Mathematical Logic 2016

Lecture 1: Introduction and background

Instructor: Ashutosh Gupta

TIFR, India

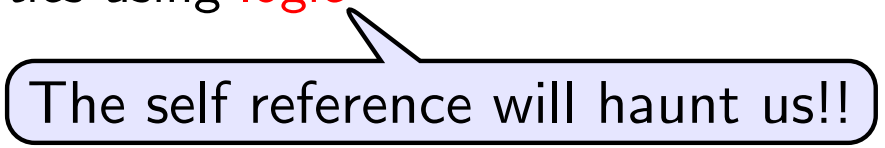
Compile date: 2016-08-06

Topic 1.1

What is logic?

What is logic?

- Have you ever said to someone "be logical"?
  - whatever your intuition was that is logic
- Mathematization/Formalization of the intuition is mathematical logic
- Two streams of studying logic
  - use of logic : logic as a tool to study something else, e. g., math
  - properties of logic: since logic has mathematical structure, we may study its mathematical properties using logic



Why study logic?

Differential equations
are the calculus of
Electrical engineering

Logic
is the calculus of
Computer science

Logic provides tools to define/manipulate computational objects

Defining logic

Logic is about inferring conclusions from given premises

Example 1.1

1. *Humans are mortal*
2. *Socrates is a human*

Socrates is mortal ✓

1. *Apostles are twelve*
2. *Peter is an apostle*

Peter is twelve ✗

What went wrong here?

Intuitive Pattern:

1. α*s are* β
2. γ *is an* α

γ *is* β

where α *and* γ *are noun and* β *is adjective*

Very easy to ill-define.
Logic needs rigorous definitions!!

Commentary: Clearly understood formalization only arrived in early 20th century. The above was one of the mistakes in the Aristotle's syllogism(inference rules), which dominated European thought until late middle ages.

Topic 1.2

Course logistics and contents

Evaluation and website

- Assignments : 40%, 4% each (strict deadlines!)
- Midterm : 20% (1 hour)
- Presentation: 10% (15 min)
- Final: 30% (1.5 hour)

For the further information

`http://www.tcs.tifr.res.in/~agupta/courses/2016-logic`

All the assignments and slides will be posted on the website.

Please read the conditions to attend the course. They are on the website.

The course

We will study the following topics

- Propositional logic
- First order logic
- Logical theories
- Incompleteness results

Propositional logic (PL)

Propositional logic

- deals with propositions,
- only infers from the structure over the propositions, and
- does not look inside the propositions.

Example 1.2

Is the following argument valid?
If the seed catalog is correct then if seeds are planted in April then the flowers bloom in July. The flowers do not bloom in July. Therefore, if seeds are planted in April then the seed catalog is not correct.

Let us symbolize our problem
If c then if s then f. not f. Therefore, if s then not c.

- c = *the seed catalogue is correct*
- s = *seeds are planted in April*
- f = *the flowers bloom in July*

PL reasons over propositional symbols and logical connectives

PL topics

We will study

- definition of PL and syntactic properties
- Proof systems for PL and their soundness, completeness, and complexity
- Low complexity subclasses
- PL solvers *aka* SAT solvers

Commentary: PL has limited expressive power. However, there are a lot of real world problems that can be *encoded* using PL. SAT solver is an effective tool to solve the problems.

First order logic (FOL)

First order logic

- looks inside the propositions,
- much more expressive,
- deals with parameterized propositions, and quantifiers, and
- can express lots of interesting math.

Example 1.3

Is the following argument valid?
Humans are mortal. Socrates is a human. Therefore, Socrates is mortal.

In the symbolic form,
For all x if $H(x)$ then $M(x)$. $H(s)$. Therefore, $M(s)$.

- $H(x) = x$ *is a human*
- $M(x) = x$ *is mortal*
- $s =$ *Socrates*

FOL is not the most general logic.
Many arguments can not be expressed in FOL

FOL topics

We will study

- definition of FOL and syntactic properties
- proof systems for FOL and their soundness, completeness, etc
- first order theorem provers

Logical theories

In a theory, we study validity of FOL arguments under some specialized assumptions (called axioms).

Example 1.4

The number theory uses symbols $0, 1, .., <, +, \cdot$ *with specialized meanings*

The following sentence has no sense until we assign the meanings to $>$ *and* $\cdot$

$$\forall x\ \exists p.\ (p > x \wedge (\forall v_1.\ (v_1 > 1 \Rightarrow \forall v_2.\ p \neq v_1 \cdot v_2)))$$

Under the meanings *it says that there are arbitrarily large prime numbers.*

In the earlier example, we had no interpretation of predicate 'x is human'. Here we precisely know what is predicate '$x < y$'.

Commentary: The specialized meaning are defined using axioms. For example, the sentence $\forall x.\ 0 + x = x$ describes one of the properties of 0 and $+$. We will cover number theory at length.

Logical theories II

The logical theories are useful in studying specialized domains.

Logic was thought to be an immensely useful general purpose tool in studying properties of various mathematical domains.

Incompleteness results

But sadly, one can prove that

Theorem 1.1 (Gödel's incompleteness(1930))

There are theories whose assumptions can not be listed.

Proof sketch.

The proof proceeds by showing that if there is such a list for the number theory then the list can prove a theorem that "the list cannot prove the theorem". Contradiction. □

The incompleteness was an epic failure of logic as a tool to do math.

From the ashes of logic,
rose computer science

Commentary: The incompleteness essentially shows that some of our mathematical intuitions cannot be formally characterized.

Topic 1.3

Basic objects : Tuples, Sets, Vectors, Functions, and Relations

How to read the slides?

- (why?) indicates a gap in a proof. It is left for the reader to fill.
- Please solve the exercises in the slides before visiting the later slides, which assume that the solution is fresh in the mind of reader.
- The highlighted term in a definition is being defined

  Definition 1.1
  This is a definition of defined term.

- To avoid too many definitions, terms may be defined as follows.

$$\textit{defined} \triangleq \textit{definition}$$

Tuples

A tuple is a finite ordered list of elements. e.g., $(a_1, \ldots, a_n)$ is an n-tuple.

Typical usage,

- immutable
- access entries by assigning distinct names or by ith-component
- used to represent objects that are built using a known small finite number of components. e.g., automata, etc.
- In particular, (a, b) denotes a pair, (a, b, c) denotes a triple

Sets

- A set is a collection of things. *e. g.*, $S = \{a, b, c\}$
- $a \in S$ denotes a is an element of set S
- $d \notin S$ denotes d is not an element of set S
- $\emptyset$ denotes a set without any element (Note: $\emptyset \neq \{\emptyset\}$)
- $\{x|P(x)\}$ denotes the set of elements that satisfy the predicate P
- $A \subseteq B$ denotes B contains all the elements of A.
- $A \subset B$ denotes $B \subseteq A$ and $B \neq A$.
- $\mathfrak{p}(A) \triangleq \{B|B \subseteq A\}$
- $|A|$ denotes cardinality (or size) of A.

Exercise 1.1

- $\{f(x)|P(x)\} = \{y|$*there is x such that* $y = f(x)$ *and* $P(x)\}$
- $\{x \in D|P(x)\} =?$
- $\{x\} \cup \{f(x, y)|P(x, y)\} =?$
- $\{3|3 < 0\} =?$

Some special sets

- $\mathcal{B}$ - set of Boolean values
- $\mathbb{N}$ - set of natural numbers
- $\mathbb{Z}$ - set of integers
- $\mathbb{Q}$ - set of rational numbers
- $\mathbb{R}$ - set of real numbers

Set operations

- $A \cup B \triangleq \{x | x \in A \text{ or } x \in B\}$
- $A \cap B \triangleq \{x | x \in A \text{ and } x \in B\}$
- $A \setminus B \triangleq \{x | x \in A \text{ and } x \notin B\}$
- $\cup$ and $\cap$ are reflexive, symmetric, and transitive
- $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$, $A \cup A = A$, and $A \cap A = A$
- $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$, and $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
- For some set U (known as universal set), $\bar{A} \triangleq U \setminus A$
- $\overline{(A \cup B)} = (\bar{A} \cap \bar{B})$ and $\overline{(A \cap B)} = (\bar{A} \cup \bar{B})$
- $\overline{A} \cup A = U$ and $\overline{A} \cap A = \emptyset$
- For $n > 1$, and sets $A_1, \ldots, A_n$,

$$A_1 \times \cdots \times A_n \triangleq \{(a_1, \ldots, a_n) | \text{for each } i \in 1..n,\ a_i \in A_i\}$$

More set notations

- Let S be a set of sets,

$$\bigcup S \triangleq \{x| \text{ there is } A \text{ s.t. } x \in A \text{ and } A \in S\}^*$$

- Let S be a function from $\mathbb{N}$ to sets and J is a subset of $\mathbb{N}$,

$$\bigcup_{i \in J} S(i) \triangleq \bigcup \{S(i)|i \in J\}$$

- Analogous notations for $\bigcap$

*s.t. stands for "such that"

Relations

- A relation R between A and B is $R \subseteq A \times B$
- $\Delta_A \triangleq \{(x,x)|x \in A\}$ and $R^{-1} \triangleq \{(y,x)|(x,y) \in R\}$
- $R \circ S \triangleq \{(x,z)|$ there is a y s.t. $(x,y) \in R$ and $(y,z) \in S\}$
- $dom(R) \triangleq \{x|(x,y) \in R\}$ and $range(R) \triangleq \{y|(x,y) \in R\}$
- For $R \subseteq A \times A$, (A,R) is often viewed as a directed graph

Transtive closure

Let $R \subseteq A \times A$

- $R^0 \triangleq \Delta_A$ and $R^{n+1} \triangleq R \circ R^n$
- Transitive closure $R^* \triangleq \bigcup_{n \geq 0} R^n$

Theorem 1.2

R^* is the least relation S that satisfies

$$\Delta_A \cup (R \circ S) \subseteq S$$

- In other words, R^* is least fixed point(lfp) of $f(S) \triangleq \Delta_A \cup (R \circ S)$
- Let $R^+ \triangleq \bigcup_{n > 0} R^n$

Exercise 1.2

R^+ is lfp of _____ ? Is the lfp unique ?

Some equivalences

1. $(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$
2. $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$
3. $(R_1 \cup R_2) \circ R_3 = (R_1 \circ R_2) \cup (R_2 \circ R_3)$
4. $R^{*-1} = R^{-1*}$

Exercise 1.3

Prove the above equivalences

Equivalence Relation

Definition 1.2

$E \subseteq A \times A$ *is an equivalence relation if*

- *reflexive:* $\Delta_A \subseteq E$
- *symmetric:* $E = E^{-1}$
- *transitive:* $E \circ E \subseteq E$

For $x \in A$,

$$[x] \triangleq \{y | (x, y) \in E\}.$$

E defines a collection of sets that are partitions of A.

$$A_{/E} \triangleq \{[x] | x \in A\}$$

Partial Orders

Definition 1.3

$\leq \subseteq A \times A$ *is a* *partial order* *if*

- *reflexive:* $\Delta_A \subseteq \leq$
- *anti-symmetric:* $\leq \cap \leq^{-1} \subseteq \Delta_A$
- *transitive:* $\leq \circ \leq \subseteq \leq$

Definition 1.4

A partial order $\leq$ *is* *total* *if for all* $x, y \in A$ *either* $x \leq y$ *or* $y \leq x$.

Definition 1.5

A partial order $\leq$ *is* *well-founded* *if for all* $S \subseteq A$ *there is a* $x \in S$ *s.t. for each* $y \in S$, $y \not\leq x$.

Preorders

Definition 1.6

$\lesssim \subseteq A \times A$ *is a preorder if*

- *reflexive:* $\Delta_A \subseteq \lesssim$
- *transitive:* $\lesssim \circ \lesssim \subseteq \lesssim$

Exercise 1.4

Let $A_{/\lesssim} \triangleq \{\{y | x \lesssim y \text{ and } y \lesssim x\} | x \in A\}$.
Show $\{(S, S') \in A_{/\lesssim} \times A_{/\lesssim} |$ *there are* $x \in S, y \in S'$ *s.t.* $x \lesssim y\}$ *is a partial order.*

Functions

Definition 1.7

$f \subseteq A \times B$ *is a* *function* *if*

- $dom(f) = A$, *and*
- *for each* x, y, *and* z, *if* $(x, y) \in f$ *and* $(x, z) \in f$ *then* $y = z$.

Let $A \to B$ denote the set of all the functions from A to B,
and $f : A \to B$ denote that f is in $A \to B$.

Function update:
$f[x \mapsto y]$ creates a new function, which is defined as follows.

$$f[x \mapsto y](z) \triangleq \begin{cases} y & \text{if } z = x \\ f(z) & \text{if } \textit{otherwise}. \end{cases}$$

Functions(contd.)

Definition 1.8

For set $A' \subseteq A$,
let $f|_{A'}$ denote a function in $A' \to B$ s.t. for each $x \in A'$, $f|_{A'}(x) = f(x)$.

Definition 1.9

$f : A \to B$ is one-to-one if for each x and y in A, if $x \neq y$ then $f(x) \neq f(y)$.

Definition 1.10

$f : A \to B$ is onto if for each $x \in B$ there is a $y \in A$ such that $x = f(y)$.

Partial function

Definition 1.11

$f \subseteq A \times B$ *is a* *partial function* *if*

- ~~$dom(f) = A$, and~~
- *for each* $x, y,$ *and* $z,$ *if* $(x, y) \in f$ *and* $(x, z) \in f$ *then* $y = z.$

Let $A \hookrightarrow B$ denote the set of all partial functions from A to B, and $f : A \hookrightarrow B$ denote that f is in $A \hookrightarrow B$.

Relations as functions

Let $R \subseteq A \times B$, we can view R as a function of type $A \to \mathfrak{p}(B)$.

$$R(a) \triangleq \{b | (a, b) \in R\}$$

We can also view R as a function of type $\mathfrak{p}(A) \to \mathfrak{p}(B)$.

$$R(S) \triangleq \bigcup \{R(a) | a \in S\}$$

We will use the above notations interchangeably.

Anonymous functions

Sometimes functions are nameless and only expressed by their body.

Such functions are written as follows

$$\lambda < \text{parameters} > . < \text{function body} >$$

Example 1.5

- $\lambda x.\ x$
- $\lambda x.\ x + 1$
- $\lambda x, y.\ x + y$

Strings or Sequences

Let **Symbs** be a set of symbols.

For $s_i \in$ **Symbs**, $s_1 \dots s_n$ be a finite string/word/sequence of symbols from **Symbs**

Let **Symbs*** be the set of finite strings from **Symbs**

Let ϵ denote the empty string

For $v \in$ **Symbs*** and $w \in$ **Symbs***, let vw denote the concatenation of v and w

We say u is a prefix of w if $uv = w$ for some v.

We say u is a proper prefix of w if $uv = w$ for some non-empty v.

Other collecting objects

Here are a few more mathematical objects that are collection of things.

- Stacks
- Vectors
- Multisets

Please familiarize yourself with the concepts!

Collecting data structures

For describing/implementing various algorithms, we may need data structures that represent collections of things with different level of functionalities.

- Arrays
- Lists
- Bags
- Maps
- Unordered maps
- ... many more ...

Due to limited time, we will not discuss them in detail.
Please refer to the standard texts!

Homomorphism

We call two sets isomorphic if we can demonstrate that there is a transformation from one to another preserving the key properties of interest.

Consider two sets A and B. Let the properties of interest are

$$P_A \subseteq \underbrace{A \times \cdots \times A}_{n} \text{ and } P_B \subseteq \underbrace{B \times \cdots \times B}_{n}.$$

Definition 1.12

A function $h : A \to B$ is a homomorphism w.r.t. properties P_A and P_B if

$$(a_1, \ldots, a_n) \in P_A \quad \textit{iff} \quad (h(a_1), \ldots, h(a_n)) \in P_B$$

Isomorphism/isomorphic

Definition 1.13

If h is one-to-one then it is called an isomorphism.
If h is also onto then A and B are considered isomorphic.

Exercise 1.5

Prove $A \to (B \to C)$ is isomorphic to $A \times B \to C$.
Hint: define the properties of interest.

Topic 1.4

Induction principle

Induction

Let us suppose we need to prove $\forall x \in A : G(x)$.

We can invoke induction principle

$$F(0) \wedge \forall n.\ (F(n) \Rightarrow F(n+1)) \quad \Rightarrow \quad \forall x \in \mathbb{N}.\ F(x)$$

Identify suitable F and onto function $f : \mathbb{N} \to A$ s.t. $\forall i \in \mathbb{N} : F(i) \Rightarrow G(f(i))$

- Prove $F(0)$
- Prove $\forall n.\ (F(n) \Rightarrow F(n+1))$
  Assume $F(n)$ and prove $F(n+1)$.
- And, we are done.

Induction problems

Exercise 1.6

Prove: If there is a human with an ancestor that is a monkey, then there is a human with a parent that is a monkey.

Exercise 1.7

Show that the following induction proof is flawed.

claim: *All horses have same color*

base case:

One horse has single color

induction step:

We assume that n horses has same colors

Take $n+1$ *horses* $h_1, .., h_{n+1}$,

$h_1, .., h_n$ *has same color (hyp.)*

$h_2, .., h_{n+1}$ *has same color (hyp.)*

Therefore, $h_1, .., h_{n+1}$ *has same color.*

Topic 1.5

Graphs

Graph

Definition 1.14

A graph is a pair $G = (V, E)$ consists of a set of nodes V and a set of edges $E \subseteq \mathfrak{p}(V)$ s.t. for each $e \in E$, $|e| = 2$.

Definition 1.15

A directed graph is a pair $G = (V, E)$ consists of a set of nodes V and a set of edges $E \subseteq V \times V$.

For $V' \subseteq V$, let $G|_{V'}$ denote the graph by removing the nodes and edges from G that do not concern with the nodes in V'.

Köing's Lemma

Theorem 1.3

For an infinite connected graph G, if degree of each node is finite then there is an infinite simple path in G from each node.

Proof.

We construct an infinite simple path $v_1, v_2, v_3, ...$ as follows.

base case:

Choose any $v_1 \in G$.Let $G_1 \triangleq G$.

induction step:

1. Assume we have a path $v_1, ..., v_i$ and an infinite connected graph G_i s.t. $v_i \in G_i$ and $v_1..v_{i-1} \notin G_i$.
2. In G_i, there is a neighbour $v_{i+1} \in G_i$ of v_i s.t. infinite nodes are reachable from v_{i+1} without visiting v_i.(why?)
3. Let S be the reachable nodes. Let $G_{i+1} \triangleq G_i|_S$. □

Exercise 1.8

Prove that any finitely-branching infinite tree must have an infinite branch.

Topic 1.6

Cardinality

Comparing sizes of sets

Cardinality is a measure of the number of elements of the set, which is denoted by $|A|$ for set A. Non-trivial to understand if $|A|$ is not finite.

Definition 1.16

$|A| \leq |B|$ *if there is an one-to-one* $f : A \to B$.

Theorem 1.4

If f *is also onto then* $|A| = |B|$.

Exercise 1.9

Prove theorem 1.4

Countable/uncountable

Definition 1.17

A is countable if $|A| \leq |\mathbb{N}|$.

Definition 1.18

A is uncountable if $|A| > |\mathbb{N}|$

Exercise 1.10

Show $\mathbb{Q}$ *is countable.*

Countable finite words

How to prove?
Find an one-to-one map to $\mathbb{N}$

Theorem 1.5

If **Symbs** *is countable,* **Symbs*** *is countable.*

Proof.

Since **Symbs** is countable there exists one-to-one f : **Symbs** $\to \mathbb{N}$.
We need to find an one-to-one h : **Symbs*** $\to \mathbb{N}$.

Let p_i be the ith prime. Our choice of h is

$$h(a_1 \dots a_n) = \Pi_{i \in 1..n} p_i^{f(a_i)}.$$

□

Exercise 1.11

Show h is one-to-one.

Cantor's theorem

Theorem 1.6

$|A| < |\mathfrak{p}(A)|$

Proof.

Consider function $h(a) = \{a\}$. h is one-to-one function.
There is an one-to-one function in $A \to \mathfrak{p}(A)$, therefore $|A| \leq |\mathfrak{p}(A)|$.

To show strictness, we need to show that there is no one-to-one and onto function in $A \to \mathfrak{p}(A)$.

Let us suppose $f : A \to \mathfrak{p}(A)$ is one-to-one and onto.
Consider, $S \triangleq \{a | a \notin f(a)\}$. Since f is onto, there is a b s.t. $f(b) = S$.
Case $b \in S$: Since $f(b) = S$, $b \in f(b)$. Due to def. S, $b \notin S$. Contradiction.
Case $b \notin S$: Since $f(b) = S$, $b \notin f(b)$. Due to def. S, $b \in S$. Contradiction.

□

Exercise 1.12

For countable A, why is A^* lot smaller than $\mathfrak{p}(A)$? Give an intuitive answer.

Topic 1.7

Problems

Does God exists?

Exercise 1.13

Is there a logical problem with the following argument aka *Ontological argument?*

1. *God is the greatest possible being that can be imagined.*
2. *God exists as an idea in the mind.*
3. *A being that exists as an idea in the mind and in reality is, other things being equal, greater than a being that exists only as an idea in the mind.*
4. *Thus, if God exists only as an idea in the mind, then we can imagine something that is greater than God.*
5. *But we cannot imagine something that is greater than God.*
6. *Therefore, God exists.*

(text source Wikipedia)
Fun side of the argument: `https://xkcd.com/1505/`

A puzzle that melt the internet!!

Exercise 1.14

Sanjay and Salman are new friends with Madhuri, and they want to know her birthday. Madhuri gives them a list of possible dates.
March 14, March 15, March 18,
April 16, April 17,
May 13, May 15,
June 13, June 14, June 16

Madhuri then tells Sanjay and Salman separately the month and the day of her birthday respectively.

Sanjay: I don't know the date, but I know that Salman doesn't know too.
Salman: At first I didn't know the date, but I know now.
Sanjay: Then I also know the date.

So when is Madhuri's birthday?

One-to-one and onto

Exercise 1.15

Prove or disprove:

For sets A and B, if there exist one-to-one functions $f : A \to B$ and $g : B \to A$, then there exists a one-to-one and onto function in $A \to B$.

Combinatorics

Exercise 1.16

For $i \in 0..m$, consider $R_i = \{h_{i1}, \ldots, h_{i5}\}$, where $h_{ij} \in 1..m$. How many ways to choose R_is such that for some $P' \subseteq 0..m$ of size t the following holds?

$$|\{j | \textit{unique } i \in P' \textit{ s.t. } j \in R_i\}| < |P'|$$

Note that it is possible that $|R_i| < 5$.

End of Lecture 1