Logic and Foundation I

Part 4. First order arithmetic and incompleteness theorems

Kazuyuki Tanaka

BIMSA

December 30, 2023

Logic and Foundations I

- **Part 1. Equational theory**
- **Part 2. First order theory**
- **Part 3. Model theory**
- **Part 4. First order arithmetic and incompleteness theorems**

Part 2. Schedule

- Dec. 07, (1) Peano arithmetic and representation theorems
- Dec. 14, (2) The first incompleteness theorem
- Dec. 21, (3) The second incompleteness theorem
- Dec. 28, (4) Presburger arithmetic

Recap

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.

The Gödel sentence π_G is defined by $T \vdash \pi_G \leftrightarrow \neg \mathrm{Bew}_T(\overline{\ulcorner \pi_G \urcorner})$.

Theorem (Gödel-Rosser incompleteness theorem)

Any Σ_1-complete and consistent CE theory is incomplete.

The Rosser sentence π_R is defined by $T \vdash \pi_R \leftrightarrow \neg \mathrm{Bew}^*_T(\overline{\ulcorner \pi_R \urcorner})$, where

$$\mathrm{Bew}^*_T(x) \equiv \exists y(\mathrm{Proof}_T(y, x) \land \forall z < y \neg \mathrm{Proof}_T(z, \neg x)).$$

Theorem (Gödel's second incompleteness theorem)

Let T be a consistent CE theory, which contains $\mathrm{I}\Sigma_1$. Then $\mathrm{Con}(T)$ cannot be proved in T.

$\mathrm{Con}(T) \equiv \neg \mathrm{Bew}_T(\overline{\ulcorner 0 = 1 \urcorner})$. $\quad T \vdash \mathrm{Con}(T) \leftrightarrow \pi_G$.

Lemma (Hilbert-Bernays-Löb's derivability condition)

Let T be a consistent CE theory containing $\mathrm{I}\Sigma_1$. For any φ, ψ,
D1. $T \vdash \varphi \Rightarrow T \vdash \mathrm{Bew}_T(\overline{\ulcorner\varphi\urcorner})$.
D2. $T \vdash \mathrm{Bew}_T(\overline{\ulcorner\varphi\urcorner}) \wedge \mathrm{Bew}_T(\overline{\ulcorner\varphi \to \psi\urcorner}) \to \mathrm{Bew}_T(\overline{\ulcorner\psi\urcorner})$.
D3. $T \vdash \mathrm{Bew}_T(\overline{\ulcorner\varphi\urcorner}) \to \mathrm{Bew}_T(\overline{\ulcorner\mathrm{Bew}_T(\overline{\ulcorner\varphi\urcorner})\urcorner})$.

Proof.

- D1 is obtained from the Σ_1 completeness of T, since $\mathrm{Bew}_T(\overline{\ulcorner\varphi\urcorner})$ is a Σ_1 formula.
- For D2, it is clear that the proof of ψ is obtained by applying MP to the proof of φ and the proof of $\varphi \to \psi$.
- D3 formalizes D1 in T. This is the most difficult, since we can not find a simple machinery to transform a proof of φ in T to a proof of $\mathrm{Bew}_T(\overline{\ulcorner\varphi\urcorner})$. There are several known ways to deal with this problem.

Alternative proof of D3

- For simplicity, let T be PA. We also identify a formula $\varphi(x)$ with the set $\{n : \varphi(n)\}$.
- In T, we can prove a countable version of the completeness theorem of first-order logic. A countable model M can be treated as its coded diagram, i.e., the set of the Gödel numbers of $\mathcal{L}_M$-sentences true in M. The arithmetized completeness theorem says that if T' is consistent then there exists (a formula expressing the diagram of) a model of T'.
- Now, we going to prove $\mathrm{Con}(T) \to \pi_G$ in T. By the completeness theorem, it is sufficient to show that any model M of $T + \mathrm{Con}(T)$ satisfies π_G. First, note that π_G is equivalet to $\neg\mathrm{Bew}_T(\overline{\ulcorner \pi_G \urcorner})$, which is also equivalet to $\mathrm{Con}(T + \neg\pi_G)$. Since M satisfies $\mathrm{Con}(T)$, we can make a model M_1 of T over M. So, if M_1 satisfies $\neg\pi_G$, then M shows $\mathrm{Con}(T + \neg\pi_G)$. If M_1 satisfies π_G, M also satisfies π_G since π_G is Π_1 and M is a submodel of M_1. (This proof is due to Kikuchi-Tanaka.)

- As a variant of the Gödel sentence, a sentence meaning "this sentence is provable" is known as a **Henkin sentence**. That is, H is a Henkin sentence if

$$\mathrm{H} \leftrightarrow \mathrm{Bew}_T(\overline{\ulcorner \mathrm{H} \urcorner}).$$

  If H is provable and true, then both sides are true and there is no problem.
  On the other hand, if H is false and unprovable, both sides are also equivalent. So, there does not seem to be any clue to determine whether or not H is provable or true.
  Yet, we can show it is actually provable.
- To this end, first let C denote the sentence "this sentence is consistent with T", i.e., $\mathrm{C} \leftrightarrow \neg\mathrm{Bew}_T(\overline{\ulcorner \neg\mathrm{C} \urcorner})$.
- Since the theory T$+\mathrm{C}$ proves its own consistency, it is inconsistent by the second incompleteness theorem. Thus, T proves $\neg\mathrm{C}$.
- On the other hand, since $\neg\mathrm{C} \leftrightarrow \mathrm{Bew}_T(\overline{\ulcorner \neg\mathrm{C} \urcorner})$, $\neg\mathrm{C}$ is the same as H, and therefore H is provable.

The above fact can be also stated as follows.

Theorem (Löb's theorem)

Let T be a consistent Σ_1 theory containing $\mathrm{I}\Sigma_1$. If T proves "if T proves σ, then σ", then T proves σ.

Proof.
Suppose T proves that "if T proves σ, then σ", which means that "if $\neg\sigma$, then T does not prove σ, that is, $T + \neg\sigma$ is consistent." That is, since $T + \neg\sigma$ proves the consistency of $T + \neg\sigma$, by the second incompleteness theorem, $T + \neg\sigma$ is inconsistent. Therefore, T proves σ. □

The Henkin sentence H satisfies that T proves "if T proves H, then H". So by the above theorem, T proves H.
A paradoxical fact derived from this theorem is that any proposition σ can be proven by assuming that there is a proof of σ.

Some commentaries on Gödel's theorem

- D. Hilbert and P. Bernays, Grundlagen der Mathematik I-II, Springer-Verlag, 1934-1939, 1968-1970 (2nd ed.). This gives the first complete proof of the second incompleteness theorem by analyzing the provability predicate.
- R.M. Smullyan, Theory of Formal Systems, revised edition, Princeton Univ. 1961. A classic masterpiece introducing recursive inseparability, etc.
- Handbook of Mathematical Logic (1977), edited by J. Barwise
  Smoryński's chapter on incompleteness theorems includes various unpublished results (particularly by Kreisel) and a wide range of mathematical viewpoints.
- P. Lindström, Aspects of Incompleteness, Lecture Notes in Logic 10, Second edition, Assoc. for Symbolic Logic, A K Peters, 2003.
  A technically advanced book. It has detailed information on Pour-El and Kripke's theorem (1967) that between any two recursive theories (including PA) there exists a recursive isomorphism that preserves propositional connectives and provability.

- R.M. Solovay (1976) studied modal propositional logic GL with $\mathrm{Bew}_T(x)$ as modality $\Box$, which is described by
  1. (1) $\vdash A \Rightarrow \vdash \Box A$,
  2. (2) $(\Box A \wedge \Box(A \to B)) \to \Box B$,
  3. (3) $\Box A \to \Box\Box A$,
  4. (4) $\Box(\Box A \to A) \to \Box A$
- The following two books are good on this topic.

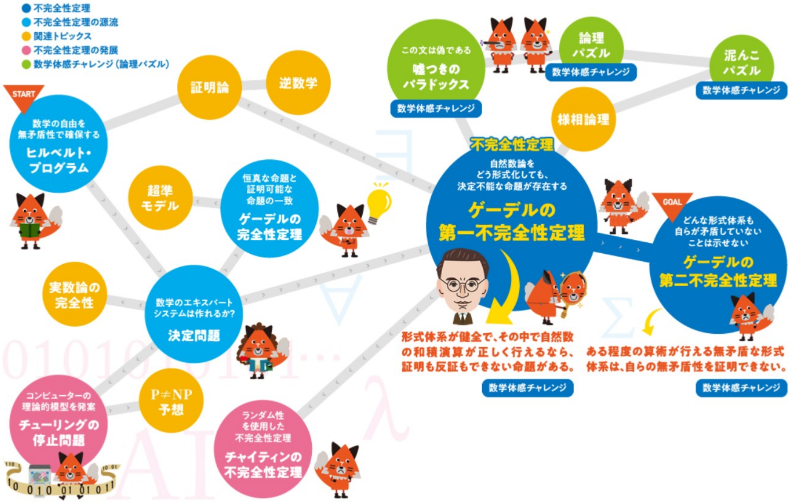
  Smoryński, Self-Reference and Modal Logic, Springer 1977.

  G. Boolos, The Logic of Provability, Cambridge 1993.

The following are excellent introductory books.

- T. Franzen, Gödel's Theorem: An Incomplete Guide to Its Use and Abuse(2005). On the use and misuse of the incompleteness theorem as a broader understanding of Godel's theorem. A Janpanse translation (with added explanations) by Tanaka (2011).
- P. Smith, Gödel's Without (Too Many) Tears, Second Edition 2022. https://www.logicmatters.net/resources/pdfs/GWT2edn.pdf Easy to read. The best reference to this lecture.

Math classroom: https://www.asahi.com/ads/math2022/



- Since Gödel, many researchers were looking for a proposition that has a natural mathematical meaning and is independent of Peano arithmetic, etc.

Jeff Paris

Leo Harrington

- Paris and Harrington found the first example in 1977. This is a slight modification of Ramsey's theorem in finite form.
- Following their findings, Kirby and Paris (1982) showed that the propositions on the Goodstein sequence and the Hydra game are independent of PA.
- H. Friedman showed that Kruskal's theorem (1982) and the Robertson-Seimor theorem in graph theory (1987) are independent of a stronger subsystem of second-order arithmetic, and also discovered various independent propositions for set theory.

Introduction

- So far we introduced Peano arithmetic PA and its subsystems, and proved their incompleteness and undecidability.
- Today, we will introduce a complete and decidable axiomatic system, called Presburger's system, which is obtained by removing multiplication from PA.
- Here, we use a powerful method called "elimination of quantifiers" to prove its completeness, which will also be used later.

First, we define the completeness and decidability of a theory.

Definition

- Let T be a theory in a language $\mathcal{L}$. T is **complete** if for every sentence σ in $\mathcal{L}$, $T \vdash \sigma$ or $T \vdash \neg\sigma$ holds.
- T is **decidable** if it is possible to determine whether $T \vdash \sigma$ or $T \nvdash \sigma$ by a finite means, that is, the set $\{\ulcorner\sigma\urcorner : T \vdash \sigma\}$ is computable.

- When we discuss the decidability of T, it is implicitly assumed that the symbol set $\mathcal{L}$ is countable, and so each formula φ has a unique Gödel number $\ulcorner\varphi\urcorner$.

The following facts show the basic relationship between "completeness" and "decidability."

Lemma

A complete Σ_1 theory T is decidable.

Proof.

- If T is inconsistent, it is decidable because all sentences can be proven. Therefore, T is assumed to be consistent.
- Since T is Σ_1, the set of (codes for) theorems of T is also Σ_1, that is, all theorems can be recursively listed. Since T is complete, for any proposition σ, either σ or $\neg\sigma$ will appear in the above list
- By the consistency of T, $T \vdash \neg\sigma$ iff $T \nvdash \sigma$. So, we can decide whether $T \vdash \sigma$ or $T \nvdash \sigma$ by checking whether σ or $\neg\sigma$ appears in the list). □

- Since most of axiomatic systems in mathematics are Σ_1 theories, we can show their decidability by checking their completeness.
- However, we should notice that there are many decidable Σ_1 theories that are incomplete (e.g. Abelian group theory).

Definition

Let T be a theory in a language $\mathcal{L}$. We say that T **admits elimination of quantifiers** if for any formula φ in language $\mathcal{L}$, there is an open formula (a formula with no quantifiers) ψ such that $T \vdash \varphi \leftrightarrow \psi$.

- In a theory that admits elimination of quantifiers, any formula can be transformed into a Boolean combination of atomic formulas. So, the truth value of a formula can be decided from those of the atomic formulas involved.
- However, it is not always possible to determine the truth values of atomic formulas. Indeed, by adding many complex atomic formulas, any theory can be modified to one that admits elimination of quantifiers.

Lemma

Any theory has a conservative extension that admits elimination of quantifiers.

Proof.

- Let T be a theory in a language $\mathcal{L}$.
- For every formula $\varphi(x_1, \dots, x_n)$ in $\mathcal{L}$, let R_φ be a new n-ary relation symbol. Then define T' as T added with the following axioms for all ϕ,

$$\forall x_1 \cdots \forall x_n (R_\varphi(x_1, \dots, x_n) \leftrightarrow \varphi(x_1, \dots, x_n))$$

- Since T' is an extension of T by definition, it is a conservative extension.
- Let ψ' be a formula in the extended language. Let ψ be a formula in $\mathcal{L}$ obtained from ψ' by replacing each R_φ in it with φ. Then, obviously, ψ' is equivalent to ψ in T', and thus it is also equivalent to R_ψ in T'. Therefore, T' admits elimination of quantifiers. □

Problem

Show that any theory T has a conservative extension T' which is a $\forall\exists$ theory and admits elimination of quantifiers.

A **basic formula** means an atomic formula or the negation of an atomic formula.
The following is a basic tool to check whether or not a theory admits elimination of quantifiers.

Lemma

- Let T be a theory in a language $\mathcal{L}$. If for any basic formulas $\alpha_1, \alpha_2, \ldots, \alpha_n$, there exists an open formula φ such that "$T \vdash \varphi \leftrightarrow \exists x(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n)$", then T admits elimination of quantifiers.
- Furthermore, supposing the negation of an atomic formula is equivalent to an open formula without negation, if for any atomic formulas $\alpha_1, \alpha_2, \ldots, \alpha_n$, there exists an open formula φ such that "$T \vdash \varphi \leftrightarrow \exists x(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n)$", then T admits elimination of quantifiers.

Proof. We eliminate all the universal quantifiers $\forall$ by $\forall x\varphi \leftrightarrow \neg\exists x\neg\varphi$.

- We first note that if a formula of the form $\exists x\theta$ (θ is open) is equivalent to an open formula, then T admits elimination of quantifiers.
- This can be easily shown by induction on the number of $\exists$ quantifiers appearing in a given formula φ. If φ has an $\exists$ quantifier, it has a subformula of the form $\exists x\theta$ (θ is open). So, if we replace that part with an equivalent open formula, we have a formula with less $\exists$ quantifiers that is equivalent to φ.

Lemma in lec02-03 of this course

Let T be a theory of $\mathcal{L}$, φ be a theory of T, and θ be a subformula of φ. Assume $T \vdash \theta \leftrightarrow \theta'$. Let φ' be a formula obtained from φ by replacing some (or all) occurrences of θ in φ with θ'. Then $T \vdash \varphi \leftrightarrow \varphi'$.

- Next, an open formula θ is transformed into the following **disjunctive normal form**

$$\theta \leftrightarrow (\alpha_{1,1} \wedge \alpha_{1,2} \wedge \cdots \wedge \alpha_{1,k_1}) \vee (\alpha_{2,1} \wedge \cdots \wedge \alpha_{2,k_2}) \vee \cdots \vee (\alpha_{m,1} \wedge \cdots \wedge \alpha_{m,k_m}),$$

where $\alpha_{i,j}$ is a basic formula.

- Since

$$\exists x((\alpha_{1,1} \land \cdots \land \alpha_{1,k_1}) \lor (\alpha_{2,1} \land \cdots \land \alpha_{2,k_2}) \lor \cdots \lor (\alpha_{m,1} \land \cdots \land \alpha_{m,k_m}))$$

$$\leftrightarrow \exists x(\alpha_{1,1} \land \cdots \land \alpha_{1,k_1}) \lor \cdots \lor \exists x(\alpha_{m,1} \land \cdots \land \alpha_{m,k_m}),$$

  if each part $\exists x(\alpha_{i,1} \land \cdots \land \alpha_{i,k_i})$ is equivalent to an open formula, then the whole formula is also equivalent to an open formula.

- Furthermore, we consider a theory where the negation of any atomic formula is equivalent to an open formula without negation.
- Then, any open formula is equivalent to an open formula without negation, hence also equivalent to a disjunctive normal form without negation.
- So, by the same argument as above, if for any atomic formulas $\alpha_1, \alpha_2, \ldots, \alpha_n$, $\exists x(\alpha_1 \land \alpha_2 \land \cdots \land \alpha_n)$ is equivalent to an open formula, then T admits elimination of quantifiers.

□

As the first example of a theory that admits elimination of quantifiers, we consider an theory of inequalities over the natural numbers $\mathsf{P}_<$. This is created by removing axioms A3 to A6 for $+$ and $\bullet$ from Peano arithmetic. Also note that for lack of $+$, the successive function is introduced as $\mathrm{S}(x) = x + 1$.

Definition

The theory $\mathsf{P}_<$ has a language $\mathcal{L}_<$ consisting of a constant symbol 0, a function symbol S, a binary relation $<$, and the following axioms.

S1. $\mathrm{S}(x) \neq 0$.
S2. $\mathrm{S}(x) = \mathrm{S}(y) \to x = y$.
S7. $x \not< 0$.
S8. $x < \mathrm{S}(y) \leftrightarrow x < y \lor x = y$.
S9. $\varphi(0) \land \forall x(\varphi(x) \to \varphi(\mathrm{S}(x))) \to \forall x \varphi(x)$, where $\varphi(x)$ is any $\mathcal{L}_<$ formula.

Lemma

In the theory $\mathsf{P}_<$, we can prove the following.

- $<$ is a linear order:

$$x < y \vee x = y \vee y < x \ ; \ x < y \to y \not< x \ ; \ (x < y \wedge y < z) \to x < z.$$

- S10. $y \neq 0 \to \exists x(\mathrm{S}(x) = y)$.

Leave the proof as an exercise.

Hints.

- By induction on x, prove $0 < \mathrm{S}(x)$, and by induction on y, prove $x < y \to \mathrm{S}(x) < \mathrm{S}(y)$.
- Then, prove $x < y \vee x = y \vee y < x$ by induction on x. Also, by induction on z, one can prove $x < y \wedge y < z \to x < z$.
- Next, by induction we show that $\mathrm{S}(x) \neq x$, and then by induction again we show that $x \not< x$, and obtain $x < y \to y \not< x$.
- S10 can be easily shown by induction on y.

Definition

Let the theory $\mathsf{P}^-_<$ be the linear ordering of $<$ + S7 + S8 + S10.

- As is clear from the definition, $\mathsf{P}^-_<$ is a subsystem of $\mathsf{P}_<$ and consists of a finite number of axioms.
- Therefore, the relationship between them is similar to that between PA and PA^-, but as shown below, $\mathsf{P}_<$ and $\mathsf{P}^-_<$ coincide.
- We show that $\mathsf{P}^-_<$ admits elimination of quantifiers, and then we derive that $\mathsf{P}^-_<$ is complete. As a result, $\mathsf{P}_<$ and $\mathsf{P}^-_<$ coincide.

Lemma

In the theory $\mathsf{P}^-_<$, we can prove the following.

- S1, S2 and
- S11. $\mathrm{S}^n(x) \neq x, \ \ n > 0$ ($\mathrm{S}^n(x)$ is abbrev. for $\overbrace{\mathrm{S}(\mathrm{S}(\cdots(\mathrm{S}}^{\text{repeat S } n \text{ times}}\ (x))\cdots)$.)

Theorem

The theory $\mathsf{P}^-_<$ admits elimination of quantifiers

Proof. To use lemma in Page 18, we first see that the negation of an atomic formula in the theory $\mathsf{P}^-_<$ can be expressed by an open formula without negation. The atomic formulas are in the following two forms:

$$\mathrm{S}^m(u) = \mathrm{S}^n(v) \text{ and } \mathrm{S}^m(u) < \mathrm{S}^n(v) \quad (u, v \text{ is constant 0 or a variable}).$$

By the linearity of $<$, their negation can be expressed as

$$\mathrm{S}^m(u) \neq \mathrm{S}^n(v) \leftrightarrow (\mathrm{S}^m(u) < \mathrm{S}^n(v)) \lor (\mathrm{S}^n(v) < \mathrm{S}^m(u)),$$
$$\mathrm{S}^m(u) \not< \mathrm{S}^n(v) \leftrightarrow (\mathrm{S}^m(u) = \mathrm{S}^n(v)) \lor (\mathrm{S}^n(v) < \mathrm{S}^m(u))$$

Therefore, to prove that $\mathsf{P}^-_<$ admits elimination of quantifiers, it suffices to show that for atomic formulas $\alpha_1, \alpha_2, \ldots, \alpha_k$, there is an open logical formula φ such that

$$\mathsf{P}^-_< \vdash \varphi \leftrightarrow \exists x(\alpha_1 \land \alpha_2 \land \cdots \land \alpha_k).$$

- Among the atomic formulas $\alpha_1, \alpha_2, \ldots, \alpha_k$, a formula without free variables x can be moved out of the scope of $\exists x$ easily. So, we ignore such a formula. Furthermore, $\mathrm{S}^m(x) = \mathrm{S}^n(x)$ and $\mathrm{S}^m(x) < \mathrm{S}^n(x)$ are equivalent to $\mathrm{S}^m(0) = \mathrm{S}^n(0)$ and $\mathrm{S}^m(0) < \mathrm{S}^n(0)$, respectively, and so can be treated as a formula without free variables x.
- Therefore, to consider elimination of quantifiers, we may assume that each atomic formula α_i has one of the following three forms

$$\mathrm{S}^m(x) = \mathrm{S}^n(u),\ \mathrm{S}^m(x) < \mathrm{S}^n(u),\ \mathrm{S}^m(u) < \mathrm{S}^n(x) \quad (u \text{ is 0 or a variable other than } x).$$

- First, consider the case in which $\alpha_1, \alpha_2, \ldots, \alpha_k$ includes an equation. For simplicity, we assume that α_1 is $\mathrm{S}^m(x) = \mathrm{S}^n(u)$.
- For each $i > 1$, define α_i' which is equivalent to α_i under α_1 as follows. $\alpha_i \equiv \mathrm{S}^l(x) \lesseqgtr \mathrm{S}^{l'}(v)$ ($\lesseqgtr$ is $=$, $<$, or $>$), then α_i is equivalent to $\mathrm{S}^{l+m}(x) \lesseqgtr \mathrm{S}^{l'+m}(v)$, and under α_1, also equivalent to $\mathrm{S}^{l+n}(u) \lesseqgtr \mathrm{S}^{l'+m}(v)$, denoted as α_i'.
- Since α_i' does not have a free variable x,

$$\mathsf{P}^-_< \vdash \exists x(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_k) \leftrightarrow \mathrm{S}^m(0) < \mathrm{S}^{n+1}(u) \wedge \alpha_2' \wedge \cdots \wedge \alpha_k',$$

and thus quantification can be eliminated.

- Next, we consider all α_i are in the form of $\mathrm{S}^m(u) < \mathrm{S}^n(v)$ (either u or v is x). Then, $\exists x(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_k)$ can be reformulated as

$$\exists x \bigwedge_{i,j} (s_i < \mathrm{S}^{m_i}(x) \wedge \mathrm{S}^{n_j}(x) < t_j),$$

where s_i, t_j are terms that do not include x.

- Then, the above formula is equivalent to

$$\exists x \bigwedge_{i,j} (\mathrm{S}^{n_j}(s_i) < \mathrm{S}^{m_i+n_j}(x) < \mathrm{S}^{m_i}(t_j))$$

and moreover it is equivalent to

$$\bigwedge_{i,j} (\mathrm{S}^{n_j+1}(s_i) < \mathrm{S}^{m_i}(t_j)) \wedge \bigwedge_{j} (\mathrm{S}^{n_j}(0) < t_j).$$

- Since this is an open formula, the quantification can be eliminated. □

Corollary

The theory $\mathsf{P}^-_<$ is complete. Therefore, it is decidable.

Proof.

- By the last theorem, any sentence in this language is equivalent to a disjunctive normal form consisting of atomic sentences $\mathrm{S}^m(0) = \mathrm{S}^n(0)$ or $\mathrm{S}^m(0) < \mathrm{S}^n(0)$.
- Obviously $m = n \Leftrightarrow \mathsf{P}^-_< \vdash \mathrm{S}^m(0) = \mathrm{S}^n(0)$ and $m \neq n \Leftrightarrow \mathsf{P}^-_< \vdash \mathrm{S}^m(0) \neq \mathrm{S}^n(0)$. Similarly for $\mathrm{S}^m(0) \not< \mathrm{S}^n(0)$.
- Thus, such a disjunctive normal form is provable in $\mathsf{P}^-_<$ iff it is true. Therefore, $\mathsf{P}^-_<$ is complete.
- $\mathsf{P}^-_<$ is decidable because this theory is Σ_1. □

The above corollary claims that the set of the theorems of $\mathsf{P}^-_<$ is computable, but in fact it is primitive recursive.

Corollary

The theory $\mathsf{P}^-_<$ and the theory $\mathsf{P}_<$ coinside. Therefore, the theory $\mathsf{P}_<$ also admits elimination of quantifiers, is complete and decidable.

Proof. If there is a theorem σ of theory $\mathsf{P}_<$ that is not provable in theory $\mathsf{P}^-_<$, then since $\mathsf{P}^-_<$ is complete, $\neg\sigma$ would be provable in $\mathsf{P}^-_<$. However, since $\mathsf{P}^-_<$ is a subsystem of $\mathsf{P}_<$, $\mathsf{P}_<$ also proves $\neg\sigma$, which is a contradiction. □

Problem 8

Let P_S be a theory in the language $\mathcal{L}_\mathrm{S}$ consisting only of the constant symbol 0 and a function symbol S as stated above, and having axioms S1, S2, S10, and S11. Show that this theory admits elimination of quantifiers, and is complete and decidable.

Next, we define Presburger system, which is obtained by adding addition to $\mathsf{P}^-_<$. [1]

Definition

Presburger arithmetic P_+ is a theory in $\mathcal{L}_+ = \{+, 0, 1, <\}$ consisting of the following axioms.

- A1. $\neg(x + 1 = 0)$.
- A2. $x + 1 = y + 1 \to x = y$.
- A3. $x + 0 = x$.
- A4. $x + (y + 1) = (x + y) + 1$.
- A7. $(x < 0)$.
- A8. $x < y + 1 \leftrightarrow x < y \lor x = y$.
- A9. $\varphi(0) \land \forall x(\varphi(x) \to \varphi(x + 1)) \to \forall x \varphi(x)$,
  where $\varphi(x)$ is any $\mathcal{L}_+$ formula and may include free variables other than x.

[1] It consists of axioms of PA without A5 and A6.

Problem 9

Show that the followings are provable in the theory P_+.

(1) Commutative monoid axiom regarding $+$.

(2) Difference axiom $x < y \rightarrow \exists z(z + x + 1 = y)$.

(3) Axiom of discrete linear order with 0 as the minimum element.

(4) The relation of operation and order $x < y \rightarrow x + z < y + z$.

(5) $\forall x \exists y \exists r < n(x = \overbrace{y + \cdots + y}^{n \text{ copies}} + r)$, for any natural number $n > 0$.

- P_+ and a theory of axioms (1) to (5) coincide, but the details are left to the students.

The theory P_+ does not admit elimination of quantifiers as it is.
For example, it seems difficult to rewrite a formula $\exists y(x = y + y)$, which means "x is an even number," as an open formula.

Now, we introduce the following relation $\equiv_m$ for each natural number m.

$$x \equiv_m y \Leftrightarrow \exists w(x = \overbrace{w + \cdots + w}^{m \text{ copies}} + y \vee y = \overbrace{w + \cdots + w}^{m \text{ copies}} + x).$$

We denote the language and theory obtained by adding this as $\mathcal{L}_{+,\equiv}$ and $\mathsf{P}_{+,\equiv}$, respectively.

Theorem

The theory $\mathsf{P}_{+,\equiv}$ admits elimination of quantifiers.

We also introduce some new notation which is just abbreviations rather than definitions of new symbols.

- First, $\overbrace{u + \cdots + u}^{k \text{ copies}}$ is written as ku (Multiplication is not introduced!). In particular, $k1$ is also written as k (previously, it was written as $\overline{k}$).
- We use subtraction $-$, e.g., $s_1 - s_2 < t_1 - t_2$, which formally represents $s_1 + t_2 < t_1 + s_2$.
- Thus, $x \equiv_m y$ is $\exists w(x - y = mw \vee y - x = mw)$.

Proof.

- First, we show that in the theory $\mathsf{P}_{+,\equiv}$, the negation of an atomic formula can be expressed as an open formula without negation.
- There are three forms of atomic formulas: $s = t$, $s < t$, and $s \equiv_m t$. Their negations can be expressed in $\mathsf{P}_{+,\equiv}$ as

$$s \neq t \leftrightarrow s < t \lor t < s,$$

$$s \not< t \leftrightarrow s = t \lor s < t,$$

$$s \not\equiv_m t \leftrightarrow s + 1 \equiv_m t \lor \cdots \lor s + (m-1) \equiv_m t.$$

- Therefore, to prove $\mathsf{P}_{+,\equiv}$ admits elimination of quantifiers, it sufficient to show that for atomic formula $\alpha_1, \alpha_2, \ldots, \alpha_l$ with free variables x, letting $\psi \equiv \alpha_1 \land \alpha_2 \land \cdots \land \alpha_l$, $\exists x \psi$ is equivalent to an open formula φ.

- To make it easier to see, we transform the atomic formulas $\alpha_1, \alpha_2, \ldots, \alpha_l$ into one of the following four forms

$$nx = t, \quad nx < t, \quad nx > t, \quad nx \equiv_m t,$$

where $n > 0$ and t is a term that does not include x.

- Note that an equality (or inequality) is equivalent to one obtained by multiplying both sides by a positive number. The congruence $x \equiv_m y$ is equivalent to $kx \equiv_{km} ky$ in $\mathsf{P}_{+,\equiv}$. So we may assume that the coefficients n of x (formally, the number of occurrences of x) in $\alpha_1, \alpha_2, \ldots, \alpha_l$ are all equal.
- Then, by replacing $y = nx$ in each expression, we have assertions about y instead of x. In addition, we need to add $y \equiv_n 0$ to an atomic formula of the conjunction.

- Based on the above arguments, we can assume that each atomic formula $\alpha_1, \alpha_2, \ldots, \alpha_l$ has one of the following forms (changing the variable y to x again)

$$x = t, \quad x < t, \quad x > t, \quad x \equiv_m t.$$

- If an equation $x = t$ appears in it, replace the equation with $t + 1 > 0$, and replace x in other formulas with t. Then we can obtain an equivalent and open conjunction that does not include x. Thus, we can eliminate $\exists x$.
- Hence, we assume that $\alpha_1, \alpha_2, \ldots, \alpha_l$ is one of the following.

$$x < t, \quad x > t, \quad x \equiv_m t.$$

So, we want to show the following is equivalent to an open formula

$$\exists x(\bigwedge_i r_i < x \wedge \bigwedge_j x < s_j \wedge \bigwedge_k x \equiv_{m_k} t_k).$$

- In the following, in order to keep the condition $x \geq 0$, we assume that $r_i = 0 - 1$ is included for some i.

- If $\bigwedge_k x \equiv_{m_k} t_k$ is not included, the above formula is equivalent to an open formula

$$\bigwedge_{i,j} r_i + 1 < s_j.$$

- Next, we assume $\bigwedge_k x \equiv_{m_k} t_k$ is included and let M be the least common multiple of all m_k.
- Then, since $x \equiv_{m_k} x \pm M$ for all k, if $\bigwedge_k x \equiv_{m_k} t_k$ has a solution x, then for any L, there is a solution x in the range $(L, L+M]$.
- Therefore, the given expression can be rewritten as follows.

$$\bigvee_{i_0} \bigvee_{0<p\leq M} (\bigwedge_i (r_i < r_{i_0} + p) \wedge \bigwedge_j (r_{i_0} + p < s_j) \wedge \bigwedge_k (r_{i_0} + p \equiv_{m_k} t_k)).$$

- Thus we prove that $\mathsf{P}_{+,\equiv}$ admits elimination of quantifiers. □

Corollary

Presburger arithmetic P_+ is complete. Therefore, it is decidable.

Proof. By the last theorem, it is easy to see that $\mathsf{P}_{+,\equiv}$ is complete. Since $\mathsf{P}_{+,\equiv}$ is a conservative extension of P_+, the completeness of P_+ follows. Then we immediately obtain that P_+ is decidable since it is Σ_1. □

- Similarly for the theory $\mathsf{P}_{<}^{-}$, the set of theorems of P_{+} is also primitively recursive.
- Peano arithmetic is obtained by adding the axiom of multiplication to P_{+}, but since Peano arithmetic is incomplete, we can see that multiplication cannot be defined in P_{+}.
- However, it is known that Th$((\mathbb{N}, \bullet))$ that involves only multiplication (though it cannot be expressed as simple axioms) is also computable, and therefore, addition cannot be defined by multiplication.
- According to A.L. Semenov (1980), the system that adds the exponential operation $2^{x+1} = 2^x + 2^x$ to the Presburger arithmetic P_{+} admits elimination of quantifiers if a logarithmic function is also added besides the congruence relations.

Problem 10

Show that the theory Th$(\mathbb{Q}, +, 0, 1, <)$ admits elimination of quantifiers.

Thank you for your attention!