

CMSC 3110 Week 9: Gödel's incompleteness and Hilbert's 10th problem

Lecture: Ketan Mulmuley

November 20, 2006

—Gödel's work and foundation of mathematics—

○ **Basic Question:** Can every truth be proven? \Rightarrow No.

- What is a truth?] Semantics (Model)
- What is a proof?] Language, Syntax

○ **Number theory**

Model (domain): \mathbb{N} (natural number)

0, 1: constant

+	}	Basic function
-		
\times		
exp	}	Basic prediction
>		
=		

○ **Axioms:** Basic operation & predicates satisfy

$(a + b) * c = a * c + b * c$ } Peano's axiom

\wedge	}	Boolean operation
\vee		
\neg		
$\forall x$		
$\exists x$		

- well formula

$$\forall a \forall b \forall c \quad (a + b) * c = a * c + b * c$$

○ **Hilbert**

Given a sentence σ in Number theory is there are algorithm to decide if σ is true or not.

○ **Fermata lost theorem**

$$\neg[\exists(n, x, y, z):(n > 2) \& (x^n + y^n = z^n)]$$

$x^n + y^n = z^n$ has no integer solution if $n > 2$

○ **Hilbert 10 th problem**

Given a Diophantine equation, so that

$$2x^2y^3z^4 - 3x^3y^2z^5 + 5xyz = 0.$$

- Fundamental problem

Given a Diophantine equation decide if it has an integer solution.

- Hilbert's 10 th problem [No]

Give an algorithm, which, given a Diophantine equation $F(x_1, L, x_n) = 0$ decides in finite time if it has an integer solution.

○ **Gödel's Incompleteness theorem**

No Number theory is undecidable.

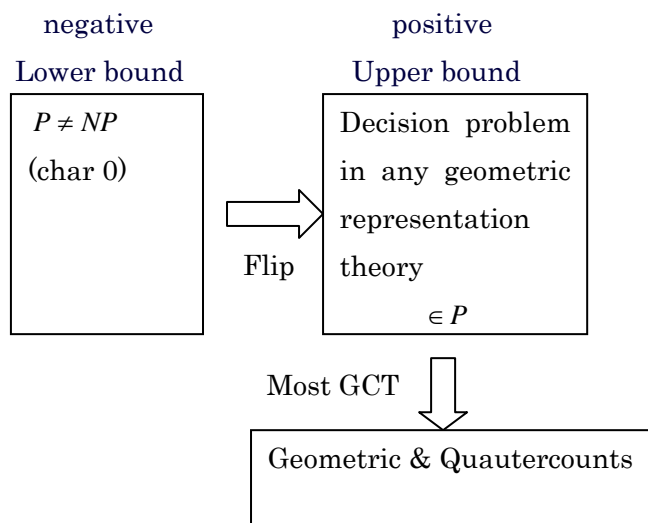
There is no algorithm, which given a sentence σ in number can decide if σ is true.

○ **Geometric Complexity theorem (GCT)**

Nonrelativizable form of diagonalization

0) Proof – Algorithm

1) Flip: negative to positive



- **H.Weyl:** Any finite dimension representation of $GL_n(\mathbb{C})$ splits of a direct sum of irreducible representation.

$$\lambda: \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n \geq 0$$

$V_\lambda(GL_n(\mathbb{C}))$: Weyl model

$$V_\alpha \otimes V_\beta = \bigoplus C_\lambda^{\alpha\beta} V_\lambda$$

- Decision question: $C_\lambda^{\alpha\beta} > 0$?

Give α, β, λ whether $C_\lambda^{\alpha\beta}$ is representation can be decided in $\text{poly}(\langle \alpha \rangle, \langle \beta \rangle, \langle \lambda \rangle)$.

1) $C_\lambda^{\alpha\beta}$: #P formula LiHleword-Richardson rule

2) $(\alpha, \beta, \lambda) \rightarrow P_{\alpha\beta}^\lambda$ such that $C_\lambda^{\alpha\beta} = \varphi(P_{\alpha\beta}^\lambda)$

3) $P_{\alpha\beta}^\lambda$ is nonempty the $C_\lambda^{\alpha\beta} \neq 0$ Saturation theorem of Kuitsen-Tac

4) Ellipsoid method

$$GL_n(\mathbb{C}) \rightarrow GL(w) \rightarrow GL(X)$$

Given $V_\lambda(GL_n(\mathbb{C}))$, does it occur in X.

1) Quontum-Group [Drinfeld]

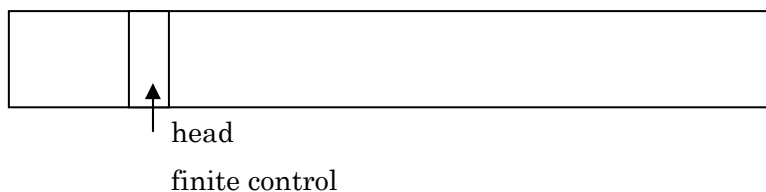
2) ???

3) Saturation theorem

4) ???

○ Church-Turing Theory

Computable \Leftrightarrow Turing-Machine Computable

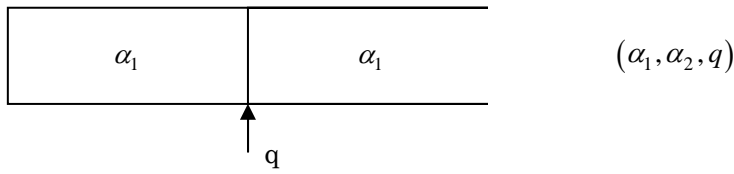


- Machine Transition rule

$$\Sigma \times Q \rightarrow \Sigma \times Q \times D$$

Tape symbol states new symbol new state $\{L, R\}$

○ ID (instantaneous description)



q_0 : initial ID



- Computation

Encoding: $\# \beta_0 \# \beta_1 \# L \# \beta_l \#$

- Basic idea

Undecidable: Given M, ϵ , does M accept ϵ ?

Undecidability of Number theory \leftarrow Undecidability of the Halting problem

$M \Rightarrow \sigma(M)$: Gödel number
 Chinese Remainder theorem } M accepts ϵ
 iff $\sigma(M)$ is true

$\beta \approx (\beta_0, \beta_1, L, \beta_l)$

$\sigma(M) : \exists \beta, \exists m$ bound on length of any β_i

(1) How to encode a computation?

(2) $Em(\beta)$: Predicate which is true if β denote a valid computation of M in which no ID exceeds length m

○ **Chinese remainder theorem**

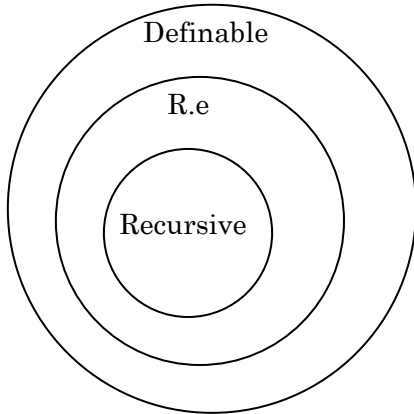
Given relative some integer m , $0 \leq i \leq n$, and $0 \leq a_i < m_i$, $\exists a$ unique integer A :
 $0 \leq A < \pi m_i$ such that $A = a_i \pmod{m_i}$.

$Em(\beta)$:

$$\left\{ \begin{array}{l} (1) \beta_0 = \beta \pmod{m_i} \\ (2) \beta_i \underset{M}{|-} \beta_{i+1} \\ (3) \beta_i \text{ is accepting ID} \end{array} \right.$$

○ **Tarski Undefinability theorem**

A predicate $p(x_1, L, x_n)$ is definable if $p(x_1, L, x_n)$ holds iff $\models \varphi(x_1, L, x_n)$.



$\text{Th}(\mathbb{N}) = \{\sigma \mid \models \sigma\}$: theory in \mathbb{N}

$\#\text{Th}(\mathbb{N}) = \{\#\sigma \mid \models \sigma\}$ is undefinable

○ **Fixed point Lemma**

Given any formula $\beta(x)$, we can construct a sentence σ such that

$$\models \{\sigma \leftrightarrow \beta(\#\sigma)\}.$$

σ is saying that β is true of me.

Proof: Suppose to the contrary that $\#\text{Th}(\mathbb{N})$ is definable by a formula $\beta(x)$.

By fixed point lemma, $\exists a$ sentence σ such that

$$\models \{-\sigma \leftrightarrow \neg\beta(\#\sigma)\}$$

σ is saying that I am not decidable.