Logic and Computation II

Part 4. Formal arithmetic and Gödel's incompleteness theorems

Kazuyuki Tanaka

BIMSA

March 10, 2023

北京雁栖湖应用数学研究院
YANQI LAKE BEIJING INSTITUTE OF MATHEMATICAL SCIENCES AND APPLICATIONS

Outline of the Course

1. This is an introductory graduate-level course in **mathematical logic** and **theory of computation**. Its first part delivered in the last semester covered the basic topics of the two fields and their interactions. In this semester, we discuss more advanced topics emphasizing on decidability and definability.
2. Each week, there are two lectures, in Tuesday and Thursday. Every Thursday, we will assign simple homework problems or questionnaires to registered students, who are motivated to attend the class continuously. Normally, homeworks are due next Monday.
3. TA (Dr. Li) will handle homeworks as well as questions and comments from students via WeChat. We may assign harder problems to students, who will presumably go to the research level with us in the following years.
4. Lecture slides will be uploaded on the lecture page at BIMSA.

Logic and Computation II

- **Part 4. Formal arithmetic and Gödel's incompleteness theorems**
- **Part 5. Automata on infinite objects**
- **Part 6. Recursion-theoretic hierarchies**
- **Part 7. Admissible ordinals and second order arithmetic**

Part 4. Schedule

- Mar. 7, (1) First-order logic
- Mar. 9, (2) Arithmetical formulas
- Mar.14, (3) Gödel's first incompleteness theorem
- Mar.16, (4) Gödel's second incompleteness theorem
- Mar.21, (5) Second-order logic
- Mar.23, (6) Analytical formulas

Today's topics

1. Recap
2. Formal system of first-order logic
3. Completeness theorem
4. Application of the compactness theorem
5. Formal arithmetic
6. Peano arithmetic
7. Arithmetical hierarchy

Recap

- First-order logic is developed in the common logical symbols and specific mathematical symbols. Major logical symbols are propositional connectives, quantifiers $\forall x$ and $\exists x$ and equality $=$. The set of mathematical symbols to use is called a **language**.
- A **structure** in language $\mathcal{L}$ (simply, a $\mathcal{L}$-structure) is defined as a non-empty set A equipped with an interpretation of the symbols in $\mathcal{L}$.
- A **term** is a symbol string to denote an element of a structure. A **formula** is a symbol string to describe a property of a structure. A formula without free variables is called a **sentence**.
- "A sentence φ is **true** in $\mathcal{A}$, written as $\mathcal{A} \models \varphi$" is defined by Tarski's clauses. The truth of a formula with free variables is defined by the truth of its universal closure.
- A set of sentences in the language $\mathcal{L}$ is called a **theory**. $\mathcal{A}$ is a **model** of T, denoted by $\mathcal{A} \models T$, if $\forall \varphi \in T \ (\mathcal{A} \models \varphi)$.
- We say that φ holds in T, written as $T \models \varphi$, if $\forall \mathcal{A}(\mathcal{A} \models T \to \mathcal{A} \models \varphi)$.

Formal system of first-order logic

Axiom system

P1. $\varphi \to (\psi \to \varphi)$

P2. $\big(\varphi \to (\psi \to \theta)\big) \to \big((\varphi \to \psi) \to (\varphi \to \theta)\big)$

P3. $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$

P4. $\forall x \varphi(x) \to \varphi(t)$ (the quantification axiom)

Inference rules

(1) If φ and $\varphi \to \psi$ are theorems, so is ψ [a]

(2) If $\psi \to \varphi(x)$ (where ψ does not include x) is a theorem, then so is $\psi \to \forall x \varphi(x)$ (the generalization rule)

[a] known as Modus ponens(MP) or cut rule

- In languages with equality, the axiom Eq is assumed (reflexive, symmetrical, transitive, and for each symbol f or R, its value is preserved with equality).
- If a sentence σ can be proved from the set of sentences T, then σ is called a **theorem** of T, and written as $T \vdash \sigma$.
- The quantification axiom and the equality axiom hold trivially in any structure, and the generalization rule also clearly preserves truth (because the free variable x of a formula is interpreted by universal closure). So if $T \vdash \sigma$ then $T \models \sigma$ (**soundness theorem**).

Theorem (Completeness theorem (a weak version))

For any sentence σ, $\models \sigma$ iff $\vdash \sigma$.

- We only need to show that for any sentence σ, if $\models \sigma$, then $\vdash \sigma$.
- By the Skolem-Herbrand method. Let $\forall \vec{x} \varphi(\vec{x})$ be the $\mathrm{SNF}\sigma^S$ of σ. If $\neg\sigma$ is valid, there are n pairs of terms $\vec{t_i}$ such that $\neg\varphi(\vec{t_1}) \vee \cdots \vee \neg\varphi(\vec{t_k})$ is a tautology, and so provable in propositional logic, hence provable in first-oder logic. Therefore, $\exists \vec{x} \neg\varphi(\vec{x})$, i.e., $\neg\sigma$ is provable in first-oder logic.
- To show the completeness theorem, Gödel introduced new relation symbols instead of Skolem functions, and transformed any sentence into a $\forall\exists$ sentence.

The compactness theorem of first order logic is also deduced from the compactness of propositional logic.

Theorem (Compactness theorem)

If a set T of sentences of first order logic is not satisfiable, then there exists some finite subset of T which is not satisfiable.

From this we can derive the general completeness theorem.

Theorem (Gödel's completeness theorem)

In first order logic, $T \vdash \varphi \Leftrightarrow T \models \varphi$.

Proof. $\Rightarrow$ has been proved.

- To show $\Leftarrow$, assume $T \models \varphi$. Then $T \cup \{\neg\varphi\}$ is not satisfiable.
- By the compactness theorem, there exists a finite set $\{\sigma_1, \ldots, \sigma_n\}$ of T such that $\{\sigma_1, \ldots, \sigma_n, \neg\varphi\}$ is not satisfiable.
- Then $(\sigma_1 \wedge \cdots \wedge \sigma_n) \to \varphi$ is valid.
- From the completeness theorem (a weak version), $(\sigma_1 \wedge \cdots \wedge \sigma_n) \to \varphi$ is provable, and from MP, $\{\sigma_1, \ldots, \sigma_n\} \vdash \varphi$, hence $T \vdash \varphi$.

- Subsequently, L. Henkin introduced a constant $c_{\exists x\varphi(x)}$ (**Henkin constant**) for each sentence $\exists x\varphi(x)$, and assume the following formula $\exists x\varphi(x) \to \varphi(c_{\exists x\varphi(x)})$ as an additional axiom, called the Henkin axiom. By the Henkin axioms, any sentence can be rewritten as a formula without quantifiers.

- Henkin proved by contradiction that $T \nvdash \varphi \Rightarrow T \not\models \varphi$. $T \nvdash \varphi$ is equivalent to the consistency of $T \cup \{\neg\varphi\}$. $T \not\models \varphi$ is equivalent to the satisfiability of $T \cup \{\neg\varphi\}$ So, the following is enough for the completeness theorem.

Theorem (Model existence theorem)

If a set T of sentences of first order logic is consistent, then there exists a model of T.

- **Henkin's lemma**: If T is consistent, $T \cup \{\exists x \varphi(x) \to \varphi(c_{\exists x \varphi(x)})\}$ is also consistent.
- For a consistent theory T in a language $\mathcal{L}$, there are a set C of constants such that any sentence of the form $\exists x \varphi(x)$ in $\mathcal{L} \cup C$ has its Henkin constant in C.
- Let T_H be a consistent extension of T with all Henkin axioms H in C. Let $\hat{S}$ a maximal consistent set of T_H (with the equality axioms). Then, we define a model $\mathcal{A}$ of T as follows.
- First define an equivalence relation $\approx$ on C by $\mathrm{c} \approx \mathrm{d} \Leftrightarrow (\mathrm{c} = \mathrm{d}) \in \hat{S}$. Let $A = C/\approx$. Then define the interpretations of f and R on A as follows

$$\mathrm{f}^{\mathcal{A}}([\mathrm{c}_1], [\mathrm{c}_2], \ldots, [\mathrm{c}_n]) = [\mathrm{d}] \Leftrightarrow (\mathrm{f}(\mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_n) = \mathrm{d}) \in \hat{S}$$

$$\mathrm{R}^{\mathcal{A}}([\mathrm{c}_1], [\mathrm{c}_2], \ldots, [\mathrm{c}_n]) \Leftrightarrow \mathrm{R}(\mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_n) \in \hat{S}$$

Here, a structure $\mathcal{A}$ is well-defined since $\hat{S}$ includes all the equality axioms. Then, we can also show by induction that $\mathcal{A} \models \varphi([\mathrm{c}_1], \ldots, [\mathrm{c}_n]) \Leftrightarrow \varphi(\mathrm{c}_1, \ldots, \mathrm{c}_n) \in \hat{S}$. Thus, $\mathcal{A}$ is a model of T.

Existence of non-standard models of arithmetic

- Let $\mathcal{N} = (\mathbb{N}, 0, 1, +, \cdot, <)$ be the standard model of arithmetic (natural number theory).
- Let Th($\mathcal{N}$) $:= \{\sigma : \mathcal{N} \models \sigma\}$. $\mathcal{N}$ is naturally a model of Th($\mathcal{N}$), but there also exist models of Th($\mathcal{N}$) that are not isomorphic to $\mathcal{N}$, which are called **nonstandard models** of arithmetic.
- Using the compactness theorem, we construct a nonstandard model of arithmetic as follows. First, with c as a new constant, for each $k \in \mathbb{N}$

$$T_k = \mathrm{Th}(\mathcal{N}) \cup \{0 < \mathrm{c}, 1 < \mathrm{c}, 1+1 < \mathrm{c}, 1+1+1 < \mathrm{c}, \ldots, \overbrace{1+1+\cdots+1}^{k \text{ times}} < \mathrm{c}\}$$

- The structure of $\mathcal{N}$ plus the interpretation of the constant c as $k+1$ is a model of T_k.
- Let $T = \bigcup_{k \in \mathbb{N}} T_k$. Any finite subset of T is contained in some T_k and so satisfiable. Hence, by the compactness theorem, T also has a model $\mathcal{M}$, where the value of c is larger than any standard natural number.
- That is, $\mathcal{M}$ has elements that are not standard natural numbers.
- By removing the constant c from the structure, $\mathcal{M}$ can be regarded as a non-standard model of arithmetic in the language $\mathcal{L}_{\mathrm{OR}}$.

Existence of arbitrarily large models

- If T has an arbitrarily large finite model, then T has a model of arbitrarily large infinite cardinality.
- Let $\{c_i : i \in \kappa\}$ be a set of constants with infinite cardinality κ. We consider
$$T' = T \cup \{c_i \neq c_j : i \neq j \text{ and } i, j \in \kappa\}$$
- For any finite subset of T', it is satisfiable if we take a finite model of T with at least the number of constants c_i in it, and interpret each constant as a distinct element.
- Therefore, from the compactness theorem, T' also has a model, which is a model of T with more than κ elements.
- To construct a model with exactly the same cardinality as T, we use a generalized version of the Löwenheim-Skolem's downward theorem.

Peano Arithmetic

- So-called "**Peano's postulates**" (1889) is famous as an axiomatic treatment of the natural numbers. However, it is not a formal system in the sense of modern logic, since its underlying logic is ambiguous. Moreover, we should also notice previous advanced studies by C.S. Peirce (1881) and R. Dedekind (1888).
- It was Hilbert who began to consider natural number theory as a formal theory in first-order logic.
- In fact, Peano arithmetic PA as a strict formal system were established through Gödel's arguments of his incompleteness theorem.

G. Peano

C.S. Peirce

R. Dedekind

Peano arithmetic is a first-order theory in the language of ordered rings $\mathcal{L}_{\mathrm{OR}} = \{+, \cdot, 0, 1, <\}$.

Definition

Peano arithmetic (PA) consists of the following axioms.

Successor:	$\neg(x+1=0)$,	$x+1=y+1 \to x=y$.
Addition:	$x+0=x$,	$x+(y+1)=(x+y)+1$.
Multiplication:	$x \cdot 0 = 0$,	$x \cdot (y+1) = x \cdot y + x$.
Inequality	$\neg(x<0)$,	$x<y+1 \leftrightarrow x<y \lor x=y$.
Induction:	$\varphi(0) \land \forall x(\varphi(x) \to \varphi(x+1)) \to \forall x \varphi(x)$.	

- Induction is not a single formula, but an axiom scheme that collects the formulas for all the $\varphi(x)$ in $\mathcal{L}_{\mathrm{OR}}$. Note that $\varphi(x)$ may include free variables other than x.
- In "Peano's postulates", induction is expressed in terms of sets, but Peano arithmetic does not presuppose set theory.

- In a modern formal system, to introduce a new function by definition, it must be defined explicitly so that the extended system is a conservative extension.
- The primitive recursive definition is not an explicit definition. In fact, if we add the primitive recursive definition of multiplication to Presburger arithmetic (a system of only addition), the resulting system loses completeness and decidability, and it is not a conservative extension.
- In other words, multiplication is not definable from addition in the formal sense.
- On the other hand, the inequality $x < y$ can be defined from addition as abbreviation for $\exists z(y = (x + z) + 1)$. However, we prefer to include the inequality as a primitive symbol, because it allows us to define the hierarchy of formulas simply.
- Similarly, in the following, we assume that $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\forall$, $\exists$, etc. are all pre-set.

Arithmetical Hierarchy

- We inductively define hierarchical classes of formulas Σ_i and Π_i ($i \in \mathbb{N}$).

Definition

- The **bounded** formulas are constructed from atomic formulas by using propositional connectives and bounded quantifiers $\forall x < t$ and $\exists x < t$, where $\forall x < t$ and $\exists x < t$ are abbreviations for $\forall x(x < t \rightarrow \cdots)$ and $\exists x(x < t \wedge \cdots)$, respectively, and t is a term that does not includes x. A bounded formula is also called a Σ_0 ($=\Pi_0$) formula.
- For any $i, k \in \mathbb{N}$:
  - if φ is a Σ_i formula, $\forall x_1 \cdots \forall x_k \varphi$ is a Π_{i+1} formula,
  - if φ is a Π_i formula, $\exists x_1 \cdots \exists x_k \varphi$ is a Σ_{i+1} formula.

- Σ_i / Π_i also denotes the set of all Σ_i / Π_i formulas.

- In the above definition, there are many formulas that do not belong to any class. So, the (lowest) class to which the equivalent formula belongs is regarded as the class of the formula.

Examples

- $\neg\exists y(y + y = x)$ does not belong to any of the above class.
- But it is logically equivalent to a Π_1 formula $\forall y \neg(y + y = x)$.
- So $\neg\exists y(y + y = x)$ is a Π_1 formula.

- If a Π_i formula is equivalent to some Σ_i formula or a Σ_i formula equivalent to some Π_i formula, such a formula is called a Δ_i formula.

Example

- The following $\Sigma_0(=\Pi_0)$ formula $\mathrm{P}(x)$ expresses "x is a prime number"

$$\mathrm{P}(x) \equiv \neg\exists d < x \exists e < x (d \cdot e = x) \wedge \neg(x = 0) \wedge \neg(x = 1).$$

- The proposition "every even number greater than or equal to 4 is the sum of two primes" (the "Goldbach conjecture") is expressed by the following Π_1 formula:

$$\forall x > 1 \exists p < 2x \exists q < 2x \ (2x = p + q \wedge \mathrm{P}(p) \wedge \mathrm{P}(q)).$$

- "There are infinitely many primes" is expressed as a Π_2 formula $\forall x \exists y > x \mathrm{P}(y)$. It can be expressed as a Π_1 formula (exercise).

Let us define a subsystem of Peano arithmetic PA by restricting its induction axiom.

Definition

Let Γ be a class of formulas in $\mathcal{L}_{\mathrm{OR}}$. By I$\Gamma$, we denote a subsystem of PA obtained by restricting ($\varphi(x)$ of) induction to the class Γ.

- The main subsystems of PA are I$\Sigma_1 \supset$ I$\Sigma_0 \supset$ IOpen, where Open is the set of formulas without quantifiers.

Another system weaker than IOpen is the system Q defined by R. Robinson.

Definition

Robinson's system Q is obtained from PA by removing the axioms of inequality and induction, and instead adding the following axiom:

Predecessor: $\forall x(x \neq 0 \to \exists y(y+1=x))$.

So, it is a theory in the language of ring $\mathcal{L}_{\mathrm{R}} = \{+, \cdot, 0, 1\}$.

Let $\mathrm{Q}_<$ be the system Q plus the definition of the inequality symbol.

Example: Show that $\mathsf{Q} \vdash 0 + 1 = 1$

- First, we show $\mathsf{Q} \vdash 1 \neq 0$. If $1 = 0$, then $0 + 1 = 0 + 0$. On the other hand, we have $0 + 1 \neq 0$ according to the successor axiom, and $0 + 0 = 0$ according to the axiom of addition. So it is a contradiction.
- Then we have y such that $y + 1 = 1$ by applying the predecessor axiom.
- Next we show $y = 0$. Assume $y \neq 0$. Then, by axiom of addition $0 + 1 = 0 + (y + 1) = (0 + y) + 1$, we have $0 = 0 + y$. Again by the predecessor axiom, there is z such that $z + 1 = y$. Thus $0 = 0 + (z + 1) = (0 + z) + 1$, a contradiction.

Lemma

In IOpen, all axioms of **theory of discrete ordered semirings** PA^- can be proved.

(1) Semiring axiom (excluding the existence of additive inverses from the commutative ring axiom).

(2) difference axiom $x < y \to \exists z(z + (x + 1) = y)$.

(3) 0 as the minimum element in linear order and discrete $(0 < x \leftrightarrow 1 \leq x)$.

(4) Order preservation $x < y \to x + z < y + z \land (x \cdot z < y \cdot z \lor z = 0)$.

Problem

- In PA^-, the predecessor axiom holds.
- In IOpen, the associative law of addition $(x + y) + z = x + (y + z)$ holds. [a]
- In IOpen, the difference axiom $x < y \to \exists z(z + (x + 1) = y)$ holds.

[a] This claim has already been shown in Peirce's paper, On the Logic of Number, American Journal of Mathematics, Vol. 4, No. 1 (1881), pp.85-95.

Corollary

$\mathsf{Q}_< \subset \mathsf{PA}^- \subset \mathrm{IOpen} \subset \mathrm{I}\Sigma_0 \subset \mathrm{I}\Sigma_1 \subset \mathsf{PA}$.

Example

- Let $\mathbb{Z}[X]$ be the set of polynomials of integer coefficients with X as a variable. $+, \cdot, 0, 1$ are naturally defined on it, making it a ring.
- For $p \in \mathbb{Z}[X]$, define $p > 0$ when its highest order coefficient is positive, and $p > q \Leftrightarrow p - q > 0$ defines an order between the two polynomials p, q.
- Let $\mathbb{Z}[X]^+ = \{p \in \mathbb{Z}[X] : p \geq 0\}$. Then it is a (non-standard) model of PA^-.
- In $\mathbb{Z}[X]^+$, the standard part $\mathbb{N}$ is immediately followed by a $\mathbb{Z}$-structure containing X, then followed by $\mathbb{Z}$-structure containing $2X$, then followed by $\mathbb{Z}$-structure containing $3X$, etc.
- Between those string of $\mathbb{Z}$-structures and the $\mathbb{Z}$-structure containing X^2 there is an infinite descending sequence of $\mathbb{Z}$ structures containing $X^2 - nX$.

- Since $\mathrm{Q}_<$ lacks induction, it cannot prove many propositions that something holds for all x (eg, $\forall x(0+x=x)$).
- However, it proves correct equalities and inequalities consiting of only concrete numbers.
- In other words, an atomic formula $s=t$ or $s<t$ without variables can be proved if true, and its negation can be proved if false[1].
- Furthermore, propositional connectives and bounded quantifiers preserve the correspondence between truth and provability.
- A bounded formulas without free variables can be proved/disproved in $\mathrm{Q}_<$ if it is true/false.
- A system is said to be Σ_1-**complete** if it proves all true Σ_1 sentences. This seems to be very strong condition, but indeed $\mathrm{Q}_<$ is Σ_1-complete.

[1] This fact is strictly shown by meta-induction on the composition of the terms, not by induction in the system. For details, see Section 4.2 of my book `https://www.kinokuniya.co.jp/f/dsg-01-9784785315757`.

- In a formal system, a natural number n is denoted by a term $\overline{n} = \overbrace{1 + \cdots + 1}^{n \text{ times}}$ (called a **numeral**). Note $\overline{0} = 0$.

Theorem (Σ_1-completeness of $Q_<$)

$Q_<$ proves all true Σ_1 sentences.

Proof

- If a Σ_1 sentence $\exists x_1 \exists x_2 \ldots \exists x_k \varphi(x_1, x_2, \ldots, x_k)$ is true, there exist concrete numbers $n_1, n_2, \ldots, n_k$ such that $\varphi(\overline{n_1}, \overline{n_2}, \ldots, \overline{n_k})$ holds.
- Since $\varphi(\overline{n_1}, \overline{n_2}, \ldots, \overline{n_k})$ is a bounded formula, it is provable if it is true. From the rule of first-order logic, $\exists x_1 \exists x_2 \ldots \exists x_k \varphi(x_1, x_2, \ldots, x_k)$ is also provable. □

- Now, a typical condition for a theory to induce the first incompleteness theorem is often described as including a weak arithmetic (such as $\mathsf{Q}_<$).
- This is simply rephrased as Σ_1-complete. All the arithmetic systems we will discuss are extensions of $\mathsf{Q}_<$, and thus Σ_1-complete.
- Another condition introduced by Gödel is ω-consistency. A system T is said to be ω-**consistent** if "$\varphi(\overline{n})$ can be proved by T for all natural numbers n, $\exists x \neg\varphi(x)$ cannot be proved by T."
- However, only the case where this $\varphi(x)$ is a Σ_0 formula is sufficient to prove the incompleteness theorem. ω-consistency when $\varphi(x)$ is restricted to Σ_0 is called **1-consistency**.
- ω-consistency is strictly stronger than 1-consistency, and 1-consistency is strictly stronger than consistency.
- A system in which all provable Σ_n statements are true is said to be Σ_n-**sound**. Then, 1-consistency and Σ_1-soundness are equivalent in the Σ_1-complete theory (Exercise). So, Σ_1-soundness is sometimes called 1-consistency.
- It is known that Π_3-soundness can be derived from ω-consistency, but Σ_3-soundness cannot be derived.

In the next lecture, we are going to prove

Theorem (Gödel's first incompleteness theorem)

Any Σ_1-complete and 1-consistent CE theory is incomplete, that is, there is a sentence that cannot be proved or disproved.

Thank you for your attention!