Logic for Computer Science

Summer semester
2019-2020

LECTURE 13: INCOMPLETENESS

Lectures: LORENZO CLEMENTE
Tutorials: DARIA WALUKIEWICZ, JACEK CHRZASZCZ, JĘDRZEJ KOŁODZIEJSKI
Labs: DARIA, JACEK + PIOTR HOFMAN

SUMMARY

- Axiomatising arithmetic $Th(\mathbb{N}, +, *)$.
- Undecidability of arithmetic.
- Consequences:
  - Gödel's incompleteness result.
  - No proof system for second-order logic.
- Summary of the course.
- Further directions.

THE STANDARD MODEL of ARITHMETIC

$(\mathbb{N}, 0, s, +, *)$ our signature Σ containing:

0 : zero

s : successor function

$+$: addition

$*$: multiplication

$TR(\mathbb{N}) = \{\varphi \in Th(\Sigma) \mid \mathbb{N} \models \varphi\}$ first-order theory of $\mathbb{N}$.

GOAL 1: Find a set of axioms Δ : $Th(\Delta) = Th(\mathbb{N})^*$.

GOAL 2: Solve the decision problem $\varphi \overset{?}{\in} Th(\mathbb{N})$.

$^*Th(\Delta) = \{\varphi \mid \Delta \models \varphi\}$

GOAL 1: FIND Δ s.t. $Th(\Delta) = Th(\mathbb{N})$

- Trivial answer $\Delta = Th(\mathbb{N})$. Refined goal: Δ recursive ($\varphi \overset{?}{\in} \Delta$ decidable).
- Consider Hilbert's FO axioms A1 – A9 plus:

$$\left.\begin{array}{ll} P1: & \forall x,y.\ s(x) = s(y) \to x = y. \\ P2: & \forall x.\ s(x) \neq 0. \\ P3: & \forall x.\ x \neq 0 \to \exists y.\ x = s(y) \end{array}\right] s$$

$$\left.\begin{array}{ll} P4: & \forall x.\ x + 0 = x. \\ P5: & \forall x,y.\ x + s(y) = s(x+y). \end{array}\right] +$$

$$\left.\begin{array}{ll} P6: & \forall x.\ x * 0 = 0. \\ P7: & \forall x,y.\ x * s(y) = x * y + x. \end{array}\right] *$$

Robinson's arithmetic '50

RA

(sometimes called Q)

finitely many axioms!

RA is very weak: $1+2 = 2+1 \in Th(RA)$, but $\forall x,y.\ x+y = y+x \notin Th(RA)$!

What is missing? INDUCTION.

GOAL 1: FIND Δ s.t. $\mathrm{Th}(\Delta) = \mathrm{Th}(\mathbb{N})$

Solution 1: Add an infinite set of formulas, one for each φ:

$$\boxed{I_{FO} : (\forall x.\ \varphi(x) \to \varphi(s(y))) \to \varphi(0) \to \forall x.\ \varphi(x).}$$

$PA = RA + \underbrace{I_{FO}}_{\text{infinite}}$, $\mathrm{Th}(PA)$: (first-order) Peano arithmetic*.

- PA consistent: $\mathbb{N} \models PA$. - $\forall x, y.\ x+y = y+x \in \mathrm{Th}(PA)$.
- $\mathcal{A} \models PA \overset{?}{\Rightarrow} \mathcal{A} \underset{\text{isomorphism}}{\cong} \mathbb{N}$: No! $\to$ Skolem-Löwenheim.
- $\mathcal{A} \models PA \overset{?}{\Rightarrow} \mathcal{A} \underset{\text{elementarily equivalent}}{\equiv_{FO}} \mathbb{N}$: No! $\to$ Compactness (non-standard models).
- $\mathrm{Th}(PA) \overset{?}{\equiv} \mathrm{Th}(\mathbb{N})$. No! $\to$ Gödel's syntactic incompleteness theorem.

("strengthened Ramsey theorem" $\in \mathrm{Th}(\mathbb{N}) \setminus \mathrm{Th}(PA)$ (Paris-Harrington '77).)

* In fact previously discovered by Dedekind, confirming Stigler's LAW of EPONIMY.

GOAL 1: FIND Δ s.t. $Th(\Delta) = Th(\mathbb{N})$

Solution 2: add a second-order induction axiom:

$$\boxed{I_{SO} : \forall P^{(1)}. \left(\forall x. P(x) \to P(s(y))\right) \to P(0) \to \forall x. P(x).}$$

- Consistent: $\mathbb{N} \models RA + I_{SO}$.
- $\mathbb{A} \models RA + I_{SO} \Rightarrow \mathbb{A} \overset{\text{isomorphism}}{\cong} \mathbb{N}$.
- $Th(RA + I_{SO}) \overset{?}{=} Th(\mathbb{N})$? YES!
  - $\hookrightarrow = \{\varphi \mid RA + I_{SO} \models \varphi\}$
- ... $Th(\mathbb{N})$ is undecidable $\Rightarrow$ $\boxed{\text{no sound proof system for SECOND-ORDER LOGIC!}}$

GOAL 2: $Th(\mathbb{N}, 0, s, +, *)$ UNDECIDABLE

Encode finite Tiling: tiles $T \subseteq_{fin} \mathbb{N}$, $H, V \subseteq T \times T$, $a, b \in T$.

- natural strict total order $<$ defined as $\varphi_<(x,y) \equiv x \neq y \wedge \exists z \cdot x = y + z$.
- assume there is a formula $Z[x,y]=r$ with 4 free variables z, x, y, r:

$\forall m \in \mathbb{N}\ \forall M \in \mathbb{N}^{m \times m}\ \exists \hat{M} \in \mathbb{N}\ \forall i,j \in \{1, \dots, m\}\ \forall k \in \mathbb{N}$:

$$\boxed{M_{i,j} = k \quad \text{iff} \quad PA, z : \hat{M}, x : i, y : j, r : k \models Z[x,y] = r.}$$

- Tiling: $\varphi \equiv \exists m \cdot \exists M \cdot M[0,0] = a \wedge M[m,m] = b \quad \wedge$

$$\forall x,y \cdot \Big(x < m \rightarrow \bigvee_{(c,d) \in H} M[x,y] = c \wedge M[s(x),y] = d\Big) \quad \wedge$$

$$\Big(y < m \rightarrow \bigvee_{(c,d) \in V} M[x,y] = c \wedge M[x,s(y)] = d\Big).$$

- Correctness: $\mathbb{N} \models \varphi$ iff there is a finite Tiling.

CONSEQUENCES of UNDECIDABILITY of $Th(\mathbb{N})$

Gödel syntactic incompleteness theorem:

For every decidable set of axioms Δ s.t. $\mathbb{N} \models \Delta$ there is φ s.t. $\Delta \not\vdash \varphi$ and $\Delta \not\vdash \neg\varphi$.

Proof: If not, can decide whether $\varphi \in Th(\mathbb{N})$ by finding either a proof of $\underbrace{\Delta \vdash \varphi \text{ or } \Delta \vdash \neg\varphi}$.

iff $\Delta \models \varphi$ or $\Delta \models \neg\varphi$ by semantic completeness

CONSEQUENCES of UNDECIDABILITY of $Th(\mathbb{N})$

No sound & semantically complete proof system for second-order logic.

Proof: Otherwise can decide $\varphi \in Th(\mathbb{N})$ by finding a proof of either $\underbrace{PA + I_{SO} \vdash \varphi \text{ or } PA + I_{SO} \vdash \neg\varphi}$.

$\Leftrightarrow PA + I_{SO} \models \varphi$ or $PA + I_{SO} \models \neg\varphi$ by semantic completeness of FO

$\Leftrightarrow \mathbb{N} \models \varphi$ or $\mathbb{N} \models \neg\varphi$

$\Leftrightarrow$ true by syntactic completeness of $Th(\mathbb{N})$.

Bonus: - $Th(\mathbb{Z}, +, *)$ undecidable (PS.2,7).

- $Th(\mathbb{Q}, +, *)$ undecidable (harder).

REMARKS

- We gave a modern efficient proof based on undecidability of $Th(\mathbb{N})$.
- Gödel proved syntactic incompleteness by constructing $\varphi : \Delta \nvdash \varphi$ and $\Delta \nvdash \neg\varphi$.
- Second incompleteness theorem: PA cannot prove its own consistency.
  (There are proofs of consistency of PA in stronger theories ...)
- Complete & decidable arithmetic theories:

$(\mathbb{N}, +)$ Presburger arithmetic
$(\mathbb{N}, \cdot)$ Skolem arithmetic
$(\mathbb{R}, +, \cdot)$ Tarski algebra
$(\mathbb{C}, +, \cdot)$ Algebraic-closed fields

Building mathematics bottom-up
$\emptyset, \{\,\} \to \mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$
$\longrightarrow$ increasing complexity $\longrightarrow$

But $Th(\mathbb{R}, +, \cdot)$ simpler than $Th(\mathbb{N}, +, \cdot)$.

- Truth in $\mathbb{N}$ vs. provability in PA:
  - "infinitely many primes": true and provable in PA.
  - Gödel, Paris-Harrington, Goodstein: φ true but proved unprovable in PA.
  - Fermat's last theorem: true and not known to be provable in PA.
  - Twin prime conjecture: not known to be true also not known to be unprovable in PA.

GÖDEL'S FUNCTION β

- Goal : express "$Z[x,y]=r$" in $(\mathbb{N}, 0, s, +, *)$.

1) There is a function $\beta : \mathbb{N}\times\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ s.t. $\forall a_1,\dots,a_n\in\mathbb{N}$
$\exists a,b\in\mathbb{N}$ s.t. $\forall i\in\{1,\dots,n\} : \beta(a,b,i)=a_i$.

Proof : $b := (\max(a_1,\dots,a_n,n))!$, $b_i := 1+(i+1)b$.

Consider the system of modular equations :

$$\begin{cases} a \equiv a_1 \pmod{b_1} \\ \vdots \\ a \equiv a_n \pmod{b_n} \end{cases} \Longrightarrow$$

since $b_1,\dots,b_n$ are co-prime, by the Chinese Remainder Theorem there is a solution a.

Let $\beta(a,b,i) := a \bmod b_i$.

2) There is a formula $\varphi_\beta(x,y,z,r)$ defining β : $\forall a,b,c,i\in\mathbb{N}$,
$\mathbb{N}, x:a, y:b, z:i, r:c \models \varphi_\beta(x,y,z,r)$ iff $\beta(a,b,i)=c$.

GÖDEL'S FUNCTION β

- Goal : express "$z[x,y]=r$" in $(\mathbb{N}, 0, s, +, *)$.

3) Compression : let $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be a bijection.

Cantor : $f^{-1}(m,n) := \frac{(m+n)(m+n+1)}{2} + n$.

Let $\chi(r,i) : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be $\chi(r,i) := \beta(f(r), i)$.

Also χ is definable by a formula $\varphi_\chi(x,y,z)$.

4) The matrix $z[x,y]$ encoded as nested arrays :

$z[x,y] = \chi(\chi(z,x), y)$.

This leads to a formula $\varphi(z,x,y,r)$ encoding $z[x,y]=r$.

SUMMARY of the COURSE

- Propositional logic:
  - semantic completeness ($\models \Rightarrow \vdash$).
  - resolution, SAT solvers (DP, DPLL).
  - intuitionistic propositional logic.
    (Curry - Howard Correspondence).
- First-order logic:
  - Normal forms (NNF, PNF, SNF, Skolemisation).
  - FO = Relational algebra.
  - Evaluation in finite structures PSPACE-c. (AC_0 for every fixed formula).
  - Gödel's semantic completeness theorem ($\models \Rightarrow \vdash$).
  - Intuitionistic first-order logic (λ-calculus, dependent types).
  - Compactness theorem.
    - Non-standard models (infinitesimals).
  - Skolem-Löwenheim theorems.
  - Ehrenfeucht-Fraïssé games.

  non axiomatizability

  - Decidable theories (finite model property, quantifier elimination).
  - Undecidability (Church-Turing, Trakhtenbrot), syntactic incompleteness.

SUMMARY of the COURSE

- Second-order logic:
  - Expressive power.
  - No compactness, semantic completeness, Skolem-Löwenheim.
  - Ehrenfeucht-Fraïssé games survive, but "too strong".
  - $\exists SO = NP$ (Fagin).
  - $SO = PH$ (Stockmeyer).
  - $MSO =$ Regular on word models (Büchi-Elgot-Trakhtenbrot)
- Arithmetic:
  - Gödel's syntactic incompleteness theorem.

GOING FURTHER

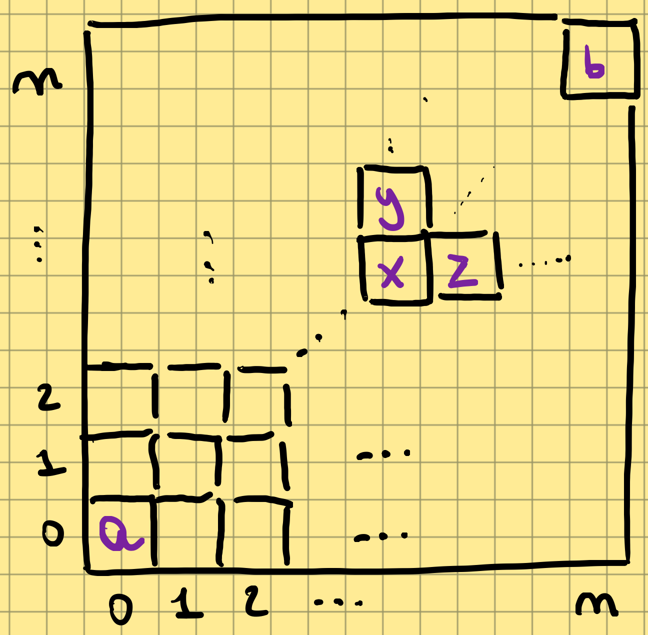
landmark result!

- MSO is decidable on infinite words (Büchi '62) and trees (Rabin '69).
  - Automata on infinite words and trees.
- Applications of logic to verification of hardware & software:
  - Temporal logics (CTL, LTL, μ-calculus, ...).
  - Model checking on finite and infinite structures.
- Automata over infinite alphabets
  - Register automata, timed automata, ...
- Intuitionistic logic:
  - Rebuild mathematics intuitionistically.
  - Isolate the use of law of excluded middle.
  - Foundation for proof assistants: add data, recursion, induction.

FINITE TILING PROBLEM

Input: A finite set of tiles $T \subseteq \mathbb{N}$, initial and final tiles $a, b \in T$, vertical and horizontal compatibility relations $V, H \subseteq T \times T$.

Output: YES iff there is $m \in \mathbb{N}$ and a tiling of $\{0, \dots, m\} \times \{0, \dots, m\}$:



$\Rightarrow (x, y) \in V$ & $(x, z) \in H$

The finite tiling problem is UNDECIDABLE.