Hilbert's Tenth Problem

HEINZ NIXDORF INSTITUTE
University of Paderborn
Algorithms and Complexity

- David Hilbert (1900), Tenth Problem:
  - *Devise a 'mechanical procedure'* (=algorithm) *for deciding truth of arithmetical formula*
  - e.g. of " $\forall n\, \exists x,y,z:\quad x^n+y^n=z^n$ "
- Gödel (1931): There exist arithmetical formula which can neither be proven nor refuted!
- Yuri V. Matiyasevich (1970): There exists a computable mapping $P \to p_P$ of programs to multivariate integer polynomials such that P terminates iff p_P has an integer root.

Recall Undecidability

HEINZ NIXDORF INSTITUTE
University of Paderborn
Algorithms and Complexity

- Decidable problems: $\emptyset$, $\{ 0^n 1^n \mid n \}$, SAT, …
- Many undecidable problems:
  - diagonal language *D*, *H*, *H* complement
  - **`Hilbert's Tenth Problem`**
  - Properties of languages accepted by a given program (Rice's Theorem)
  - **`Post Correspondence Problem`**
  - *Word Problem for Finitely Presented Groups*
  - *Simply-Connectedness of Simplicial Complexes*
- Higher degrees of undecidability…

Definition: "$A \leq B$" iff *A* decidable by $\mathbf{BF}^B$. Poset

Note: The above problems are linearly ordered: Undecidability proofs by reduction to *D*.

Post‘s Question

- Decidable problems
- Undecidable L s.t. H is decidable by $\mathbf{BF}^L$
- Undecidable problems stricly beyond H: T, H^H
- Emil Post 1944: a) Is anything in between?
  b) Are there incomparable problems?
- That is, do there exist
  - semi-decidable problems A, B
  - such that A is not decidable by $\mathbf{BF}^B$
  - nor is B decidable by $\mathbf{BF}^A$?
- Answered 1956/57 by Friedberg & Muchnik

Recap on Diagonalization

HEINZ NIXDORF INSTITUTE
University of Paderborn
Algorithms and Complexity

$D = \{ \langle P \rangle \mid$ program P does <u>not</u> terminate on input $\langle P \rangle \}$

$D_t := \{ \langle P \rangle\#0^k$: program P does not accept $\langle P \rangle\#0^k$ within $t(n)\cdot n$ steps, $n:=|\langle P \rangle|+k \}$

Define disjoint increasing sequences of finite sets

$\emptyset \subseteq B_1 \subseteq B_2 \subseteq B_3 \subseteq \ldots B \quad \emptyset \subseteq C_1 \subseteq C_2 \subseteq C_3 \subseteq \ldots C$

i-1→i: Take $n_i > n_{i-1}$ s.t. $B_{i-1}, C_{i-1} \subseteq \Sigma^{<n_i} \wedge 2^{n_i} > n_i^i + i$

Now 'simulate' $M_i^?$ on input $\underline{x} := 1^{n_i}$:

Start with $Z := \emptyset$; oracle queries "$\underline{y} \in ?$"

- in case $\underline{y} \in B_{i-1}$, answer **yes**
- in case $\underline{y} \in C_{i-1}$, answer **no**
- otherweise answer **no** and let $Z := Z \cup \{\underline{y}\}$

If accepts, let $B_i := B_{i-1} \subseteq \Sigma^{<n_i}$ and $C_i := C_{i-1} \cup Z$;

if rejects, $B_i := B_{i-1} \cup \{\underline{w}\}$ and $C_i := C_{i-1} \cup Z$,

$w \in \Sigma^{n} \wedge Z$