^{n-1}(0) \wedge \ell'_1 \wedge ... \wedge \ell'_k$;
else
    return $\top$;

Example: Quantifer elimination in $\mathcal{T}_s$

Example 1.6

Consider $\exists x.\ s(y) \approx s(s(x)) \wedge s(x) \approx z$

Let us choose $s(y) \approx s(s(x))$ *atom for substitution.*

$s(y)$ *has to be greater than 1. We need to add:* $s(y) \not\approx 0 \wedge s(y) \not\approx s(0)$.

After the substitution, the first term will be trivially true.

Let us apply the substitution on the second atom.

- $s(x) \approx z$
- $s(s(s(x))) \approx s(s(z))$ *// add enough s*
- $s(y) \approx s(s(z))$ *// apply substitution*

Final output: $s(y) \not\approx 0 \wedge s(y) \not\approx s(0) \wedge s(y) \approx s(s(z))$

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 1.7

Consider the following model

$$0 \longrightarrow 1 \longrightarrow 2 \dashrightarrow$$

$$\underbrace{\dashrightarrow a_{-2} \longrightarrow a_{-1} \longrightarrow a \longrightarrow a_1 \longrightarrow a_2 \dashrightarrow}_{\text{called Z-chains}}$$

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 1.6

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

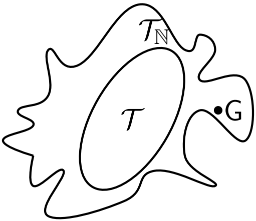
Gödel's incompleteness theorem

Theorem 1.7

$m_{\mathbb{N}}$ can not be axiomatized.

Proof structure.

1. Choose a set A_D of valid sentences in $m_{\mathbb{N}}$ s.t. that $\mathcal{T}_D = Cn(A_D)$ can encode the proofs in any subtheory of $m_{\mathbb{N}}$
2. This allows us to construct a sentence G for a theory $\mathcal{T}$ of any given axiomatization such that $m_{\mathbb{N}} \models G$ but $G \notin \mathcal{T}$.
3. Therefore, no axiomatization of $m_{\mathbb{N}}$ □



Exercise 1.7

What if we add G as an axiom in $\mathcal{T}$?

Topic 1.5

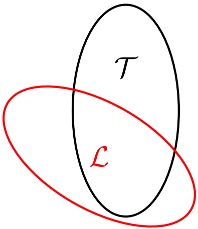
Fragments/Logics

Fragments

We may restrict F syntactically to achieve decidablity or low complexity.

Definition 1.12

Let $\mathcal{T}$ be a theory and $\mathcal{L}$ be a set of **S***-sentences. $\mathcal{L}$ wrt $\mathcal{T}$ is decidable if there is an algorithm that takes $\mathsf{F} \in \mathcal{L}$ as input and returns if $\mathsf{F} \in \mathcal{T}$ or not.*



Sentences

Example : fragments

Example 1.8 (Horn clauses)

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

Example 1.9 (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(QF) fragment has free variables that are assumed to be existentially quantified.(unlike FOL clauses!!)

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

Example 1.10

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

Some times the fragments are also referred as logics.

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