November 26 2013

LECTURE # 11

Logic.

Theory T:

Consider a formalism: Axiomatic theory T.
~ which describes a given domain of objects $\mathcal{A}$.

E.g. $\begin{cases} \text{Natural Numbers} \\ \text{Sets} \\ \text{Topology} \end{cases}$
etc.

Gödelian Systems.

T can describe in its language $\mathcal{L}$ about its
$\begin{cases} \text{Own syntax} \longrightarrow \text{FIXED-POINT} \\ \& \\ \text{proof from its axioms} \longrightarrow \text{PROVABILITY}. \end{cases}$

Number Theory.

PA: Peano Arithmetic

A first order theory in $\mathcal{L}_{AR}$

AXIOMS:

$\mathcal{N} = (\mathbb{N}, 0, S, +, \times)$

1) $\forall x \; Sx \neq 0$ 2) $\forall x \;\; x+0 = x$ 3) $\forall x \;\; x \times 0 = x$

4) $\forall x \; (Sx = Sy \rightarrow x = y)$

5) $\forall xy \;\; x + Sy = S(x+y)$ 6) $\forall xy \;\; x \times Sy = x \times y + x$

INDUCTION SCHEMA (IS)

$$\varphi^{x}_{0} \wedge \forall x \, (\varphi \rightarrow \varphi^{x}_{Sx}) \longrightarrow \forall x \, \varphi$$

SET THEORY

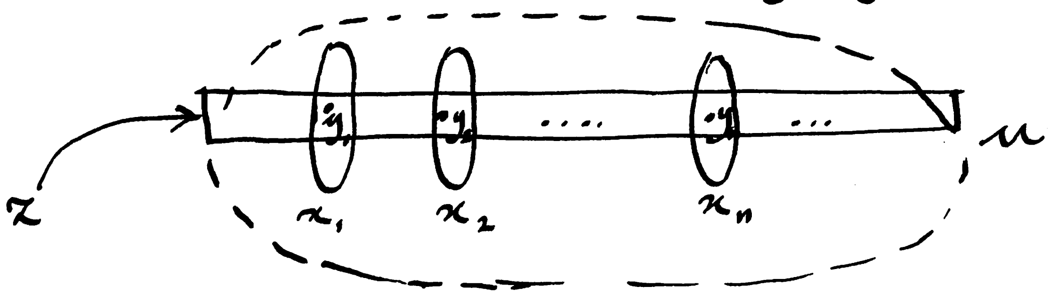
ZFC (Z = Zermelo, F = Fraenkel, C = Axiom of Choice)

A first order theory in $\mathcal{L}_{\in}$.

$\boxed{\text{AC}}$ C in ZFC $\Rightarrow$ Axiom of Choice (AC)

For every set u of disjoint nonempty sets x there is a <u>choice set</u> z that picks up precisely one element from each x in u.

$$\forall u \, [\, \phi \notin u \ \wedge \ (\forall x \in u)(\forall y \in u)\,(x \neq y \to x \cap y = \phi)$$
$$\to \ \exists z \ (\forall x \in u)\ \exists! y \ (y \in x \cap z)\,]$$



$\boxed{\text{AE}}$ Axiom of Extensionality

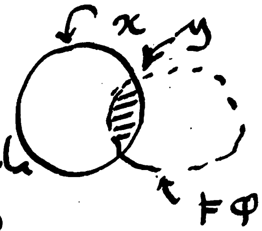
$$\forall z\,(z \in x \leftrightarrow z \in y) \ \to \ x = y$$

$\boxed{\text{AS}}$ Axiom of Separation

$$\exists y \ \forall z\,(z \in y \leftrightarrow \varphi \wedge z \in x)$$

$\begin{cases} \varphi = \mathcal{L}_{\in} \text{ formula} \\ y \notin \text{free } \varphi \end{cases}$

$y := \{z \in x \mid \varphi\}$



Unique Empty Set: ϕ

$$\exists! y \ \forall z\,(z \in y \leftrightarrow z \notin x \wedge z \in x)$$

$$u := \{z \in x \mid z \notin x\} = \phi$$

AU Axiom of Union:

$$\forall x\, \exists y\, \forall z\, (z \in y \leftrightarrow \exists_{u \in x}\, z \in u)$$

$$x \mapsto \bigcup x$$

AP Axiom of Powerset

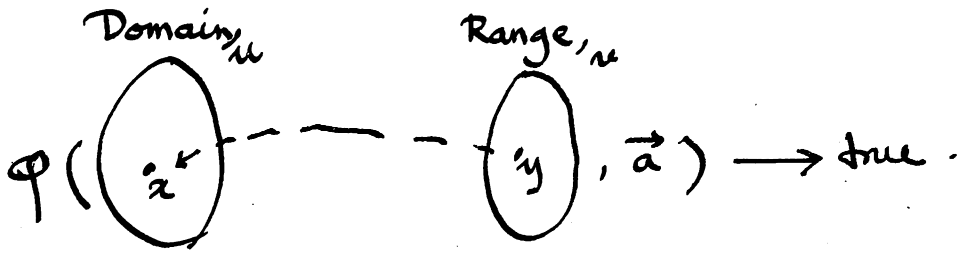
$$\forall x\, \exists y\, \forall z\, (z \in y \leftrightarrow z \subseteq x)$$

$$x \mapsto \mathcal{P}(x)$$

AR Axiom of Replacement

$$\forall x\, \exists!y\, \varphi \rightarrow \forall u\, \exists v\, \forall y\, (y \in v \leftrightarrow (\exists x \in u)\varphi)$$

$$\varphi = \varphi(x, y, \vec{a}) \qquad u, v \notin \text{free}\, \varphi$$



$$x \mapsto Fx$$

The image of a set u under F is also a set (v)

$$\{Fx \mid x \in u\}$$

$\boxed{\text{AI}}$ Axiom of Infinity

$$\exists u\,[\,\phi \in u \wedge \forall x\,(x \in u \rightarrow \underbrace{x \cup \{x\} \in u}_{Sx := x \cup \{x\}})\,]$$

$$u := \{\phi, \{\phi\}, \{\phi, \{\phi\}\}, \{\phi, \{\phi, \{\phi\}\}\}, \ldots\}$$

$\boxed{\text{AF}}$ Axiom of Foundation

$$\forall x \neq \phi \;\; \exists y \in x \;\; x \cap y = \phi$$

$\Rightarrow$ There is no set x with $x \in x$.

Gödelization

(in PA)

Recursive & Primitive Recursive Functions.

$\mathbb{F}_n$ (resp. $\mathbb{P}_n$) denotes the set of all n-ary functions (resp. predicates) with arguments and values in $\mathbb{N}$.

$$\mathbb{F}_n : \mathbb{N}^n \rightarrow \mathbb{N}. \qquad \mathbb{P}_n \subseteq \mathbb{N}^n$$

$$\mathbb{F} := \bigcup_{n \in \mathbb{N}} \mathbb{F}_n \; ; \qquad \mathbb{P} := \bigcup_{n \in \mathbb{N}} \mathbb{P}_n$$

$\boxed{Oc:}$

If $h \in \mathbb{F}_m$ and $g_1, g_2, \cdots g_m \in \mathbb{F}$ are computable, so too is their composition

$$f: h[g_1, \cdots g_m] : \mathbb{N}^{n_1} \times \cdots \times \mathbb{N}^{n_m} \to \mathbb{N}$$

$\boxed{Op:}$ If $g \in \mathbb{F}_n$ and $h \in \mathbb{F}_{n+2}$ are computable, so too is $f \in \mathbb{F}_{n+1}$ uniquely determined by the equations

$$\left.\begin{aligned} f(\vec{a}, 0) &= g(\vec{a}) \\ f(\vec{a}, Sb) &= h(\vec{a}, b, f(\vec{a}, b)) \end{aligned}\right\} : \mathbb{N}^{n+1} \to \mathbb{N}$$

<u>Primitive Recursion</u> $\to$ Oc + Op + Init

$\boxed{O\mu:}$ Let $g \in \mathbb{F}_{n+1}$ be such that

$$\forall \vec{a} \; \exists_b \; g(\vec{a}, b) = 0$$

Define $f \in \mathbb{F}_n$ by the (LFP: Least FixPoint) equation

$$f\vec{a} = \mu b.[g(\vec{a}, b) = 0]$$

[Smallest b satisfying [...]]

If g is computable, so too is f (resulting from g by μ-operation)

<u>Recursion</u> $\to$ Oc + Op + Oμ + Init

$\boxed{\text{Initial Function}}$

0 = constant

S = unary successor function

I^n_ν = Projection function

$$I^n_\nu : \vec{a} \mapsto a_\nu , \quad 1 \le \nu \le n$$

$\boxed{\text{PRIMALITY}}$

$$p_0 = 2$$

$$p_{n+1} = \mu q \le p_n! + 1 \; [\text{prim } q \wedge q > p_n]$$

$$\text{prim } q \equiv \forall_r \; r | q \to r = 1 \vee r = q$$

<u>Prime Decomposition</u>:

$$\langle a_0, \dots, a_n \rangle := p_0^{a_0+1} \cdots p_n^{a_n+1} = \prod_{i=1}^{n} p_i^{a_i+1}$$

$$= \text{Gödel number of } (a_0, \dots, a_n)$$

1) $a \in \mathcal{GN} \Leftrightarrow a \neq 0 \wedge \forall_{p \le a} \forall_{q \le p} [\text{prim } p, q \wedge p | a \to q | a]$

2) $a \in \mathcal{GN} \Rightarrow la := \mu k \le a \, [p_k \nmid a]$ $\Big\}$ "Length" of a

3) $a \in \mathcal{GN} \Rightarrow (a)_i = \mu k \le a \, [p_i^{k+2} \nmid a]$ $\Big\}$ "ith entry" of a; Projection

$\therefore$ $a \in \mathcal{GN} \Rightarrow a \mapsto (a_0, \dots, a_n)$

= Primitive Recursive

$(a_0, \dots, a_n) \mapsto \langle a_0, \dots a_n \rangle = a \in \mathcal{GN}$

= Primitive Recursive

$\therefore$ $\langle a_0, \dots, a_n \rangle = \langle b_0, \dots, b_n \rangle$

$\Leftrightarrow m = n \wedge \forall_i \; a_i = b_i$

4) Concatenation

$a, b \in \mathcal{GN}$

$$a * b = a \times \prod_{i < lb} p_{la+i}^{(b)_i + 1}$$

$\therefore$ $\langle a_1, \dots, a_n \rangle * \langle b_1, \dots, b_n \rangle$

$= \langle a_1, \dots, a_n, b_1, \dots, b_n \rangle$

Course of Value Recursion.

$$f \in \mathbb{F}_{n+1}$$

Define $\bar{f} \in \mathbb{F}_{n+1}$

$$\bar{f}(\vec{a},0) = \langle\,\rangle \qquad (\text{i.e. } \langle\,\rangle = 1)$$
$$\bar{f}(\vec{a},b) = \langle f(\vec{a},0), f(\vec{a},1), \dots, f(\vec{a},b-1)\rangle$$
when $b>0$.

$\boxed{\text{Oq:}}$ Let $F \in \mathbb{F}_{n+2}$

Define $f \in \mathbb{F}_{n+1}$

$$f(\vec{a},b) = F(\vec{a},b,\bar{f}(\vec{a},b))$$

If F is primitive recursive, so too is f.

Note Oq $\Rightarrow$

$$f(\vec{a},0) = F(\vec{a},0,1)$$
$$f(\vec{a},1) = F(\vec{a},1,\bar{f}(\vec{a},1))$$
$$= F(\vec{a},1,\langle f(\vec{a},0)\rangle)$$
$$= F(\vec{a},1,\langle F(\vec{a},0,1)\rangle)$$
$$f(\vec{a},2) = F(\vec{a},2,\langle F(\vec{a},0,1), F(\vec{a},1,\langle F(\vec{a},0,1)\rangle)\rangle)$$

$$\vdots$$

$F(b,c) = b; \quad b \leq 1.$

$F(b,c) = (c)_{b-1} + (c)_{b-2}; \quad \text{otherwise}.$

故

$$
\begin{aligned}
f0 &= F(0, \bar{f}0) = 0 \\
f1 &= F(1, \bar{f}1) = 1 \\
f2 &= F(2, \bar{f}2) = F(2, \langle f0, f1 \rangle) \\
&= f0 + f1 = 1 \\
f3 &= F(3, \bar{f}3) = F(3, \langle f0, f1, f2 \rangle) \\
&= f1 + f2 = 2 \\
&\vdots \\
fn &= F(n, \bar{f}n) = F(n, \langle f0, f1, \dots, fn-2, fn-1 \rangle) \\
&= f(n-2) + f(n-1)
\end{aligned}
$$

Gödelization (Arithmetization)

$\mathcal{L} = \mathcal{L}_{AR}$ $\quad s \in \mathcal{L}$ = Basic Symbols

$\# s$ = Its "symbol code"

$\# = : 1$ $\quad \# \neg : 3$ $\quad \# \wedge : 5$ $\quad \# \forall : 7$

$\# (: 9$ $\quad \#) : 11$ $\quad \# 0 : 13$ $\quad \# S : 15$

$\# + : 17$ $\quad \# \times : 19$ $\quad \# v_0 : 21$ $\quad \cdots$

Only odd #'s are used (*)

$$0=0 \mapsto \langle 13, 1, 13 \rangle \equiv 2^{14} 3^{2} 5^{14}$$

$$\underline{0} \mapsto \langle 13 \rangle = 2^{14}$$

$$\underline{1} \mapsto \langle 15, 13 \rangle = 2^{16} 3^{14} \quad (\underline{1} = \underline{S0})$$

$$\underline{2} \mapsto \langle 15, 15, 13 \rangle = (2 \times 3)^{16} 5^{14}$$

$$\vdots$$

$\xi \in S_{\mathcal{L}}$ ← A sentence in the language $\mathcal{L}$

$\mapsto \dot{\xi} = \langle \xi \rangle$ = Gödel Number of $\xi \in S_{\mathcal{L}}$

$$(\xi\eta)^{\cdot} = \dot{\xi} * \dot{\eta}$$

$\dot{S}_{\mathcal{L}} = \{ \dot{\xi} \mid \xi \in S_{\mathcal{L}} \}$ = p.r. subset of all Gödel numbers.

$\subseteq \mathcal{GN}$

Note: $n \in \dot{S}_{\mathcal{L}}$ iff $n \in \mathcal{GN} \wedge (\forall_{k < \ell n})\ 2 \mid (n)_k$ $\quad (\because *)$

$\dot{W} = \{ \dot{\xi} \mid \xi \in W \}$

Predicates

⇐ Primitive Recursive. / Recursive.

$\mathcal{L}_{AR}$ = A Gödelian System.

(G1) Diagonalizer is computable

$$K(n)\ \begin{cases} n \in GN \\ \text{check } n \in \dot{W} \\ \text{Compute } H_n \in W \\ \text{Write } H_n(n) \\ \text{Compute } S_{n^*} \\ \text{Evaluate } H_n(n^*) \end{cases}$$

(G2) Provability Predicate is computable.

$\Phi = (\varphi_0, \cdots \varphi_n)$ = Proof from $X \subseteq \mathcal{L}_{AR}$

$X \vdash_{\mathcal{L}_{AR}} \varphi_n$

Finite sequence of $\mathcal{L}_{AR}$-formulas.

$\dot{\Phi} = \langle \dot{\varphi}_0, \dot{\varphi}_1, \cdots \dot{\varphi}_n \rangle$ = Gödel number of the proof.

$$pf_T(b) \iff b \in GN \ \wedge\ b \neq 1 \ \wedge$$
$$(\forall_{k < \ell b}) \left[(b)_k \in \dot{X} \cup \dot{\Lambda} \right.$$
$$\left. \vee\ (\exists_{i,j<k}\ (b)_i^{\cdot} = ((b)_j \rightarrow (b)_k)^{\cdot} \right]$$

$bew_T(b, a) \iff pf_T(b) \wedge a = (b)_{last}$ [beweis = proof]

$bwb_T(a) \iff \exists_b\ bew_T(b, a)$ [beweisbar = provable]