Propositional and Predicate Logic - XIII

Petr Gregor

KTIML MFF UK

WS 2022/2023

Openly axiomatizable theories

Theorem *If a theory T is openly axiomatizable, then every substructure of a model of T is also a model of T.*

Proof Let T' be open axiomatization of $M(T)$, $\mathcal{A} \models T'$ and $\mathcal{B} \subseteq \mathcal{A}$. We know that $\mathcal{B} \models \varphi$ for every $\varphi \in T'$ since φ is open. Thus $\mathcal{B}$ is a model of T'. □

Remark *The other implication holds as well, i.e. if every substructure of every model of T is also a model of T, then T is openly axiomatizable.*

For example, the theory DeLO is not openly axiomatizable since e.g. any finite substructure of a model of DeLO is not a model DeLO.

At most n-element groups for a fixed $n > 1$ are openly axiomatized by

$$T \cup \{ \bigvee_{\substack{0 \leq i,j \leq n \\ i \neq j}} x_i = x_j \},$$

where T is the (open) theory of groups.

Recursive axiomatization and decidability

- A theory T is *recursively axiomatized* if there is an algorithm that halts for every input formula φ and outputs whether $\varphi \in T$.
- A theory T is *decidable* if there is an algorithm that halts for every input formula and outputs whether $\varphi \in Thm(T)$.
- A theory T is *partially decidable* if there is an algorithm that for every input formula φ, it halts if and only if $\varphi \in Thm(T)$.

Proposition *For every recursively axiomatized theory T,*

(i) *T is partially decidable,*

(ii) *if T is complete, then T is decidable.*

Proof (i) The construction of systematic tableau from T with a root $F\varphi$ gives an algorithm that recognizes $T \vdash \varphi$. (ii) If T is complete, then the parallel construction of systematic tableaux from T with roots $F\varphi$ resp. $T\varphi$ gives an algorithm that decides whether $T \vdash \varphi$. □

Recursively enumerable completion

What happens if we are able to describe all simple complete extensions?

We say that a theory T has *recursively enumerable completion* if there exists an algorithm $\alpha(i, j)$ that generates the i-th axiom of the j-th simple complete extension of T (in some enumeration) or announces that it (such an axiom or an extension) does not exist.

Proposition *If a theory T is recursively axiomatized and T has recursively enumerable completion, then T is decidable.*

Proof By the previous proposition there is an algorithm to recognize $T \vdash \varphi$. On the other hand, if $T \nvdash \varphi$ then $T' \vdash \neg\varphi$ is some simple complete extension T' of T. This can be recognized by parallel construction of systematic tableaux with the root $T\varphi$ from all extensions. In the i-th step we construct tableaux up to i levels for the first i extensions. □

Examples of decidable theories

The following theories are decidable although not complete.

- the theory of pure equality; with no axioms, in $L = \langle\rangle$ with equality,
- the theory of unary predicate; with no axioms, in $L = \langle U \rangle$ with equality, where U is a unary relation symbol,
- the theory of dense linear orders $DeLO^*$,
- the theory of algebraically closed fields in $L = \langle +, -, \cdot, 0, 1 \rangle$ with equality, with the axioms of fields, and moreover the axioms for all $n \geq 1$,

  $$(\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0 = 0),$$

  where y^k is a shortcut for the term $y \cdot y \cdot \;\cdots\; \cdot y$ ($\cdot$ applied $(k-1)$-times).
- the theory of Abelian groups,
- the theory of Boolean algebras.

Recursive axiomatizability

Can we "effectively" describe common mathematical structures?

A class $K \subseteq M(L)$ is *recursively axiomatizable* if there exists a recursively axiomatized theory T of language L with $M(T) = K$.

Proposition *Every finite structure $\mathcal{A}$ in a finite language with equality is recursively axiomatizable (up to isomorphism). Thus, $\mathrm{Th}(\mathcal{A})$ is decidable.*

Proof Let $A = \{a_1, \ldots, a_n\}$. $\mathrm{Th}(\mathcal{A})$ can be axiomatized by a single sentence (thus recursively) that describes $\mathcal{A}$. It is of the form *"there are exactly n elements $a_1, \ldots, a_n$ and they satisfy exactly those atomic formulas on function values and relations that are valid in the structure $\mathcal{A}$."* □

Examples of recursive axiomatizability

The following structures $\mathcal{A}$ are recursively axiomatizable.

- $\langle \mathbb{Z}, \leq \rangle$, by the theory of discrete linear orderings,
- $\langle \mathbb{Q}, \leq \rangle$, by the theory of dense linear orderings without ends ($DeLO$),
- $\langle \mathbb{N}, S, 0 \rangle$, by the theory of successor with zero,
- $\langle \mathbb{N}, S, +, 0 \rangle$, by so called Presburger arithmetic,
- $\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$, by the theory of real closed fields,
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$, by the theory of algebraically closed fields with characteristic 0.

Corollary *For all the above structures $\mathcal{A}$ the theory $\mathrm{Th}(\mathcal{A})$ is decidable.*

Remark *However, $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ is not recursively axiomatizable. (This follows from the Gödel's incompleteness theorem).*

Robinson arithmetic

How to effectively and "almost" completely axiomatize $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$*?*

The language of arithmetic is $L = \langle S, +, \cdot, 0, \leq \rangle$ with equality.

Robinson arithmetic Q has axioms (finitely many)

$$S(x) \neq 0 \qquad x \cdot 0 = 0$$
$$S(x) = S(y) \rightarrow x = y \qquad x \cdot S(y) = x \cdot y + x$$
$$x + 0 = x \qquad x \neq 0 \rightarrow (\exists y)(x = S(y))$$
$$x + S(y) = S(x + y) \qquad x \leq y \leftrightarrow (\exists z)(z + x = y)$$

Remark Q *is quite weak; for example, it does not prove commutativity or associativity of* $+$*,* $\cdot$*, or transitivity of* $\leq$*. However, it suffices to prove, for example, existential sentences on numerals that are true in* $\underline{\mathbb{N}}$*.*

For example, for $\varphi(x, y)$ *in the form* $(\exists z)(x + z = y)$ *it is*

$$Q \vdash \varphi(\underline{1}, \underline{2}), \quad \text{where } \underline{1} = S(0) \text{ and } \underline{2} = S(S(0)).$$

Peano arithmetic

Peano arithmetic PA has axioms of

(a) Robinson arithmetic Q,

(b) scheme of induction; that is, for every formula $\varphi(x, \overline{y})$ of L the axiom

$$(\varphi(0, \overline{y}) \wedge (\forall x)(\varphi(x, \overline{y}) \rightarrow \varphi(S(x), \overline{y}))) \rightarrow (\forall x)\varphi(x, \overline{y}).$$

Remark PA *is quite successful approximation of* $\mathrm{Th}(\underline{\mathbb{N}})$*, it proves all "elementary" properties that are true in* $\underline{\mathbb{N}}$ *(e.g. commutativity of* $+$*). But it is still incomplete, there are sentences that are true in* $\underline{\mathbb{N}}$ *but independent in* PA*.*

Remark *In the second-order language we can completely axiomatize* $\underline{\mathbb{N}}$ *(up to isomorphism) by taking directly the following (second-order) axiom of induction instead of scheme of induction*

$$(\forall X)\ ((X(0) \wedge (\forall x)(X(x) \rightarrow X(S(x)))) \rightarrow (\forall x)\ X(x)).$$

Hilbert's 10th problem

- Let $p(x_1, \ldots, x_n)$ be a polynomial with integer coefficients. Does the *Diophantine equation* $p(x_1, \ldots, x_n) = 0$ have a solution in integers?
- Hilbert (1900) *"Find an algorithm that determines in finitely many steps whether a given Diophantine equation in an arbitrary number of variables and with integer coefficient has an integer solution."*

Remark *Equivalently, one may ask for an algorithm to determine whether there is a solution in natural numbers.*

Theorem (DPRM, 1970) *The problem of existence of integer solution to a given Diophantine equation with integer coefficients is alg. undecidable.*

Corollary *There is no algorithm to determine for given polynomials* $p(x_1, \ldots, x_n)$, $q(x_1, \ldots, x_n)$ *with natural coefficients whether*

$$\underline{\mathbb{N}} \models (\exists x_1) \ldots (\exists x_n)(p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)).$$

Undecidability of predicate logic

Is there an algorithm to decide whether a given sentence is (logically) true?

- We know that Robinson arithmetic Q has finitely many axioms, model $\underline{\mathbb{N}}$, and proves existential sentences on numerals that are true in $\underline{\mathbb{N}}$.
- More precisely, for every existential formula $\varphi(x_1, \ldots, x_n)$ in arithmetic,
$$Q \vdash \varphi(x_1/\underline{a_1}, \ldots, x_n/\underline{a_n}) \quad \Leftrightarrow \quad \underline{\mathbb{N}} \models \varphi[e(x_1/a_1, \ldots, x_n/a_n)]$$
for every $a_1, \ldots, a_n \in \mathbb{N}$ where $\underline{a_i}$ denotes the a_i-th numeral.
- In particular, for φ in form $(\exists x_1) \ldots (\exists x_n)(p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n))$, where p, q are polynomials with natural coefficients (numerals) we have
$$\underline{\mathbb{N}} \models \varphi \quad \Leftrightarrow \quad Q \vdash \varphi \quad \Leftrightarrow \quad \vdash \psi \rightarrow \varphi \quad \Leftrightarrow \quad \models \psi \rightarrow \varphi,$$
where ψ is the conjunction of (closures) of all axioms of Q.
- Thus, if there was an algorithm deciding on logical truth of sentences, there would be also an algorithm to decide $\underline{\mathbb{N}} \models \varphi$, which is impossible.

Gödel's incompleteness theorems

Theorem (1st) *For every consistent recursively axiomatized extension T of Robinson arithmetic there is a sentence true in $\underline{\mathbb{N}}$ and unprovable in T.*

Remarks

- *"Recursively axiomatized" means that T is "effectively given".*
- *"Extension of R. arithmetic" means that T is "sufficiently strong".*
- *If, moreover, $\underline{\mathbb{N}} \models T$, the theory T is incomplete.*
- *The sentence constructed in the proof says "I am not provable in T".*
- *The proof is based on two principles:*

  (a) *arithmetization of syntax,*

  (b) *self-reference.*

Arithmetization - provability predicate

- Finite objects of syntax (symbols of language, terms, formulas, finite tableaux, proofs) can be (effectively) encoded by natural numbers.
- Let $\ulcorner\varphi\urcorner$ denote the code of formula φ and let $\underline{\varphi}$ denote the numeral (a term of arithmetic) representing $\ulcorner\varphi\urcorner$.
- If T has recursive axiomatization, the relation $\mathrm{Prf}_T \subseteq \mathbb{N}^2$ is recursive.

  $\mathrm{Prf}_T(x, y) \quad \Leftrightarrow \quad$ *a (tableau) y is a proof of (a sentence) x in T.*

- If, moreover, T extends Robinson arithmetic Q, the relation Prf_T can be represented by some formula $Prf_T(x, y)$ such that for every $x, y \in \mathbb{N}$

$$Q \vdash Prf_T(\underline{x}, \underline{y}), \quad \text{if} \quad \mathrm{Prf}_T(x, y),$$
$$Q \vdash \neg Prf_T(\underline{x}, \underline{y}), \quad \text{otherwise.}$$

- $Prf_T(x, y)$ expresses that *"y is a proof of x in T"*.
- $(\exists y)Prf_T(x, y)$ expresses that *"x is provable in T"*.
- If $T \vdash \varphi$, then $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\varphi}, y)$ and moreover $T \vdash (\exists y)Prf_T(\underline{\varphi}, y)$.

Self-reference principle

- *This sentence has 24 letters.*

  In formal systems self-reference is not always available straightforwardly.

- *The following sentence has 32 letters "The following sentence has 32 letters".*

  Such direct reference is available, if we can "talk" about sequences of symbols. But the above sentence is not self-referencial.

- *The following sentence written once and then once more again between quotation marks has 116 letters "The following sentence written once and then once more again between quotation marks has 116 letters".*

  With use of direct reference we can have self-reference. Instead of *"it has x letters"* we can have other property.

- ```
  main(){char *c="main(){char *c=%c%s%c; printf(c,34,c,34);}"; printf(c,34,c,34);}
  ```
  ```

Fixed-point theorem

Theorem *Let T be a consistent extension of Robinson arithmetic. For every formula $\varphi(x)$ in language of theory T there is a sentence ψ s.t. $T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$.*

Remark ψ is self-referencial, it says *"This formula satisfies condition φ"*.

Proof (idea) Consider the *doubling* function d such that for every formula $\chi(x)$

$$d(\ulcorner\chi(x)\urcorner) = \ulcorner\chi(\underline{\chi(x)})\urcorner$$

- It can be shown that d is expressible in T. Assume *(for simplicity)* that it is expressible by some term, denoted also by d.
- Then for every formula $\chi(x)$ in language of theory T it holds that

$$T \vdash d(\underline{\chi(x)}) = \underline{\chi(\underline{\chi(x)})} \qquad (1)$$

- We take $\varphi(d(\underline{\varphi(d(x))}))$ for ψ. If suffices to verify that $T \vdash d(\underline{\varphi(d(x))}) = \underline{\psi}$.
- This follows from (1) for $\chi(x)$ being $\varphi(d(x))$, since in this case

$$T \vdash d(\underline{\varphi(d(x))}) = \underline{\varphi(d(\underline{\varphi(d(x))}))} \qquad \square$$

Undefinability of truth

We say that a formula $\tau(x)$ *defines truth* in theory T of arithmetical language if for every sentence φ it holds that $T \vdash \varphi \leftrightarrow \tau(\underline{\varphi})$.

Theorem *Let T be consistent extension of Robinson arithmetic. Then T has no definition of truth.*

Proof By the fixed-point theorem for $\neg\tau(x)$ there is a sentence φ such that

$$T \vdash \varphi \leftrightarrow \neg\tau(\underline{\varphi}).$$

Supposing that $\tau(x)$ defines truth in T, we would have

$$T \vdash \varphi \leftrightarrow \neg\varphi,$$

which is impossible in a consistent theory T. □

Remark *This is based on the liar paradox, the sentence φ would express "This sentence is not true in T".*

Proof of the first incompleteness theorem

Theorem (Gödel) *For every consistent recursively axiomatized extension T of Robinson arithmetic there is a sentence true in $\underline{\mathbb{N}}$ and unprovable in T.*

Proof Let $\varphi(x)$ be $\neg(\exists y)Prf_T(x, y)$, it says *"$x$ is not provable in T"*.

- By the fixed-point theorem for $\varphi(x)$ there is a sentence ψ_T such that
$$T \vdash \psi_T \leftrightarrow \neg(\exists y)Prf_T(\underline{\psi_T}, y). \quad (2)$$
ψ_T says *"I am not provable in T"*. More precisely, ψ_T is equivalent to a sentence expressing that ψ_T is not provable T (where the equivalence holds both in $\underline{\mathbb{N}}$ and in T).
- First, we show ψ_T *is not provable in T*. If $T \vdash \psi_T$, i.e. ψ_T is contradictory in $\underline{\mathbb{N}}$, then $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$ and moreover $T \vdash (\exists y)Prf_T(\underline{\psi_T}, y)$. Thus from (2) it follows $T \vdash \neg\psi_T$, which is impossible since T is consistent.
- It remains to show ψ_T is true in $\underline{\mathbb{N}}$. If not, i.e. $\underline{\mathbb{N}} \models \neg\psi_T$, then $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$. Hence $T \vdash \psi_T$, which we already disproved. □

Corollaries and a strengthened version

Corollary *If, moreover,* $\underline{\mathbb{N}} \models T$*, then the theory* T *is incomplete.*

Proof Suppose T is complete. Then $T \vdash \neg\psi_T$ and thus $\underline{\mathbb{N}} \models \neg\psi_T$, which contradicts $\underline{\mathbb{N}} \models \psi_T$. □

Corollary $\mathrm{Th}(\underline{\mathbb{N}})$ *is not recursively axiomatizable.*

Proof $\mathrm{Th}(\underline{\mathbb{N}})$ is consistent extension of Robinson arithmetic and has a model $\underline{\mathbb{N}}$. Suppose $\mathrm{Th}(\underline{\mathbb{N}})$ is recursively axiomatizable. Then by previous corollary, $\mathrm{Th}(\underline{\mathbb{N}})$ is incomplete, but $\mathrm{Th}(\underline{\mathbb{N}})$ is clearly complete. □

Gödel's first incompleteness theorem can be strengthened as follows.

Theorem (Rosser) *Every consistent recursively axiomatized extension* T *of Robinson arithmetic has an independent sentence. Thus* T *is incomplete.*

Remark *Hence the assumption in the first corollary that* $\underline{\mathbb{N}} \models T$ *is superfluous.*

Gödel's second incompleteness theorem

Let Con_T denote the sentence $\neg(\exists y)Prf_T(\underline{0=1}, y)$. We have that $\underline{\mathbb{N}} \models Con_T \Leftrightarrow T \not\vdash 0 = \underline{1}$. Thus Con_T expresses that *"T is consistent"*.

Theorem (Gödel) *For every consistent recursively axiomatized extension T of Peano arithmetic it holds that Con_T is unprovable in T.*

Proof (idea) Let ψ_T be the Gödel's sentence *"This is not provable in T"*.

- In the first part of the proof of the 1st theorem we showed that

  "If T is consistent, then ψ_T is not provable in T." (3)

  In other words, we showed it holds $Con_T \to \psi_T$.
- If T is an extension of Peano arithmetic, the proof of (3) can be formalized within the theory T itself. Hence $T \vdash Con_T \to \psi_T$.
- Since T is consistent by the assumption, from (3) we have $T \not\vdash \psi_T$.
- Therefore from the previous two bullets, it follows that $T \not\vdash Con_T$. □

Remark *Hence a such theory T cannot prove its own consistency.*

Corollaries of the second theorem

Corollary *Peano arithmetic has a model $\mathcal{A}$ s.t. $\mathcal{A} \models (\exists y) Prf_{PA}(\underline{0 = 1}, y)$.*

Remark *$\mathcal{A}$ has to be nonstandard model of PA, the witness must be some nonstandard element (other than a value of a numeral).*

Corollary *There is a consistent recursively axiomatized extension T of Peano arithmetic such that $T \vdash \neg Con_T$.*

Proof Let $T = PA \cup \{\neg Con_{PA}\}$. Then T is consistent since $PA \nvdash Con_{PA}$. Moreover, $T \vdash \neg Con_{PA}$, i.e. T proves inconsistency of $PA \subseteq T$, and thus also $T \vdash \neg Con_T$. □

Remark *$\underline{\mathbb{N}}$ cannot be a model of T.*

Corollary *If the set theory ZFC is consistent, then Con_{ZFC} is unprovable in ZFC.*