Logic in Computation and Computation in Logic

Saeed Salehi

University of Tabriz

http://SaeedSalehi.ir/

The International Conference On Contemporary Issues in Computer and Information Science
29–31 May 2012, IASBS, Zanjan, Iran

∗Dedicated to ALAN TURING in his Centenary Year 2012∗

Hilbert's Entscheidungsproblem = Decision Problem

Finding an ALGORITHM (or AL-KHWARIZMI):
Input: A (Mathematical) Statement.
Output: *YES* (if universally valid) *NO* (if not always valid).

How to write (code) mathematical statements (as input strings)?
Example from Al-Khwarizmi: If from a square, I subtract four of its roots and then take one-third of the remainder, finding this equal to four of the roots, the square will be 256.

Modern Notation: If I have $\frac{1}{3}(x^2 - 4x) = 4x$, then $x^2 = 256$.

More Modern: $\forall x[\frac{1}{3}(x^2 - 4x) = 4x \longrightarrow x^2 = 256]$.

This holds in the domain $\mathbb{N} - \{0\} = \{1, 2, 3, \cdots\}$ (but not in $\mathbb{N}$).

Indeed, $\mathbb{N} \models \forall x[\frac{1}{3}(x^2 - 4x) = 4x \longrightarrow x = 16 \vee x = 0]$.

Entscheidungsproblem = Decision Problem (Hilbert 1928)

Finding an ALGORITHM (or AL-KHWARIZMI):

Input: A (Mathematical) Statement.

Output: *YES* (if universally valid) *NO* (if not always valid).

How to write (code) mathematical statements?

Another Example from Al-Khwarizmi: What is the square which combined with ten of its roots will give a sum total of 39?

Modern Notation: What is (are) the solution(s) of $x^2 + 10x = 39$?

More Modern: $\forall x[x^2 + 10x = 39 \longrightarrow x = 3]$.

This holds in $\mathbb{N}$ but not in $\mathbb{Z}$:

$\mathbb{N} \models \forall x[x^2+10x = 39 \rightarrow x = 3], \mathbb{Z} \not\models \forall x[x^2+10x = 39 \rightarrow x = 3]$.

Indeed, $\mathbb{Z} \models \forall x[x^2 + 10x = 39 \longrightarrow x = 3 \vee x = -13]$.

First–Order Logic (SYNTAX)

Fix a set of primitive constant, function, or relation symbols.
We will use constants 0, 1; the functions $+, \cdot$; the relations $<, \leqslant$.
Terms are constructed from variables and constants by successive application of function symbols.
Examples: $0+x$, $1\cdot(x+y)$, $(x\cdot x)+y$, algebraic expressions
Atomic Formulas are relations (including $=$) between terms:

$t=u$ or $t<u$ or $t\leqslant u$.

Formulas:

- Atomic Formulas
- $\varphi\wedge\psi$, $\varphi\vee\psi$, $\varphi\rightarrow\psi$
- $\neg\varphi$ (not φ)
- $\exists x\varphi(x)$, $\forall x\varphi(x)$

Examples:

$\forall x\exists y[x=2y\vee x=2y+1]$, $\exists x\forall y[x+y=y]$,
$\forall x[x+u=x]$, $\forall y[y\cdot u=u]$, $\forall z[z\cdot u=z]$, $\exists z[z+x=y]$, $\cdots$

First–Order Logic (Semantics)

Fix a domain: a set to whose members the variables refer.
We will use the sets of numbers:

Natural ($\mathbb{N}$), Integer ($\mathbb{Z}$), Rational ($\mathbb{Q}$), Real ($\mathbb{R}$), Complex ($\mathbb{C}$).

Tarski's Definition of Truth defines satisfiability of a formula in a structure (by induction).

Examples:

- $\triangleright$ $\mathbb{N} \not\models \forall x \exists y (x + y = 0)$ but $\mathbb{Z} \models \forall x \exists y (x + y = 0)$.
- $\triangleright$ $\mathbb{Z} \not\models \forall x (x \neq 0 \rightarrow \exists y [x \cdot y = 1])$ but $\mathbb{Q} \models \forall x (x \neq 0 \rightarrow \exists y [x \cdot y = 1])$.
- $\triangleright$ $\mathbb{Q} \not\models \forall x (0 \leqslant x \rightarrow \exists y [y \cdot y = x])$ but $\mathbb{R} \models \forall x (0 \leqslant x \rightarrow \exists y [y \cdot y = x])$.
- $\triangleright$ $\mathbb{R} \not\models \exists x (x \cdot x + 1 = 0)$ but $\mathbb{C} \models \exists x (x \cdot x + 1 = 0)$.

Hilbert's Entscheidungsproblem = Decision Problem (Again)

Finding an Algorithm (or Al-Khwarizmi):

Input: A First–Order Sentence.

Output: *YES* (if universally valid) *NO* (if not always valid).

The history goes back to even G. Leibniz in the 17^{th} century.

Theorem (Gödel's Completeness Theorem 1929)

The set of (universally) valid first–order sentences is computably enumerable (i.e., listable by an algorithm).

Computably Enumerable set A: an (input-free) algorithm $\mathcal{P}$ lists all members of A; i.e., $A = \texttt{output}(\mathcal{P})$.

Computably Decidable set A: an algorithm $\mathcal{P}$ decides on any input x whether $x \in A$ (outputs $\texttt{YES}$) or $x \notin A$ (outputs $\texttt{NO}$).

Gödel's Completeness Theorem

From An Axiomatization of (Logically) Valid First–Order Formulas:

- $\alpha \rightarrow (\beta \rightarrow \alpha)$
- $(\neg\beta \rightarrow \neg\alpha) \rightarrow (\alpha \rightarrow \beta)$
- $[\alpha \rightarrow (\beta \rightarrow \gamma)] \rightarrow [(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma)]$
- $\forall x\varphi(x) \rightarrow \varphi(t)$
- $\varphi \rightarrow \forall x\varphi$ [x is not free in φ]
- $\forall x(\varphi \rightarrow \psi) \rightarrow (\forall x\varphi \rightarrow \forall x\psi)$

With the Modus Ponens Rule: $$\frac{\varphi, \quad \varphi \rightarrow \psi}{\psi}$$

All the Universally Valid Formulas CAN BE GENERATED.

Note: $A \vee B = (\neg A) \rightarrow B$, $A \wedge B = \neg[A \rightarrow (\neg B)]$, $\exists x\varphi = \neg\forall x\neg\varphi$.

Valid Formulas: Enumerable Not Decidable

Example:
The Following Formulas can be seen to be [equivalently]
(1) Universally Valid (in every structure) and
(2) Deducible in First–Order Logic from the Axioms by the Rule:

- $\forall\mathbf{x}\big([(\alpha\to\beta)\to\alpha]\to\alpha\big)$
- $\exists y\forall x\big(\varphi(y)\to\varphi(x)\big)$

Theorem (Church & Turing (1936))

The Decision Problem is NOT algorithmically solvable.

So, Hilbert's Entscheidungsproblem is (algorithmically) Un–Solvable; though he did expect an algorithm.

► A Good Outcome: Introducing Turing Machines – the grand grandfather of today's modern computers.

Universally Valid Formulas: Semi-Decidable Not Decidable

(Semi-Decidable) $\not\equiv$ (Decidable)

Post–Kleene's Theorem: A Set is Computably Decidable if and only if Both it and its Complement are Computably Enumerable.

Thus, though the set of Universally Valid formulas is Computably Enumerable, there is no algorithm for deciding whether a given first–order formula is valid in all structures or not.

What about validity of formulas in one particular structure?

Decision Problem for the Structure $(\mathfrak{M},\mathcal{L})$:

Input: A First–Order Sentence φ in the Language $\mathcal{L}$.

Output: *YES* (if $\mathfrak{M}\models\varphi$) *NO* (if $\mathfrak{M}\not\models\varphi$).

Decidability of Mathematical Structures

We study the Decision Problem for the Following Structures (domain, language)'s:

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	$\langle\mathbb{N},<\rangle$	$\langle\mathbb{Z},<\rangle$	$\langle\mathbb{Q},<\rangle$	$\langle\mathbb{R},<\rangle$	–
$\{+\}$	$\langle\mathbb{N},+\rangle$	$\langle\mathbb{Z},+\rangle$	$\langle\mathbb{Q},+\rangle$	$\langle\mathbb{R},+\rangle$	$\langle\mathbb{C},+\rangle$
$\{\cdot\}$	$\langle\mathbb{N},\cdot\rangle$	$\langle\mathbb{Z},\cdot\rangle$	$\langle\mathbb{Q},\cdot\rangle$	$\langle\mathbb{R},\cdot\rangle$	$\langle\mathbb{C},\cdot\rangle$
$\{+,<\}$	$\langle\mathbb{N},+,<\rangle$	$\langle\mathbb{Z},+,<\rangle$	$\langle\mathbb{Q},+,<\rangle$	$\langle\mathbb{R},+,<\rangle$	–
$\{+,\cdot\}$	$\langle\mathbb{N},+,\cdot\rangle$	$\langle\mathbb{Z},+,\cdot\rangle$	$\langle\mathbb{Q},+,\cdot\rangle$	$\langle\mathbb{R},+,\cdot\rangle$	$\langle\mathbb{C},+,\cdot\rangle$
$\{\cdot,<\}$	$\langle\mathbb{N},\cdot,<\rangle$	$\langle\mathbb{Z},\cdot,<\rangle$	$\langle\mathbb{Q},\cdot,<\rangle$	$\langle\mathbb{R},\cdot,<\rangle$	–
$\{+,\cdot,<\}$	$\backslash$	$\backslash$	$\backslash$	$\backslash$	–

Definability of $<$ By $+$ and $\cdot$

Order Is Definable By Addition And Multiplication.

Why not consider $\{+,\cdot,<\}$?
The Order Relation $<$ is Definable by $+$ and $\cdot$ as

- in $\mathbb{N}$: $a \leqslant b \iff \exists x\,(x + a = b)$.
- in $\mathbb{R}$: $a \leqslant b \iff \exists x\,(x \cdot x + a = b)$.

for $\mathbb{Z}$ Use Lagrange's Four Square Theorem; Every Natural (Positive) Number Can Be Written As A Sum Of Four Squares.

- in $\mathbb{Z}$: $a \leqslant b \iff \exists \alpha, \beta, \gamma, \delta\,(a + \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = b)$.

for $\mathbb{Q}$ Lagrange's Theorem Holds Too: $0 \leqslant r = m/n = (mn)/n^2 = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)/n^2 = (\alpha/n)^2 + (\beta/n)^2 + (\gamma/n)^2 + (\delta/n)^2$.

- in $\mathbb{Q}$: $a \leqslant b \iff \exists \alpha, \beta, \gamma, \delta\,(a + \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = b)$.

$\boxed{a < b \iff a \leqslant b \wedge a \neq b}$ $\boxed{a \leqslant b \iff a < b \vee a = b}$

Order $<$

The Theory of Order is Decidable in Number Domains.

The Theory of Order in $\mathbb{Q}$ and $\mathbb{R}$ Characterized:

Linear Dense Order Without End-Points

• $\forall x, y(x < y \to y \not< x)$	Anti-Symmetric
• $\forall x, y, z(x < y < z \to x < z)$	Transitive
• $\forall x, y(x < y \vee x = y \vee y < x)$	Linear
• $\forall x, y(x < y \to \exists z[x < z < y])$	Dense
• $\forall x \exists y(x < y)$	No Last Point
• $\forall x \exists y(y < x)$	No Least Point

These Axiomatize the Whole Theory of $\langle \mathbb{Q}, < \rangle$ and $\langle \mathbb{R}, < \rangle$.

Order $<$

The Theory of Order is Decidable in Number Domains.

The Theory of Order in $\mathbb{N}$ Characterized:

Linear Discrete Order Without Last-Point With Least-Point

In the Language $\{0, S, <\}$ where $S(x) = x + 1$ is the Successor Function, Definable by $<$: $S(x) = y \iff \forall z(x < z \leftrightarrow y \leqslant z)$.

• $\forall x, y(x < y \to y \not< x)$	Anti-Symmetric
• $\forall x, y, z(x < y < z \to x < z)$	Transitive
• $\forall x, y(x < y \vee x = y \vee y < x)$	Linear
• $\forall x, y(x < S(y) \leftrightarrow x = y \vee x < y)$	Discrete Order
• $\forall x(x \neq 0 \to \exists y[x = S(y)])$	Successor
• $\forall x(x \not< 0)$	Least Point

These Axiomatize the Whole Theory of $\langle \mathbb{N}, 0, S, < \rangle$.

Order $<$

The Theory of Order is Decidable in Number Domains.

The Theory of Order in $\mathbb{Z}$ Characterized:

Linear Discrete Order Without Least or Last Points

In the Language $\{S, <\}$ where $S(x) = x + 1$ is the Successor Function, Definable by $<$: $S(x) = y \iff \forall z(x < z \leftrightarrow y \leqslant z)$.

• $\forall x, y(x < y \rightarrow y \nless x)$	Anti-Symmetric
• $\forall x, y, z(x < y < z \rightarrow x < z)$	Transitive
• $\forall x, y(x < y \vee x = y \vee y < x)$	Linear
• $\forall x, y(x < S(y) \leftrightarrow x = y \vee x < y)$	Discrete Order
• $\forall x \exists y(x = S(y))$	Successor
• $\forall x \exists y(y < x)$	No Least Point

These Axiomatize the Whole Theory of $\langle \mathbb{Z}, S, < \rangle$.

Addition $(+)$; **Addition and Order** $(+,<)$

The Theory of Addition and Order $\{+,<\}$ is Decidable.

Decidability of $\langle\mathbb{N},+,<\rangle$ and $\langle\mathbb{Z},+,<\rangle$ was proved by Presburger in 1929 (and by Skolem in 1930). The Theory $\langle\mathbb{N},+\rangle$ is called Presburger Arithmetic. Let us recall that $<$ is Definable in $\langle\mathbb{N},+\rangle$: $x<y \iff \exists z(z+z\neq z \wedge z+x=y)$.

Multiplication $(\cdot)$

The Theory of Multiplication $\{\cdot\}$ is Decidable.

Decidability of the Theories $\langle\mathbb{N},\cdot\rangle$ and $\langle\mathbb{Z},\cdot\rangle$ was announced by Skolem in 1930 (called Skolem Arithmetic).

Decidable Theories

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	?	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–

The Theory $\langle\mathbb{N},+,\cdot\rangle$ Was Expected to be Decidable as well!

Theorem (Gödel's Incompleteness Theorem (1931))

The Theory $\langle\mathbb{N},+,\cdot\rangle$ *Is NOT Decidable.*
(Not Even Computably Enumerable!)

Un-Decidable Theories Come In

Decidability and Un-Decidability of Addition and Multiplication

Since $\mathbb{N}$ Is Definable in $\langle \mathbb{Z}, +, \cdot \rangle$ (by Lagrange’s Theorem) and in $\langle \mathbb{Q}, +, \cdot \rangle$ (by Robinson’s Result), The Theories $\langle \mathbb{Z}, +, \cdot \rangle$ and $\langle \mathbb{Q}, +, \cdot \rangle$ are Un-Decidable as well. Though, Tarski showed (in 1936) that The Theories $\langle \mathbb{R}, +, \cdot \rangle$ and $\langle \mathbb{C}, +, \cdot \rangle$ Are Decidable.

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	?	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+,\cdot\}$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	Δ_1	Δ_1

What About $\{\cdot,<\}$?

A. Tarski & J. Robinson

The Theory $\langle\mathbb{R},\cdot,<\rangle$ Is Decidable by Tarski’s Result (1931).
The Theory $\langle\mathbb{N},\cdot,<\rangle$ Is Un-Decidable by Robinson’s Result (1949): $+$ is Definable in $\langle\mathbb{N},\cdot,<\rangle$ by Tarski’s Identity:

$$x+y=z \iff (x{=}y{=}z{=}0)\bigvee \Big[z\neq 0\wedge S(x\cdot z)\cdot S(y\cdot z)=S(z\cdot z\cdot S(x\cdot y))\Big].$$

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	?	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+,\cdot\}$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	Δ_1	Δ_1
$\{\cdot,<\}$	$\cancel{\Delta}_1$	?	?	Δ_1	–

The Theories $\langle\mathbb{Q},\cdot\rangle$, $\langle\mathbb{Z},\cdot,<\rangle$ and $\langle\mathbb{Q},\cdot,<\rangle$?

They Are Not Mentioned Anywhere... Missing in the Literature?

Addition Is Definable in $\langle\mathbb{N},\cdot,<\rangle$ by Tarski's Identity, because in $\mathbb{N}$ we have : $x+y=0 \iff x=y=0$.

This Does Not Hold in $\mathbb{Z}$. So, The Relation $x=-y$ Should be Defined in $\langle\mathbb{Z},\cdot,<\rangle$ For Defining $+$:

$$x=-y \iff S(x)\cdot S(y)=S(x\cdot y).$$

Again Note That S Is Definable by $<$:

$$S(x)=y \iff \forall z\big(x<z \leftrightarrow y=z \vee y<z\big).$$

Another Way of Defining $x=-y$ in $\{\cdot\}$ Is:

$$x=-y \iff (x=y=0)\vee(x\neq y \wedge x\cdot x=y\cdot y).$$

The Theories $\langle\mathbb{Q},\cdot\rangle$, $\langle\mathbb{Z},\cdot,<\rangle$ and $\langle\mathbb{Q},\cdot,<\rangle$?

Theorem (Un-Decidability of $\langle\mathbb{Z},\cdot,<\rangle$)

Addition $+$ is Definable in $\langle\mathbb{Z},\cdot,<\rangle$; so $\langle\mathbb{Z},\cdot,<\rangle$ is Un-Decidable.

Proof: $x+y=z \iff \big(z=0\wedge S(x)\cdot S(y)=S(x\cdot y)\big)\bigvee$
$\big(z\neq 0\wedge S(x\cdot z)\cdot S(y\cdot z)=S(z\cdot z\cdot S(x\cdot y))\big)$. □

Theorem (Decidability of $\langle\mathbb{Q},\cdot\rangle$ and $\langle\mathbb{Q},\cdot,<\rangle$)

The Theories of $\langle\mathbb{Q},\cdot\rangle$ and $\langle\mathbb{Q},\cdot,<\rangle$ Are Decidable.

Corollary: Addition $+$ Is NOT Definable in $\langle\mathbb{Q},\cdot,<\rangle$.
Proof. Because $\langle\mathbb{Q},\cdot,<\rangle$ is Decidable But $\langle\mathbb{Q},+,\cdot,<\rangle$ is Un-Decidable. □

The Happy Ending ...

Seeing The Whole Picture

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+,\cdot\}$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	Δ_1	Δ_1
$\{\cdot,<\}$	$\cancel{\Delta}_1$	$\cancel{\Delta}_1$	Δ_1	Δ_1	–

Thanks A Lot To The Organizers

Thank You For Listening