Logique – cours 5

DER d'informatique

ENS Paris-Saclay

2ème semestre, 2025-2026

10. Elementary theories of arithmetic

Combining logic and recursive functions

Arithmetic

The signature of arithmetic is $\{\mathbf{0}, (-)', +, \cdot\}$, where $\mathbf{0}$ is a constant, $(-)'$ has arity 1, and $+$ and $\cdot$ have arity 2.

We will give the axioms of Robinson arithmetic. They say:

- $(-)'$ is injective and its image is everything but $\mathbf{0}$ (Q1–Q3),
- $+$ and $\cdot$ obey their inductive definitions on the right (Q4–Q7).

Elementary Peano arithmetic, in addition, adds a first-order induction axiom scheme.

Axioms of Robinson arithmetic

Q1	$\forall x \forall y (x' = y' \to x = y)$	successor is injective
Q2	$\forall x\ \mathbf{0} \neq x'$	zero is not in the image of successor
Q3	$\forall x (x \neq \mathbf{0} \to \exists y\ x = y')$	everything else is in the image of successor
Q4	$\forall x (x + \mathbf{0} = x)$	zero is neutral on the right of plus
Q5	$\forall x (x + y' = (x + y)')$	inductive definition of right-plus
Q6	$\forall x (x \cdot \mathbf{0} = \mathbf{0})$	zero is absorbing on the right of times
Q7	$\forall x (x \cdot y' = (x \cdot y) + x)$	inductive definition of right-times

Robinson arithmetic, Q, is the theory obtained from (Q1)–(Q7) by deductive closure.

Elementary Peano arithmetic

The induction axiom for a formula φ and variable x free in φ is

$\mathsf{Ind}_{\varphi,x}$ $[\varphi(\mathbf{0}) \wedge \forall x(\varphi(x) \to \varphi(x'))] \to \forall x \varphi(x)$.

Elementary Peano arithmetic, PA, is the theory obtained by deductive closure from (Q1)–(Q7) together with $\mathsf{Ind}_{\varphi,x}$ for all formulas φ and free variables x in φ.

The standard model of arithmetic

The standard model of arithmetic is the structure $\mathcal{N}$ based on $\mathbb{N}$, in which $\mathbf{0}$ is interpreted as 0, n' as $n+1$ for every $n \in \mathbb{N}$, and $+$ and $\cdot$ as the addition and multiplication functions, respectively.

Clearly, $\mathcal{N} \models \mathsf{Q}$ and $\mathcal{N} \models \mathsf{Ind}_{\varphi,x}$ for all φ and x, so $\mathcal{N} \models \mathsf{PA}$.

Skolem's theorem shows that there exist countable non-standard models of PA (and thus also of Q).

A non-standard model of Robinson arithmetic

Define a model $\mathcal{S}$ on $S := \mathbb{N} \sqcup \{a, b\}$ by extending the functions $(-)', +, \cdot$ as follows, for any $x \in S$,

- $a' := a$ and $b' := b$,
- $x + a := b$ and $x + b := a$,
- $a + x := \begin{cases} b \text{ if } x = a \\ a \text{ otherwise,} \end{cases} \qquad b + x := \begin{cases} a \text{ if } x = b \\ b \text{ otherwise,} \end{cases}$
- $x \cdot a := \begin{cases} b \text{ if } x = a \\ a \text{ otherwise,} \end{cases} \qquad x \cdot b := \begin{cases} a \text{ if } x = b \\ b \text{ otherwise,} \end{cases}$
- $a \cdot x := \begin{cases} 0 \text{ if } x = 0 \\ b \text{ otherwise,} \end{cases} \qquad b \cdot x := \begin{cases} 0 \text{ if } x = 0 \\ a \text{ otherwise.} \end{cases}$

Exercise. Show that $\mathcal{S}$ is a well-defined model of Q.

Weakness of Robinson arithmetic

The model $\mathcal{S}$ shows that none of the following sentences are in Q:

1. $\forall x(x \neq x')$ — successor has no fixpoints
2. $\forall x \forall y \forall z((x + y) + z = x + (y + z))$ — plus associative
3. $\forall x \forall y(x + y = y + x)$ — plus commutative
4. $\forall x(\mathbf{0} + x = x)$ — zero neutral on the left of plus
5. $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$ — times associative
6. $\forall x \forall y(x \cdot y = y \cdot x)$ — times commutative
7. $\forall x(\mathbf{0} \cdot x = \mathbf{0})$ — zero absorbing on the left of times
8. $\forall x \forall y \forall z(x \cdot (y + z) = x \cdot y + x \cdot z)$ — times distributes over plus.

All of these are in PA. Conclusion: their proofs require Ind-axioms.

Robinson arithmetic is incomplete

Proposition

Q is incomplete.

Proof.

Let $\varphi := \forall x(\mathbf{0} + x = x)$.

We just saw that $\nvdash_Q \varphi$, using the model $\mathcal{S}$ of Q.

Also, $\nvdash_Q \neg\varphi$, since φ is true in the standard model $\mathcal{N}$ of Q. ■

Remark

This is *not* Gödel's incompleteness theorem.

Numerals are provably injective

Lemma

Let $n, s \in \mathbb{N}$. If $n \neq s$, then $\vdash_{\mathsf{Q}} \mathbf{n} \neq \mathbf{s}$.

Proof.

By induction on n.

$n = 0$. If $0 \neq s$, then $\mathbf{s} = \mathbf{t}'$, with $t := s - 1$. By (Q2), $\vdash_{\mathsf{Q}} \mathbf{0} \neq \mathbf{t}'$.

$n = k + 1$. Then $\mathbf{n} = \mathbf{k}'$. Suppose $n \neq s$. There are two cases:

- $s = 0$. In this case, by (Q2), $\vdash_{\mathsf{Q}} \mathbf{k}' \neq \mathbf{0}$.
- $s = t + 1$. Then $k \neq t$. By the induction hypothesis, $\vdash_{\mathsf{Q}} \mathbf{k} \neq \mathbf{t}$. By (Q1), $\vdash_{\mathsf{Q}} \mathbf{k}' \neq \mathbf{t}'$. ■

Note. We used induction in our metatheory to prove the lemma.

We did not use any induction axioms inside Q.

Representation of functions and relations

Let T be a theory whose signature contains $\mathbf{0}$ and $'$, and $n \geq 0$.

Let $f : \mathbb{N}^n \to \mathbb{N}$ be a function. A formula $\varphi(x_1, \ldots, x_n, y)$ represents f in T if, for any $(p_1, \ldots, p_n) \in \mathbb{N}^n$,

$$\text{if } f(p_1, \ldots, p_n) = q, \text{ then } \vdash_T \forall y(\varphi(\mathbf{p_1}, \ldots, \mathbf{p_n}, y) \leftrightarrow y = \mathbf{q}).$$

Let $R \subseteq \mathbb{N}^n$. A formula $\varphi(x_1, \ldots, x_n)$ represents R in T if, for any $(p_1, \ldots, p_n) \in \mathbb{N}^n$,

$$\text{if } (p_1, \ldots, p_n) \in R \text{ then } \vdash_T \varphi(p_1, \ldots, p_n), \text{ and}$$
$$\text{if } (p_1, \ldots, p_n) \notin R \text{ then } \vdash_T \neg\varphi(p_1, \ldots, p_n).$$

Robinson arithmetic represents recursive functions and sets

We just saw that Q is a weak theory of arithmetic. Still:

Theorem

Any recursive function or set is representable in Q.

Recursive functions

A recursive function is inductively defined as follows:

- the constant zero function $\mathbb{N} \to \mathbb{N}$ is recursive;
- the successor function $\mathbb{N} \to \mathbb{N}$ is recursive;
- for each $1 \leq i \leq k$, the i^{th} projection $\pi_i^k : \mathbb{N}^k \to \mathbb{N}$ is recursive;
- the composition $f \circ \langle g_1, \ldots, g_\ell \rangle$ is recursive, for any recursive $f : \mathbb{N}^\ell \to \mathbb{N}$ and $g_1, \ldots, g_\ell : \mathbb{N}^k \to \mathbb{N}$;
- for any recursive $f : \mathbb{N}^k \to \mathbb{N}$ and $g : \mathbb{N}^{k+2} \to \mathbb{N}$, the function $h : \mathbb{N}^{k+1} \to \mathbb{N}$ defined by primitive recursion is recursive:

$$h(\bar{p}, 0) := f(\bar{p}) \quad \text{and} \quad h(\bar{p}, n+1) := g(\bar{p}, n, h(\bar{p}, n)) \ ;$$

- for any regular recursive $f : \mathbb{N}^{k+1} \to \mathbb{N}$, the minimization of f, $\mu f : \mathbb{N}^k \to \mathbb{N}$, is recursive,

where $k, \ell, n \in \mathbb{N}$.

Regular minimization

A function $f : \mathbb{N}^{k+1} \to \mathbb{N}$ is regular if, for every $\bar{p} \in \mathbb{N}^k$, there exists $n \in \mathbb{N}$ such that $f(\bar{p}, n) = 0$. (unrelated to 'regular language')

For a regular function $f : \mathbb{N}^{k+1} \to \mathbb{N}$, we define its minimization at $\bar{p} \in \mathbb{N}^k$ to be the minimal $n \in \mathbb{N}$ such that $f(\bar{p}, n) = 0$, that is,

$$\mu f(\bar{p}) := \min\{n \in \mathbb{N} \mid f(\bar{p}, n) = 0\} \ .$$

Remark

The minimization of a regular function is always total.

We will not need to consider partial recursive functions.

Recursive functions and Turing machines

Theorem

Let $f : \mathbb{N} \to \mathbb{N}$ be a function. Then

f is recursive

if, and only if,

there exists a Turing machine M such that, for every $n \in \mathbb{N}$, upon input n, the machine M halts, with $f(n)$ written on its tape.

Proof.

See the Computability course (first semester). ■

Recursive predicates

Let $k \geq 1$ and $S \subseteq \mathbb{N}^k$.

The set S is recursively enumerable if there exists a recursive function $f : \mathbb{N} \to \mathbb{N}^k$ with $\mathrm{im}(f) = S$.

The set $S \subseteq \mathbb{N}^k$ is recursive (a.k.a. decidable) if its characteristic function $\chi_S : \mathbb{N}^k \to \mathbb{N}$ is recursive, where

$$\chi_S(x_1, \ldots, x_k) := \begin{cases} 1 & \text{if } (x_1, \ldots, x_k) \in S, \\ 0 & \text{otherwise.} \end{cases}$$

Fact

A set S is recursive if, and only if, both S and $\mathbb{N}^k \setminus S$ are recursively enumerable.

The proof that recursive functions are representable in Q

. . . is not very difficult, but quite long and technical.

11. Incompleteness

Computably characterizing arithmetic is impossible

Context

- Cantor (1878) formulates the Continuum Hypothesis: any infinite set $S \subseteq \mathbb{R}$ is in bijection with either $\mathbb{N}$ or $\mathbb{R}$.
- Zermelo (1899) and Russell (1901) realize that unrestricted set comprehension lets one define the set:

$$S := \{x \mid x \notin x\}$$

  leading to a proof of $\bot$.
- Zermelo (1908) formulated a consistent set theory.
- Hilbert's Consistency Program (1920): to prove, in a finitistic way, that mathematics is consistent.
- Entscheidungsproblem (Hilbert and Ackermann, 1928): does there exist a decision procedure for provability?

Theorem (Gödel's First Incompleteness Theorem)

Let T be a consistent recursively axiomatizable theory extending Robinson arithmetic Q.

Then there exists a sentence φ which is independent from T.

Theorem (Gödel's Second Incompleteness Theorem)

Let T be a consistent theory which extends Q and admits a provability predicate, Pr. Then

$$T \nvdash \neg \mathsf{Pr}(\ulcorner \bot \urcorner) \ .$$

Plan

- We will prove the First Theorem.
- For the Second Theorem, we will only outline a proof.
- We mostly follow Boolos and Jeffrey 1989, and Smith 2020.
- We first define precisely what 'recursively axiomatizable' means.

Gödel numbering

Let L be a countable signature and let V be a countable set of variables.

The set $\mathrm{Form}(L, V)$ of formulas is countable: there exists a surjective function $\mathbb{N} \to \mathrm{Form}(L, V)$.

A Gödel numbering is a computable injective function $\mathrm{Form}(L, V) \to \mathbb{N}$, whose image is a recursive set.

Formulas as strings

Let L be the signature which contains, for every $k \geq 0$, a countable set of function symbols of arity k, $F_k = \{f_n^{(k)} : n \in \mathbb{N}\}$, and a countable set of relation symbols of arity k, $P_k = \{R_n^{(k)} : n \in \mathbb{N}\}$.

Let V be the set of variables $\{x_n : n \in \mathbb{N}\}$.

Let Σ be the union of V, F, P, and $\{(,), \wedge, \neg, \exists, \forall, =\} \cup \{,\}$.

A formula in signature L and variables V can be viewed as a string over Σ^+. Note: the alphabet is infinite, but this could be avoided.

For readability, we write $x := x_0$, $y := x_1$ $\mathbf{0} := f_0^{(0)}$, $(-)' := f_0^{(1)}$, $+ := f_0^{(2)}$, and $\cdot := f_1^{(2)}$, and we use usual postfix and infix notations for these.

A Gödel numbering

Define $\gamma_0 : \Sigma \to \{1,2,3,4,5,6,7,8,9\}^+$ as follows:

s	(	)	,	$\wedge$	$\bot$	$\neg$	$\exists$	$\forall$	$=$	x_n	$f_n^{(k)}$	$R_n^{(k)}$
$\gamma_0(s)$	1	2	29	3	39	399	4	49	499	59^n	$68^k 9^n$	$78^k 9^n$

For any non-empty string $w = w_0 \dots w_\ell$ in alphabet Σ, define $\gamma(w)$ to be the natural number denoted by $\gamma_0(w_0) \dots \gamma_0(w_\ell)$.

For example, the string '$\exists x(x =$' is sent to 4515499 by γ.

Exercise. γ, restricted to $\mathrm{Form}(L, V)$, is a Gödel numbering.

Recursivity of formula sets

From now on: we fix the signature L, the set of variables V, and a Gödel numbering γ as above.

We call a subset $S \subseteq \mathrm{Form}(L, V)$ recursive or decidable if $\gamma[S]$ is recursive, and recursively enumerable if $\gamma[S]$ is recursively enumerable.

Recursive axiomatizations

Let T be a theory.

A set $S \subseteq T$ is an axiomatization of T if T is the deductive closure of S.

The theory T is recursively axiomatizable if there exists a recursive set of sentences S which is an axiomatization of T.

Diagonalization

For any formula φ, define $\ulcorner \varphi \urcorner$ to be the numeral of $\gamma(\varphi)$.

The diagonalization of φ is the formula Δ_φ defined as

$$\exists x(x = \ulcorner \varphi \urcorner \wedge \varphi) \ .$$

For any $n \in \mathbb{N}$, define $\delta(n) := \begin{cases} \gamma(\Delta_\varphi) & \text{if } n = \gamma(\varphi), \\ 0 & \text{otherwise.} \end{cases}$

Lemma

The function δ is recursive.

Proof.

Let $n \in \mathbb{N}$. First check whether $n = \gamma(\varphi)$ for some formula φ. If so, then $\gamma(\Delta_\varphi) = 4515499\ k\ 3\ n\ 2$, where $k := \gamma(\mathbf{n})$. ■

Lemma (Diagonal Lemma)

Let T be a theory in which δ is representable. For any formula $\varphi(y)$, there exists a sentence G such that

$$\vdash_T G \leftrightarrow \varphi(\ulcorner G \urcorner) .$$

Proof.

Let $D(x, y)$ be a formula representing δ.

Define $F := \exists y(D(x, y) \wedge \varphi(y))$, and $n := \gamma(F)$.

Define $G := \exists x(x = \mathbf{n} \wedge F)$, i.e., G is the diagonalization of F.

Now $\vdash G \leftrightarrow F[\mathbf{n}/x]$, and $F[\mathbf{n}/x] = \exists y(D(\mathbf{n}, y) \wedge \varphi(y))$. $(\star)$

Write $k := \gamma(G)$. Then $\delta(n) = \gamma(\Delta_F) = k$ and $\ulcorner G \urcorner = \mathbf{k}$.

Since D represents δ, $\vdash_T \forall y(D(\mathbf{n}, y) \leftrightarrow y = \mathbf{k})$.

Thus by $(\star)$, $\vdash_T G \leftrightarrow \exists y(y = \mathbf{k} \wedge \varphi(y))$, so $\vdash_T G \leftrightarrow \varphi(\mathbf{k})$. ■

Lemma (Non-self-representability)

Let T be an extension of Q and suppose $\gamma[T]$ is representable in T. Then T is inconsistent.

Proof.

Since δ is recursive, δ is representable in Q, and thus also in T.
Suppose the formula $\varphi(y)$ represents $\gamma[T]$ in Q, and thus in T.
By the diagonal lemma, pick a sentence G such that

$$\vdash_T G \leftrightarrow \neg\varphi(\ulcorner G \urcorner) \ .$$

Let $k := \gamma(G)$, so that $\vdash_T G \leftrightarrow \neg\varphi(\mathbf{k})$ $(\star)$.
We claim that $\vdash_T G$. Towards a contradiction, suppose $\nvdash_T G$.
Then $k \notin \gamma[T]$ since γ is injective. Since φ defines $\gamma[T]$, $\vdash_T \neg\varphi(\mathbf{k})$. But then, by $(\star)$, $\vdash_T G$, contradiction.
Since $\vdash_T G$, we have $k \in \gamma[T]$. As φ defines $\gamma[T]$, $\vdash_T \varphi(\mathbf{k})$.
By $(\star)$, we get $\vdash_T \neg G$. So $\vdash_T \bot$. ■

Undecidability of arithmetic theories

Theorem

There does not exist a consistent, decidable extension of Q.

Proof.

Let T be a decidable theory extending Q. By definition, $\gamma[T]$ is a recursive set of numbers. Since decidable sets are representable in Q, in particular $\gamma[T]$ is representable in Q, and thus in T.
By the non-self-representability lemma, T is inconsistent. ■

Corollary

The theories Q, PA, and $\mathrm{Th}(\mathcal{N})$ are undecidable.

The Entscheidungsproblem is unsolvable

Theorem

There does not exist an algorithm that decides whether or not a formula φ is provable in first-order logic (without axioms).

Proof.

Let θ be the conjunction of the seven axioms of Q.
Towards a contradiction, suppose there were an algorithm A for provability in first-order logic.
We obtain an algorithm for deciding Q: given a sentence ψ, use A to determine whether or not $\vdash \theta \to \psi$. By the deduction theorem, this is equivalent to $\vdash_{\mathsf{Q}} \psi$. ■

Note. An alternative, more direct proof, due to Turing, expresses the halting problem for a machine M as a first-order sentence φ_M.

Gödel I

Theorem (Gödel's First Incompleteness Theorem)

Let T be a consistent recursively axiomatizable theory which contains Robinson arithmetic Q.
Then there exists a sentence φ which is independent from T.

Proof.

Since T is recursively axiomatizable, T is recursively enumerable.
If T were also complete, then T would have to be decidable.
But this contradicts the fact that all consistent extensions of Q are undecidable. ■

Corollary

There does not exist a recursive axiomatization of $\mathrm{Th}(\mathcal{N})$.

Two remarks

- One often sees more vague and more general-sounding statements, such as: 'any sufficiently strong theory is incomplete'. These can be made precise using a notion of first-order interpretation: if Q is interpretable in a consistent recursively axiomatizable theory T, then T is incomplete.

- Our proof of Gödel I did not construct an independent sentence.