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
  +  
  −  
  ×  
  exp 
  >  
  = 

○ **Axioms**: Basic operation & predicates satisfy
  \[(a + b) \times c = a \times c + b \times c\] Peano’s axiom

  ∧  
  ∨  
  ¬  
  ∀x  
  ∃x  

  • well formula
  \[\forall a \forall b \forall c \quad (a + b) \times c = a \times c + b \times c\]

○ **Hilbert**
Given a sentence \(\sigma\) in Number theory is there are algorithm to decide if \(\sigma\) is true or not.
- **Fermata lost theorem**
  
  \[ \neg \exists (n,x,y,z) : (n>2) \land (x^n + y^n = z^n) \]

  \[ x^n + y^n = z^n \] has no integer solution if \( n > 2 \)

- **Hilbert 10th 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 10th 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 \( \sigma \) in number can decide if \( \sigma \) is true.

- **Geometric Complexity theorem (GCT)**
  
  Nonrelativizable form of diagonalizaiton
  
  0) Proof – Algorithm
  
  1) Flip: negative to positive

  ![Diagram](image-url)
- **H.Weyl**: Any finite dimension representation of $GL_n(c)$ splits of a direct sum of irreducible representation.
  
  $\lambda: \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq 0$

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

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

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

  Given $\alpha, \beta, \lambda$ 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 LiHeWorRichardson rule

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

  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) Quantum·Group [Drinfeld]

  2) ???

  3) Saturation theorem

  4) ???

- **Church·Turing Theory**

  Computable $\iff$ 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)**

  \[ (\alpha_1, \alpha_2, q) \]

- \( q_0 \): initial ID

  \[ (\omega, \alpha_1, \alpha_2) = (\varepsilon, \omega) \]

- Computation

  Encoding: \# \beta_0 \# \beta_1 \# L \# \beta_i \#

- Basic idea

  Undecidable: Given \( M, \varepsilon \), does \( M \) accept \( \varepsilon \)?

  Undecidability of Number theory \( \leftarrow \) Undecidability of the Halting problem

  \[ \begin{align*}
  & M \Rightarrow \sigma(M): \text{Gödel number} \\
  & \text{Chinese Reminder theorem} \end{align*} \]

  \[ \begin{align*}
  & M \text{ accepts } \varepsilon \\
  & \text{iff } \sigma(M) \text{ is true} \\
  \end{align*} \]

  \[ \beta = (\beta_0, \beta_1, L, \beta_i) \]

  \[ \sigma(M): \exists \beta, \exists m \text{ bound on length of any } \beta_i \]

  (1) How to encode a computation?

  (2) \( Em(\beta) \): Predicate which is true is \( \beta \) denote a valid computation of \( M \) in which no ID exceeds length \( m \)
○ **Chinese remainder theorem**
Given relative some integer $m_i$, $0 \leq i \leq n$, and $0 \leq a_i < m_i$, $\exists a$ unique integer $A : 0 \leq A < \pi m_i$ such that $A = a_i \mod m_i$.

$Em(\beta)$:
\[
\begin{align*}
(1) \quad & \beta_0 = \beta \mod m_i \\
(2) \quad & \beta_i \mid_M \beta_{i+1} \\
(3) \quad & \beta_i \text{ is accepting ID}
\end{align*}
\]

○ **Tarski Undefinability theorem**
A predicate $p(x_1, L, x_n)$ is definable if $p(x_1, L, x_n)$ holds iff $\models \phi(x_1, L, x_n)$.

\[
\begin{array}{c}
\text{Definable} \\
\text{R.e} \\
\text{Recursive}
\end{array}
\]

Th(N) = $\{\sigma \mid \models \sigma\}$ : theory in N
\#Th(N) = $\{\#\sigma \mid \models \sigma\}$ is undefinable

○ **Fixed point Lemma**
Given any formula $\beta(x)$, are can construct a sentence $\sigma$ such that

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

$\sigma$ is saying that $\beta$ is true of me.

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

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

$\models \neg \sigma \leftrightarrow \neg \beta(\#\sigma)$

$\sigma$ is saying that I am not decidable.