

# A Quick Introduction to MATHEMATICAL LOGIC

SAEED SALEHI

Frontiers Summer School in Mathematics

Gödel's Incompleteness, 30 August 2021

## The Halting Problem (1)

Some Recursive Functions may Never Halt (may not have outputs on some inputs); e.g.,

$$D(x, y) = [\mu z. z+x=y] = \begin{cases} y-x & \text{if } x \leq y \\ \text{undefined} & \text{if } x > y \end{cases}$$

halts only when  $x \leq y$ .

**Notation:**  $\begin{cases} f(x) \downarrow & f \text{ is defined at } x \\ f(x) \uparrow & f \text{ is not defined at } x \end{cases}$

Recursive Functions can be encoded by natural numbers:

Any description (proof) of a recursive function is a well-built sequence of  $\langle Z, S, \pi_j^k, A, M, E, \chi_{\leq}, \wp, \circ, \mu \rangle$  ( $\circ$  stands for composition) and thus can be coded in  $\mathbb{N}$ .

Denote the (Gödel) code of the recursive function  $f$  by  $\ulcorner f \urcorner$ .

## The Halting Problem (2)

### Theorem (Turing 1937)

*There is no recursive function  $h$  such that for any Recursive  $f$ ,*  
 $h(\ulcorner f \urcorner) = 1 \iff f(\ulcorner f \urcorner) \downarrow$     *and*     $h(\ulcorner f \urcorner) = 0 \iff f(\ulcorner f \urcorner) \uparrow$ .

### Proof.

Otherwise,  $g(x) = \mu z. (z + h(x) = z)$  would be recursive too, for which we have  $g(\ulcorner f \urcorner) \downarrow \iff f(\ulcorner f \urcorner) \uparrow$  for every recursive  $f$ . Putting  $f = g$  we get the contradiction  $g(\ulcorner g \urcorner) \downarrow \iff g(\ulcorner g \urcorner) \uparrow$  ! ■

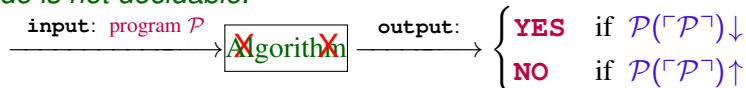
### Corollary

*There is no algorithmic way for recognizing whether a given program is a virus (self-generating) or not.*

## An Undecidable, and a Non-Enumerable Set

### Corollary (The Halting Set is *Not* Decidable)

*The set of all (single-input) programs which halt on their own code is not decidable.*



### Theorem (The Halting Set *Is* Enumerable)

*An input-free algorithm enumerates the set  $\{\mathcal{P} \mid \mathcal{P}(\ulcorner \mathcal{P} \urcorner) \downarrow\}$ .*

#### Proof.

Enumerate all the (single-input) programs  $\mathcal{P}_0, \mathcal{P}_1, \dots$ .

Let  $n := 1$ ; for  $i = 0$  to  $i = n$  run the  $n$  stages of  $\mathcal{P}_i(\ulcorner \mathcal{P}_i \urcorner)$ ; if it halts then PRINT " $i$ "; let  $n := n + 1$  and repeat. ■

### Corollary (The Non-Halting Set is *Not* Enumerable)

*The set  $\{\mathcal{P} \mid \mathcal{P}(\ulcorner \mathcal{P} \urcorner) \uparrow\}$  is not enumerable.*

## Decidable Structures

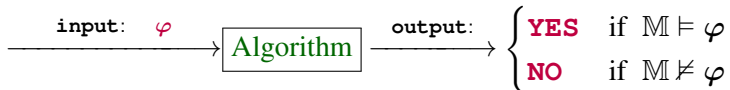
### Definition (Decision Problem for a Structure)

Fix a structure  $\langle \mathbb{M}; \mathcal{L} \rangle$ .

Input: a first-order  $\mathcal{L}$ -sentence  $\varphi$ . Output:  $\begin{cases} \text{YES} & \text{if } \mathbb{M} \models \varphi \\ \text{NO} & \text{if } \mathbb{M} \not\models \varphi \end{cases}$

### Definition (Decidable Structure)

A structure is decidable if its decision problem is algorithmically solvable.



## Enumerability in Structures

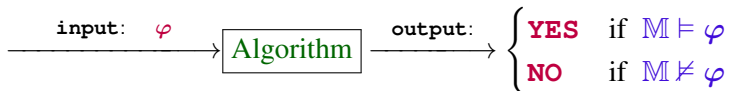


Theorem (Enumerable Structures are Decidable)

*If  $\mathbb{M}$  is an enumerable structure, then it is decidable.*

Proof.

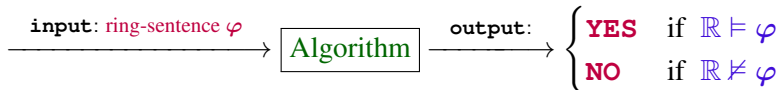
If  $\{\varphi \mid \mathbb{M} \models \varphi\}$  is enumerable, then so is its complement  $\{\psi \mid \mathbb{M} \not\models \psi\}$  because  $\{\psi \mid \mathbb{M} \not\models \psi\} = \{\psi \mid \mathbb{M} \models \neg\psi\}$ . ■



## Tarski's Theorems

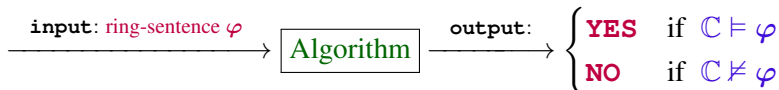
### Theorem (Decidability of the Real (Ordered) Field)

*The structure  $\langle \mathbb{R}; 0, 1, -, \iota', +, \times, \leq \rangle$  is decidable.*



### Theorem (Decidability of the Complex Field)

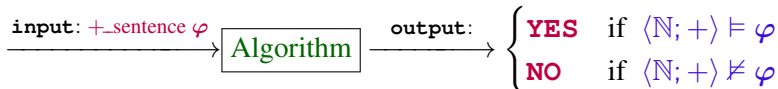
*The structure  $\langle \mathbb{C}; 0, 1, -, \iota', +, \times \rangle$  is decidable.*



## Arithmetics of Presburger and Skolem

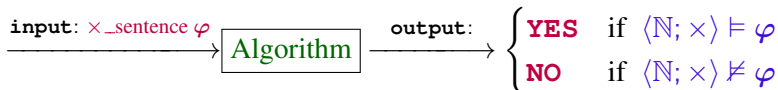
### Theorem (Presburger 1929)

*The structure  $\langle \mathbb{N}; 0, 1, +, \leq \rangle$  is decidable.*



### Theorem (Skolem 1930)

*The structure  $\langle \mathbb{N}; 0, 1, \times \rangle$  is decidable.*

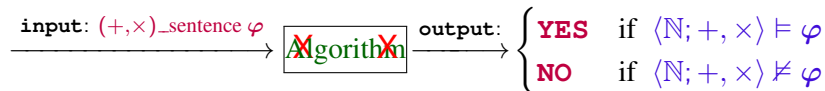




## Full Arithmetic $\langle \mathbb{N}; +, \times \rangle$

Theorem (Gödel's Incompleteness 1931)

The structure  $\langle \mathbb{N}; 0, 1, +, \times, \leq \rangle$  is *not* decidable.



### Corollary

The structure  $\langle \mathbb{Z}; 0, 1, -, +, \times, \leq \rangle$  is *undecidable* too.

### Proof.

$\mathbb{N}$  is definable in it by the formula  $0 \leq x$ . ■

## THE END

Corollary (J. Robinson 1949)

*The structure  $\langle \mathbb{Q}; 0, 1, -, i', +, \times, \leq \rangle$  is **undecidable** too.*

Corollary

*The structure  $\langle \mathbb{C}; 0, 1, -, i', e^x, +, \times \rangle$  is **undecidable** too.*

---

---

Problem (Open — Tarski)

*Is the Real Exponential Field  $\langle \mathbb{R}; 0, 1, -, i', e^x, +, \times, \leq \rangle$  decidable or not?*