Incompleteness of (Integer) Arithmetic

[Schöning, van Glabbeek]

Kurt Gödel. *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I.* 1931.

Kurt Gödel

1906	—	1978
Brünn		Princeton

Arithmetic and notation

We consider formulas over the signature $\Sigma = \{+, *, <, =\}$.

Arithmetic is the set of all Σ-sentences that are true in the interpretation with universe $\mathbb{N}$ and where $+, *, <, =$ are interpreted in the standard way.
(We substitute $\mathbb{N}$ for $\mathbb{Z}$ for convenience, it is an inessential detail.)

We denote the set of all sentences of arithmetic by W.

$F(x_1, \ldots, x_k)$ denotes a formula in which at most the variables $x_1, \ldots, x_k$ occur free.

If $n_1, \ldots, n_k \in \mathbb{N}$ then $F(n_1, \ldots, n_k)$ is the result of substituting $n_1, \ldots, n_k$ for the free occurrences of $x_1, \ldots, x_k$.

Example

$$\begin{aligned} F(x, y) &= (x = y \ \wedge \ \exists x.\, x = y) \\ F(5, 7) &= (5 = 7 \ \wedge \ \exists x.\, x = 7) \end{aligned}$$

Arithmetically representable functions and relations

Formulas with free variables can represent functions and relations.

The formula

$$F(x, y) = (\exists z.\ y = x + z + 1)$$

represents the relation "$x < y$"

The formula

$$F(x, y, z) = (\exists k.\ x = k * y + z \land z < y)$$

represents the relation "$z = x \bmod y$".

Definition

A k-ary relation $R \subseteq \mathbb{N}^k$ is arithmetically representable iff there is a formula $F(x_1, \ldots, x_k)$ s.t. for all $n_1, \ldots, n_k \in \mathbb{N}$:

$$(n_1, \ldots, n_k) \in R \quad \text{iff} \quad F(n_1, \ldots, n_k,) \in W$$

We call F a representation of R.

Representing the transition relation of Turing machines

Given a deterministic Turing machine M with states $\{0, \ldots, n\}$ over the tape alphabet $\{0, 1\}$, we encode a configuration c of M as a tuple $\underline{c} = (l, q, r) \in \mathbb{N}^3$ where

- q encodes the state of M;
- l encodes the left-string: the string to the left of the head, read as a binary number with an additional leading 1;
- r encodes the right-string: the string including the square where the head is, and extending to the right, read *in reverse* as a binary number with an additional leading 1.

Definition

The transition relation of M is the relation $T_M \subseteq \mathbb{N}^6$ given by

$$T_M = \{(\underline{c}_1, \underline{c}_2) \mid c_2 \text{ is the successor configuration of } c_1\} .$$

Representing the transition relation of Turing machines

Lemma

For every Turing machine M the relation T_M is arithmetically representable.

Proof idea: Let $c_1 \xrightarrow{q,a} c_2$ denote that c_1 is a configuration with state q where the head reads a and c_2 is the successor of c_1

For every state q and symbol a of M define

$$T_M^{q,a} := \{(\underline{c}_1, \underline{c}_2) \mid c_1 \xrightarrow{q,a} c_2\}$$

and define an arithmetic representation of $F_M^{(q,a)}$.

For example, if $\delta(3,0) = (5,1,R)$ then define

$$\begin{aligned} &F_M^{3,0}(l_1, q_1, r_1, l_2, q_2, r_2) \\ =:\ &(q_1 = 3 \wedge q_2 = 5 \wedge l_2 = l_1 * 2 + 1 \wedge r_1 = r_2 * 2) \end{aligned}$$

The formula $F_M := \bigvee_{q \in Q_M, a \in \Sigma_M} F_M^{q,a}$ is a representation of T_M

Representing the reachability relation of Turing machines

Lemma

For every Turing machine M the transitive closure T_M^* of T_M is arithmetically representable.

We only sketch the proof of a weaker result.

Given a formula $F(x, y)$ of arithmetic representing a binary relation R we can effectively construct a formula $F^*(x, y)$ of arithmetic with exponentiation representing R^*.

A full proof of the lemma requires to express exponentiation in arithmetic and extend the result to formulas $F(\vec{x}, \vec{y})$.

Key idea of the proof: encode a sequence $a_n, a_{n-1}, \ldots, a_0 \in (\mathbb{N} \setminus \{0\})^*$ of arbitrary length as a pair $(t, p) \in \mathbb{N}^2$ where

- $p > a_i$ for all $0 \leq i \leq n$ and
- the word $a_n \ldots a_1 a_0 \in [p]^*$ is the p-ary representation of t.

Representing the reachability relation of Turing machines

Represent the relation "$y = a_0$" by the formula

$$Last(t, p, y) = y < p \wedge \exists x\, (t = x * p + y)$$

Represent "$x = a_n$" by

$$First(t, p, x) = x < p \wedge \exists z\, \exists w\, (t = x * p^z + w \wedge w < p^z)$$

Represent "v comes after u" by

$$\begin{aligned} Next(t, p, u, v) \quad = \quad & u < p \wedge v < p \wedge \\ & \exists i\, \exists y\, \exists z\, \big(t = y * p^{i+2} + u * p^{i+1} + v * p^i + z \\ & \qquad\qquad \wedge\, z < p^x \wedge y + u > 0\big) \end{aligned}$$

Take

$$\begin{aligned} F^*(x, y) \quad = \quad & \exists t\, \exists p\, \big(First(t, p, x) \wedge Last(t, p, y) \wedge \\ & \qquad\qquad \forall u\, \forall v\, (Next(t, p, u, v) \rightarrow F(u, v))\big) \end{aligned}$$

Arithmetic is not semi-decidable

Theorem

W is not semi-decidable.

Proof. By reduction from the set of all pairs (M, x) where M is a Turing machine, x is an input for M, and M does not halt on x. This set is known to not be semi-decidable.

Let M be a Turing machine with states $\{0, \ldots, n\}$ and let x be an input for M. Assume n is the only final state.

Let F_M be a representation of the transition relation T_M of M. Let c_0 be the initial configuration of M on input x.

Define

$$NH_{M,x} = \neg \exists l \, \exists q \, \exists r \, (F_M^*(\underline{c}_0, l, q, r) \wedge q = n)$$

$Wehave: NH_{M,x} \in W$ iff M does not halt on input x.

Proof systems

What is a *proof system*? Minimal requirement: It must be decidable if a given text is a proof of a given formula.

We encode texts as natural numbers.

Definition

Let S be the set of all sentences over the signature of arithmetic. A proof system for arithmetic is a decidable predicate

$$Prf : \mathbb{N} \times S \;\rightarrow\; \{0, 1\}$$

(Read $Prf(p, F)$ as "'p is a proof of F"'.)

A proof system Prf is correct or sound iff $Prf(p, F)$ implies $F \in W$. ("Everything provable is true.")

A proof system Prf is complete iff for every $F \in W$ there exists a proof p such that $Prf(p, F)$. ("Everything true is provable.")

Gödel's Incompleteness Theorem

Theorem (Gödel)

There is no correct and complete proof system for arithmetic.

Proof. Assume there exists a correct and complete proof system. The following procedure semi-decides W:

Input: sentence F

$p := 0;$
while $Prf(p, F) = 0$ **do** $p := p + 1;$
output("$F \in W$")

Corollary

For every correct proof system for arithmetic there exists a sentence F such that neither F nor $\neg F$ can be proved.

Hilbert's 10th Problem

> *Given a diophantine equation: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in integers.*

Hilbert, ICM, Paris, 1900

Theorem (Matiyasevich, Robinson, Davis, Putnam, 1949-1970)

It is undecidable if a diophantine equation has a solution.