Sept. 10. 2013.

Lecture #2

Definition :

Notation .

Modern Logic.

Object Language (Formalizable)	...	Metalanguage (Semi-formalizable)
Proof Theory (Syntax)	...	Model Theory . (Semantics)
Algorithms / Complexity (SAT Solver/ Theorem prover)	...	Applications . (Model Checker)

We will explore the connections between these two aspects of logic.

Sets. Collection of elements.
A fundamental object of mathematics.

Set operations: union $\cup$
intersection $\cap$
complement $\setminus$

$\mathbb{N}$ = Set of natural numbers (Convention: include 0).
$\{0, 1, 2, 3, \dots\}$

$\mathbb{Z}$ = Set of integers.

$\mathbb{Q}$ = Set of rational numbers.

$\mathbb{A}$ = Set of algebraic numbers.

$\mathbb{R}$ = Set of real numbers.

$\mathbb{N}_+$, $\mathbb{Z}_+$, $\mathbb{Q}_+$, $\mathbb{A}_+$, $\mathbb{R}_+$ $\Big\{$ Set of positive numbers of the corresponding sets.

$n, m, i, j, k \rightarrow$ Variables ranging over $\mathbb{N}$.

M, N = Sets

$M \subseteq N$ inclusion
$M \subset N$ proper inclusion
$M \setminus N$ set difference
(when M is fixed, write $\sim N$ or $\neg N$)
$M \times N$ Cartesian product.
ϕ = Empty set
$\mathcal{P}M = \{S \mid S \subseteq M\}$ = Set of all subsets of M
= Power set of M.

Relation.

A <u>relation</u> between M and N is a subset of $M \times N$ (Cartesian product of M and N)

$$M \times N = \{ (a,b) \mid a \in M, b \in N \}$$

↳ ordered pairs.

$$R \subseteq M \times N = \text{Binary Relation.}$$

$$\forall_{a \in M, b \in N} \quad aRb \text{ iff } (a,b) \in R.$$

Function

A <u>function</u> (or <u>mapping</u>) from M to N is a relation

$$f \subseteq M \times N$$

if for each $a \in M$ there is possibly one $b \in N$ with $(a,b) \in f$.

$$\forall_{a \in M} \quad |\{ b \mid (a,b) \in f \}| \leq 1.$$

$b \equiv f(a)$ = value of f at a.

$$f : M \to N$$
$$: a \mapsto f(a)$$

$\text{dom } f \equiv M$ = Domain of f

$\text{ran } f \equiv \{ f(x) : x \in M \} \subseteq N$

= Range of f

$$\mathrm{id}_M : M \to M \qquad \text{identity function on } M.$$
$$: x \mapsto x$$

$f : M \to N$

Injective (ONE-TO-ONE) if $\forall x, y \in M$ $f(x) = f(y) \Rightarrow x = y$ ~~$\forall x, y \in M$~~.

Surjective (ONTO) if $\forall y \in N \; \exists x \; f(x) = y$ $(\operatorname{ran} f = N)$

Bijective (BOTH ONE-TO-ONE & ONTO) if f is both injective and surjective.

M^I = The set of all functions from the set I to M.
$= \{ f : I \to M \}$

Let f and g be two functions s.t.

$$\operatorname{ran} g \subseteq \operatorname{dom} f$$

$$h : \operatorname{dom} g \to \operatorname{ran} f$$
$$: x \mapsto f(g(x))$$

is called their <u>composition</u> (product).

$$h \equiv f \circ g.$$

If A is an <u>alphabet</u> (i.e. if the elements $s \in A$ are <u>symbols</u> or <u>named symbols</u>) then the <u>sequence</u>

map
$f : \{1, \ldots, n\} \to A$
$: i \mapsto s_i$
index set to its range

$$(s_1, s_2, \ldots, s_n) \in A^n$$

is written as

$$s_1 s_2 \ldots s_n$$

and is called a <u>string</u> or <u>word</u> over the <u>alphabet</u> A.

$A^* =$ Set of all strings over A.

Empty string $= \phi$ (empty sequence)
Atomic string (a single symbol from the alphabet)

Let $\xi\eta$ denote concatenation of the strings $\xi \in A^*$ and $\eta \in A^*$

~~that~~ $\xi\eta \in A^*$

Let $\xi = \xi_1 \eta \xi_2 \in A^*$ for some strings ξ_1, η and ξ_2

$\eta \neq \phi \Rightarrow \eta$ is called a <u>substring</u> (or <u>segment</u>) of ξ.

$\{\eta$ is called a <u>proper substring</u> if $\xi \neq \eta\}$

$\xi_1 = \phi \Rightarrow \eta$ is called a <u>prefix</u> (or <u>initial</u>) of ξ.

$\xi_2 = \phi \Rightarrow \eta$ is called a <u>suffix</u> (or <u>final</u>) of ξ.

PREDICATE.

Subsets $P, Q, R, \dots \subseteq M^n = \underbrace{M \times M \times \cdots \times M}_{n}$

are called <u>n-ary predicate</u> of M.
(n-ary relation)

A <u>unary predicate</u> $\equiv$ subset of M

$P \equiv \phi \Rightarrow P = \perp$ (always false)
$P \equiv M \Rightarrow P = T$ (always true)

$P\vec{a} = \text{True}$ iff $\vec{a} \in P$
$\neg P\vec{a} = \text{True}$ iff $\vec{a} \notin P$ iff $P\vec{a} = \text{False}$.

An <u>n-ary operation</u> of M is a function

$$f : M^n \to M$$

Note $M^0 = \{\phi\}$ $\left.\begin{array}{l} f : M^0 \to M \\ \quad : \phi \mapsto c \end{array}\right\}$ is a 0-ary operation

A <u>0-ary operation</u> of M is of the form

$\{(\phi, c)\}$ with $c \in M$

$\equiv$ Denoted by c and is called a <u>constant</u>.

$$\text{graph } f = \{(a_1, a_2, \ldots, a_n, a_{n+1}) \mid f(a_1, a_2, \ldots, a_n) = a_{n+1}\} \subseteq M^{n+1}$$

= $(n+1)$ ary predicate corresponding to an n-ary operation f.

An operation $f : M^n \to M$ is uniquely described by the predicate graph $f \subseteq M^{n+1}$.

Binary operation on a set A

$$\circ : A^2 \to A$$

Commutative if $\forall a, b \in A \quad a \circ b = b \circ a$

Associative if $\forall a, b, c \in A \quad (a \circ b) \circ c = a \circ (b \circ c)$

Idempotent if $\forall a \in A \quad a \circ a = a$

Invertible if $\forall a, b \in A \; \exists x, y \in A \quad a \circ x = b \wedge y \circ a = b$.

right-inverse of a if $b = 1$

left-inverse of a if $b = 1$.

Meta Language

Expressions in our metalanguage

H, Θ

$H \Leftrightarrow \Theta$	H iff Θ	Boolean Conjunctives.
$H \Rightarrow \Theta$	if H then Θ	
$H \wedge \Theta$	H and Θ	
$H \vee \Theta$	H or Θ	

Propositional Logic = PL

a) Principle of Bivalence: PL is two-valued

True False
T F

Top Bottom
$\top$ $\bot$

Zero One
0 1

A, B, ... = Sentences in PL

b) Principle of Extensionality:
PL studies analysis of connections among the terms of given sentences ...

$A \wedge B$	A and B
$A \vee B$	A or B
$\neg A$	not A
$A \Rightarrow B$	if A then B

Modes ... Modal Logic
(Local features)

$\Diamond A$, $\Box A$, $A \cup B$

Possibly A, Necessarily A,
Sometimes A, Always A, A until B ...

Quantifiers ... First-Order Logic

$\forall$ = universal quantifiers
$\exists$ = existential quantifiers.

$\forall x_1, \dots x_n \quad P(x_1, \dots, x_n)$ For all

$\exists x_1, \dots x_n \quad Q(x_1, \dots, x_n)$ For some

Many-valued Logic

Non-classical Logic.

FORMAL LOGIC.

↳ Forms ⟶ Semantics.

Two fundamental principles.

1) Principle of Bivalence: Only two truth values exist.

2) Principle of Extensionality: The truth value of a connected sentence is determined by the truth values of their parts.

There is at least one snark.
There is at most one snark.
Every snark is a boojum.

$$\exists_x \; S(x)$$
$$\forall_{x,y} \; S(x) = S(y) \Rightarrow x = y$$
$$\forall_x \; S(x) \Rightarrow B(x)$$

$$\cfrac{\exists_x \; S(x) \;\wedge\; \forall_x \; S(x) \Rightarrow B(x)}{\cfrac{\exists_x \; S(x) \wedge S(x) \Rightarrow B(x)}{\exists_x \; B(x)} \; (MP)}$$

There must be a boojum