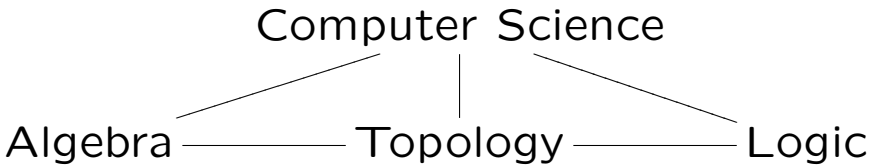
# From Logic to Computer Science back and forth

Antonino Salibra

Università Ca'Foscari Venezia

# Logic




- Starting with Logic: Formal Language of Mathematics
  (i) – Classical Propositional Calculus ("and", "or", "not")
  – Boolean Algebras (1847)
  – The propositional calculus is too weak for formalising Mathematics.

  (ii) The language of Mathematics:
  – Some odd natural number divides 122:

$$\exists x(\text{Odd}(x) \wedge x \text{ divides } 122)$$

  – Every triangle admits an acute angle:

$$\forall x(\text{triangle}(x) \rightarrow \exists y(\text{acute-angle}(y) \wedge y \text{ angle-of } x))$$

  (iii) Mathematical Logic studies mathematical theories through the formal language representing Mathematics.

# Logic

- Starting with Logic: Formal Proofs

(i) Some Propositional Rules:

$$\frac{\begin{array}{cc}\vdots & \vdots \\ A \to B & A\end{array}}{B} \qquad \frac{\begin{array}{cc}\vdots & \vdots \\ A & B\end{array}}{A \wedge B} \qquad \frac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \to B}$$

(ii) Some Rules for Quantifiers:

$$\frac{\begin{array}{c}\vdots \\ P(a)\end{array}}{\exists x P(x)} \qquad \frac{\begin{array}{c}\vdots \\ P(x)\end{array}}{\forall x P(x)}$$ [variable $x$ not used in other assumptions]

(iii) A proof is an algorithm! Computer Science comes in!

(iv) We now have very sophisticated theorem provers. They help mathematicians in their work.
Two years ago...

# Logic

- Starting with Logic: Semantics

(i) What is a model?

$$\forall x R(x,x); \qquad \forall x \forall y (R(x,y) \rightarrow R(y,x))$$

A model satisfying the two axioms is any set $A$ with a binary relation $R \subseteq A \times A$, which is reflexive and symmetric.

(ii) $$\forall x \forall y . x + (y + 1) = (x + y) + 1$$

A model satisfying the two axioms is the model of arithmetics.
But not only that! Consider the truth values $\{0, 1\}$ and interpret the symbol "+" as "or".

(iii) Many different models for the same sentences.

# Logic

- Starting with Logic: Semantics

(i) *Second-Order Logic* (Frege-Peano 1890)

$$\forall P(P(0) \wedge \forall x(P(x) \rightarrow P(x+1)) \rightarrow \forall x P(x)).$$

We do not have "sufficient powerful" logical deduction rules for second-order logic.
Second-order Peano Arithmetics is categorical: Only the model of natural numbers.

(ii) *First-Order Logic* (FOL)

$$P(0) \wedge \forall x(P(x) \rightarrow P(x+1)) \rightarrow \forall x P(x)$$

where $P(x)$ is an arbitrary formula in the first-order language of arithmetics.

(iii) Second-order Logic is categorical, First-order Logic is not categorical

(iv) Gödel's Completeness Theorem for first-order logic (1930):

$$\text{Ax} \vdash \phi \text{ iff, } \forall \text{ model } \mathbf{M},\ \mathbf{M} \models \phi$$

# Foundation of Mathematics

- Starting with Sets:

  (i) New mathematics in XIXth century:
  Non-Euclidean Geometries, High-order Functions, etc.
  Mathematicians start to work with infinite sets of functions,...

  (ii) Set Theory as Foundation of Mathematics (Cantor 1870)

$$x \in Y$$

  (iii) Different types of Infinite, Cardinal Numbers (Cantor)

  (iv) Sets are defined by properties written in arbitrary languages:

$$Y = \{x : P(x)\}$$

  Russel's Paradox and Self-Reference (1900):

$$R = \{x : x \notin x\}; \qquad R \in R \Leftrightarrow R \notin R$$

  Then SET THEORY is inconsistent.

  (v) Axiomatic Set Theory is defined in first-order logic.
  - Many different models. Independence of Continuum Hypothesis.
  - Is Axiomatic Set Theory consistent? Nobody knows and, after Godel, nobody will know!

# Computability

- Starting with Algorithms (after Russel):

(i) Axiomatic Approach to Mathematics (Hilbert, Grundlagen der Geometrie 1899)

(ii) Infinite sets are dangerous after Russel's paradox.
INFINITE = NOT FINITE is not dangerous

(iii) Hilbert's Program: formal languages + axioms, and formal proofs to show that the system is consistent.

(iv) Curry (Combinatory Logic), Church (Lambda Calculus), Kleene (Recursive Equations), Turing (Turing Machines),...All these systems are equivalent. They compute the same functions.
COMPUTER SCIENCE STARTS!

(v) We go to study the most important theorem of XXth century: Gödel's Incompleteness Theorem.

# Russel and Self-Reference

**Lemma 1** *(Russel Diagonalisation Lemma) Let $A$ be a set, $R \subseteq A \times A$ be a binary relation and $\neg R = A \times A \setminus R$. Then*

$$\neg\exists a \forall x (aRx \text{ iff } \neg xRx).$$

Meaning: each element $b \in A$ codifies (is a name of) the unary relation $\{x \in A : bRx\}$. The unary relation $\{x \in A : \neg xRx\}$ has no name.

Self-reference:

- Programs P working on data which are programs

- Formulas specifying properties of formulas

# The shortest proof of Gödel's Incompleteness

## Tarski's Theorem on Undefinability of Truth

**Theorem 1** *Let* $\mathbf{A}$ *be a model of a logic such that there exists a bijective map*

$$\ulcorner\ \urcorner : \mathrm{FORM}_1 \longrightarrow A \text{ (}\textit{Gödel numbering}\text{)}.$$

*Let* $\mathbf{Truth} = \{(\ulcorner\varphi(x)\urcorner, a) : \mathbf{A} \models \varphi(a)\}$.

1. *The complement of* $\mathbf{Truth}$ *is not representable in* $\mathbf{A}$.
2. *If* $\mathbf{A}$ *is complemented, then* $\mathbf{Truth}$ *is also not representable in* $\mathbf{A}$.

**Proof** 1. By the diagonalisation lemma:

$$\neg\exists a\forall b.(a,b) \in \mathbf{Truth} \text{ iff } (b,b) \notin \mathbf{Truth}.$$

If the complement of $\mathbf{Truth}$ were representable in $\mathbf{A}$ by a formula $\psi(x,y) \in \mathrm{FORM}_2$, then the formula $\psi(x,x) \in \mathrm{FORM}_1$ would represent the unary relation $\{b : (b,b) \notin \mathbf{True}\}$. Thus, the Gödel numbering $\ulcorner\psi(x,x)\urcorner$ would contradicts the diagonalisation lemma:

$$(\ulcorner\psi(x,x)\urcorner, b) \in \mathbf{Truth} \text{ iff } (b,b) \notin \mathbf{Truth}.$$

2. If $\mathbf{True}$ were representable, then the complement of $\mathbf{Truth}$ would be. $\square$

# The shortest proof of Gödel's Incompleteness

**Corollary 1** *If* $\mathbf{A}$ *is a (complemented) model, where all semidecidable sets are representable, then* $\mathbf{Truth}$ *is not decidable (semidecidable).*

**Corollary 2** *The arithmetical truths are not semidecidable.*

No hope to prove all arithmetical truths!
Mathematics is more complex than computer science.

**Corollary 3** *The Halting Problem is not decidable.*

**Proof** Consider the set of formulas $P_n$, where $P$ is a program and $n \geq 1$ is a natural number. We define a model for this logical language as follows:

Universe: the set $\mathcal{P}$ of all programs.

Interpretation: $P_n^{\mathcal{P}} = \{(Q_1, \ldots, Q_n) : P{\downarrow}(Q_1, \ldots, Q_n)\}$.

Then $\mathbf{Truth} = \{(P_1, Q) : P{\downarrow}Q\}$ is not decidable! $\square$

# Provability $\vdash$ against Truth $\models$

## First Gödel's incompleteness theorem

**Theorem 2** *Let* $\mathbf{A}$ *be a complemented model of a logic* $\vdash$ *such that there exists a bijective map*

$$\ulcorner\ \urcorner : \mathrm{FORM}_1 \longrightarrow A \text{ (}\textit{Gödel numbering}\text{)}.$$

*If* $\mathbf{Prov} = \{(\ulcorner\psi(x)\urcorner, a) : \vdash \psi(a)\}$ *is representable in* $\mathbf{A}$*, then there exists a formula* $\varphi(x)$ *such that*

1. $\mathbf{A} \models \varphi(\ulcorner\varphi\urcorner)$ *iff* $\nvdash \varphi(\ulcorner\varphi\urcorner)$ *(intuitive meaning:* $\varphi(\ulcorner\varphi\urcorner)$ *says 'I am not provable') so that* $\mathbf{Prov} \neq \mathbf{Truth}$*.*
2. *If the system* $\vdash$ *is consistent (that is, we can prove only true sentences:* $\mathbf{Prov} \subseteq \mathbf{Truth}$*), then* $\mathbf{A} \models \varphi(\ulcorner\varphi\urcorner)$ *and* $\varphi(\ulcorner\varphi\urcorner)$ *is not provable. The formula* $\neg\varphi(\ulcorner\varphi\urcorner)$*, which says '*$\varphi(\ulcorner\varphi\urcorner)$ *is provable', is also not provable.*

**Proof** 1. Let $Prov(x, y)$ be a formula such that

$$\mathbf{A} \models Prov(\ulcorner\psi(x)\urcorner, a) \text{ iff } \vdash \psi(a).$$

Define $\varphi \equiv \neg Prov(x, x)$. Then we have:

$$\mathbf{A} \models \varphi(\ulcorner\varphi\urcorner) \text{ iff } \nvdash \varphi(\ulcorner\varphi\urcorner).$$

# I can not prove my consistency

## Second Gödel's incompleteness theorem

The formula $(0 = 1)$ is false. Then the consistency of provability $\vdash$ can be expressed by the formula

$$Cons \equiv \neg Prov(\ulcorner(0 = x)\urcorner, 1).$$

**Theorem 3** *Let* $\mathbf{A}$ *be a complemented model of a logic* $\vdash$ *such that there exists a Gödel numbering*

$$\ulcorner\ \urcorner : \mathrm{FORM}_1 \longrightarrow A$$

*and* $\mathbf{Prov} = \{(\ulcorner\psi(x)\urcorner, a) : \vdash \psi(a)\}$ *is representable in* $\mathbf{A}$.
*If the system* $\vdash$ *can internalise the proof of the first incompleteness theorem* $\vdash Cons \to \varphi(\ulcorner\varphi\urcorner)$, *then* $\nvdash Cons$ *(where* $\varphi(\ulcorner\varphi\urcorner)$ *means 'I am not provable').*

**Proof**

If $\vdash Cons$ and $\vdash Cons \to \varphi(\ulcorner\varphi\urcorner)$ then by Modus Ponens $\vdash \varphi(\ulcorner\varphi\urcorner)$. This contradicts First Incompleteness Theorem. $\square$

THIS IS THE END OF HILBERT'S PROGRAM.

MATHEMATICS IS NOT SAFE.

COMPUTER SCIENCE IS BETTER!