# 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? ⇒ No.

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

○ Number theory

Model (domain): N (natural number)

0, 1: constant

+<br>
−  } Basic function<br>
×<br>
exp<br>
>  } Basic prediction<br>
=

○ Axioms: Basic operation & predicates satisfy

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

$\wedge$<br>
$\vee$  } Boolean operation<br>
$\neg$<br>
$\forall x$<br>
$\exists x$

- well formula

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

○ Hilbert

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

○ **Fermata lost theorem**

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

$x^n+y^n=z^n$ 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 $F(x_1,\ldots,x_n)=0$ decides in finite time if it has an integer solution.

○ **Gödel's Incompleteness theorem**

No Number theory is undecidable.

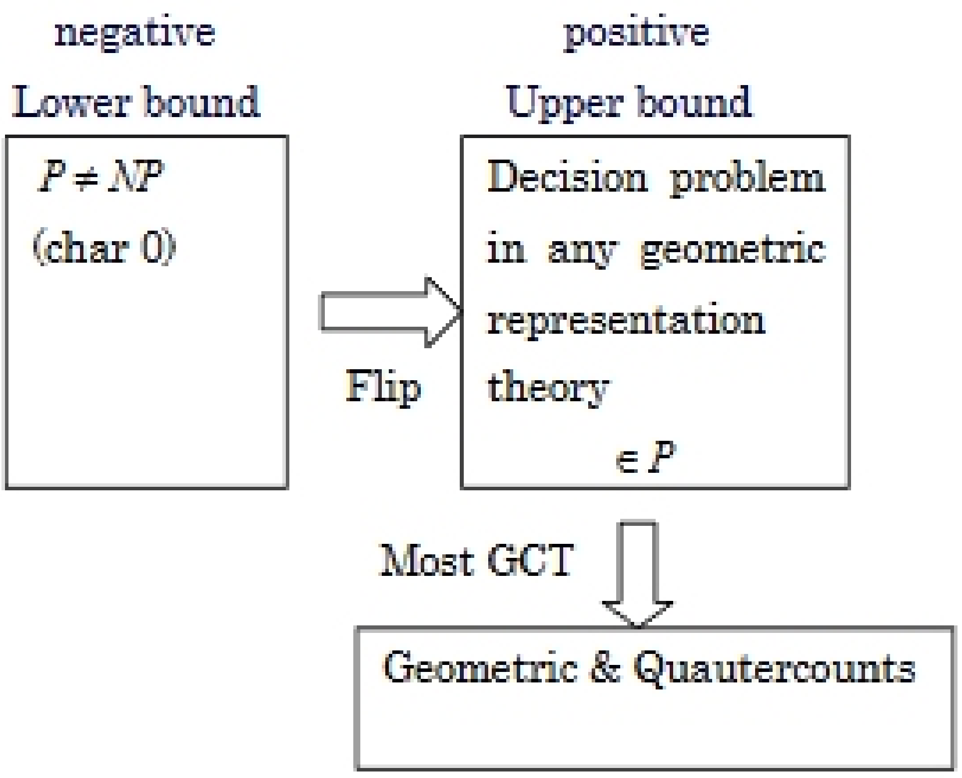
There is no algorithm, which given a sentence $\sigma$ in number can decide if $\sigma$ is true.

○ **Geometric Complexity theorem (GCT)**

Nonrelativizable form of diagonalizaiton

0) Proof – Algorithm

1) Flip: negative to positive



- H.Weyl: Any finite dimension representation of GLn(c) splits of a direct sum of irreducible representation.

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

  $V_\lambda(GLn(c))$: Weyl model

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

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

Give $\alpha, \beta, \lambda$ whether $C_\lambda^{\alpha\beta}$ is representation can be decided in 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

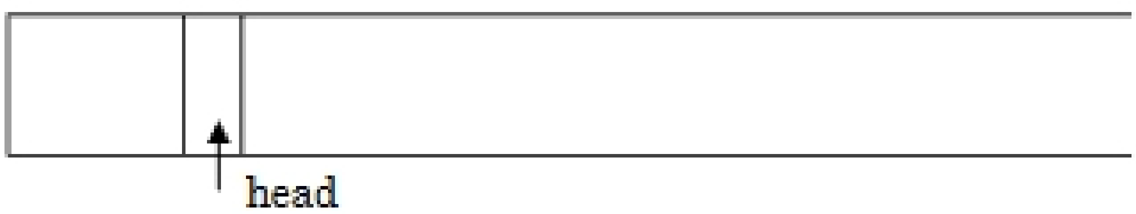
$GL_n(c) \rightarrow GL(w) \rightarrow GL(X)$

Given $V_\lambda(GL_n(c))$, does it occur in X.

1) Quontum-Group [Drinfeld]
2) ???
3) Saturation theorem
4) ???

○ **Church-Turing Theory**

Computable ⇔ Turing-Machine Computable



head

finite control

- Machine Transition rule

| $\Sigma$ | $\times$ | $Q$ | $\rightarrow$ | $\Sigma$ | $\times$ | $Q$ | $\times$ | $D$ |
|---|---|---|---|---|---|---|---|---|
| Tape symbol | | states | | new symbol | | new state | | $\{L, R\}$ |