Incompleteness of (Integer) Arithmetic

[Schöning, *Theoretische Informatik*]

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

Kurt Gödel
1906 (Brünn) –
1978 (Princeton)

Syntax of arithmetic:

$$\begin{array}{rrcl} \text{Variablen:} & V & \to & x \mid y \mid z \mid \ldots \\ \text{Zahlen:} & N & \to & 0 \mid 1 \mid 2 \mid \ldots \\ \text{Terme:} & T & \to & V \mid N \mid (T + T) \mid (T * T) \\ \text{Formeln:} & F & \to & (T = T) \mid \neg F \mid (F \wedge F) \mid (F \vee F) \mid \exists V.\, F \end{array}$$

We consider $\forall x.\, F$ as an abberviation for $\neg\exists x.\, \neg F$.

Definition

An occurrence of a variable x in a formula F is bound iff the occurrence is in a subformula of the form $\exists x.\, F'$ within F'.
An occurrence is free iff it is not bound.

Notation: $F(x_1, \ldots, x_k)$ 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

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

A sentence is a formula without free variables.

Example

$$\exists x.\ \exists y.\, x = y$$

S is the set of arithmetic sentences.

Definition

W is the set of true sentences of arithmetic:

$$
\begin{aligned}
(t_1 = t_2) \in W \quad &\text{iff} \quad t_1 \text{ and } t_2 \text{ have the same value.} \\
\neg F \in W \quad &\text{iff} \quad F \notin W \\
(F \wedge G) \in W \quad &\text{iff} \quad F \in W \text{ and } G \in W \\
(F \vee G) \in W \quad &\text{iff} \quad F \in W \text{ or } G \in W \\
\exists x.\, F(x) \in W \quad &\text{iff} \quad \text{there is some } n \in \mathbb{N} \text{ s.t. } F(n) \in W
\end{aligned}
$$

Fact

For every sentence F: $F \in W$ iff $\neg F \notin W$,

NB If a formula with free variables is true or not can depend on the value of the free variables:

$$\exists x.\, x + x = y$$

Therefore absolute truth only makes sense for sentences.

Formulas can represent functions and relations.

Examples

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

represents "$x < y$": $t_1 < t_2$ is an abbreviation of $F(t_1, t_2)$.

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

represents "$z = x \bmod y$"

Definition

A partial function $f : \mathbb{N}^k \to \mathbb{N}$ is arithmetically representable iff there is a formula $F(x_1, \ldots, x_k, y)$ s.t. for all $n_1, \ldots, n_k, m \in \mathbb{N}$:

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

Theorem

Every WHILE-computable function is arithmetically representable.

Theorem

W is not decidable.

Proof.

Let $U \subseteq \mathbb{N}$ be a semi-decidabe but not decidable set.
$\Rightarrow \chi'_U$ is WHILE-computable
$\Rightarrow \chi'_U$ is arithmetically representable by some $F(x, y)$
$\Rightarrow n \in U$ iff $\chi'_U(n) = 1$ iff $F(n, 1) \in W$
$\Rightarrow W$ is not decidable. □

Corollary

W is not semi-decidable.

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

We code proofs as natural numbers.

Definition

A proof system for arithmetic is a decidable predicate

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

where $Prf(p, F)$ means "'p is a proof for the sentence F"'.
A proof system Prf is correct iff

$$Prf(p, F) \Rightarrow F \in W.$$

A proof system Prf is complete iff

$$F \in W \Rightarrow \text{ there exists a } p \text{ with } Prf(p, F).$$

Theorem (Gödel)

There is no correct and complete proof system for arithmetic.

Proof.

With every correct and complete proof system
$\chi'_W(F)$ can be programmed:

$p := 0$
while $Prf(p, F) = 0$ **do** $p := p + 1$
output(1)

□

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 (Yuri Matiyasevich, Julia Robinson, Martin Davis, Hilary Putnam, 1949-1970)

It is in general undecidable if a diophantine equation has a solution.

An Isabelle Proof

J. Bayer, M. David, B. Stock, A. Pal, D. Schleicher.
Diophantine Equations and the DPRM Theorem.
Archive of Formal Proofs. 2022.

DPRM = Davis, Putnam, Robinson, Matiyasevich