

PROOF THEORY OF ARITHMETIC
Lecture 2 – Peano Arithmetic

Anupam Das

University of Birmingham

34TH EUROPEAN SUMMER SCHOOL
IN LOGIC, LANGUAGE AND INFORMATION

Ljubljana, Slovenia

8 August 2023



These slides are available at <http://www.anupamdas.com/ess11i23>.

- 1 First-order arithmetic and Robinson's axioms
- 2 Induction and Peano's axioms
- 3 Sequent calculus formulation
- 4 Break: exercises and questions
- 5 Digging deeper: formalisation and soundness

The **language of arithmetic** \mathcal{L}_A is a first-order vocabulary, given by,

$$\mathcal{L}_A := \{0, s, +, \times\}$$

where:

- 0 is a constant symbol.
- s is a unary function symbol.
- + is a binary function symbol, written infix.
- \times is a binary function symbol, written infix.

We *always include equality* =.

We will use logical symbols $\perp, \top, \vee, \wedge, \rightarrow, \leftrightarrow, \exists, \forall$ as usual.

We shall *identify* each $n \in \mathbb{N}$ with the (closed) term $\overbrace{s \cdots s}^n 0$.

NB: All theories and structures will be over \mathcal{L}_A , unless otherwise specified.

(Blank slide)

The 'standard model'

Write \mathfrak{N} for the **structure** given by:

- The domain $|\mathfrak{N}|$ of \mathfrak{N} is \mathbb{N} .
- $0^{\mathfrak{N}} := 0 \in \mathbb{N}$.
- $s^{\mathfrak{N}} : \mathbb{N} \rightarrow \mathbb{N}$ by $n \mapsto n + 1$.
- $+^{\mathfrak{N}} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ by $(m, n) \mapsto m + n$.
- $\times^{\mathfrak{N}} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ by $(m, n) \mapsto mn$.

As usual, $=$ is interpreted as **true equality**.

Remark

There are all sorts of other '**non-standard**' \mathcal{L}_A -structures, but we shall (mostly) not concern ourselves with them.

(Blank slide)

Robinson arithmetic

Q is the theory axiomatised by the **universal closures** of:

- $\neg sx = 0$
- $sx = sy \rightarrow x = y$
- $x = 0 \vee \exists y x = sy$

- $x + 0 = x$
- $x + sy = s(x + y)$
- $x \times 0 = 0$
- $x \times sy = x \times y + x$

} $(S, 0)$ form a free algebra.

} prim. rec. defns.
of $+, \times$

$\forall x, y, \dots$

$\mathcal{L}_A + \{P\}$

$p0 = 0$

$psx = x$

Convention

We henceforth speak of axioms and theorems that are **open formulas** (i.e. with free variables). These should always be interpreted as their **universal closures**.

Proposition (Soundness)

$\mathfrak{N} \models Q$.

But Q is **very weak** and admits many non-standard models.

Exercise

- Show that $\mathbb{N} \cup \{\infty\}$ with $s\infty = \infty$ extends to a model of Q.
- Show that $\mathbb{N} \cup \{\infty_0, \infty_1\}$ with
 - $\infty_0 + n = \infty_0$ and $\infty_1 + n = \infty_1$, for all $n \in \mathbb{N}$; but,
 - $n + \infty_0 = \infty_1$ and $n + \infty_1 = \infty_0$, for all $n \in \mathbb{N}$.
- Conclude that Q does **not prove commutativity** of $+$, i.e. $x + y = y + x$.

(Blank slide)

Upper bounds for Q

On the other hand, Q is still strong enough to formalise a lot of basic (meta)mathematics.

Incompleteness

Q proves each instance of the *Diagonal Lemma*, and its provability predicate satisfies the *HBL conditions*. Thus Q is **incomplete**.

Theorem (Σ_1 -completeness (weak version))

If $\mathfrak{N} \models \exists x\varphi(x)$, where $\varphi(x)$ is *quantifier-free* with only free variable x , then $Q \vdash \exists x\varphi(x)$.

NB: trying to prove this directly by induction on the structure of $\varphi(x)$ **does not work**. We need some intermediate machinery.

De Morgan normal form

The **De Morgan** formulas are generated by:

$$\varphi, \psi ::= s = t \mid s \neq t \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \exists x \varphi \mid \forall x \varphi$$

We extend **negation** $\bar{\cdot}$ to all formulas by:

- $\overline{t = u} := t \neq u$
- $\overline{t \neq u} := t = u$
- $\overline{\varphi \vee \psi} := \bar{\varphi} \wedge \bar{\psi}$
- $\overline{\varphi \wedge \psi} := \bar{\varphi} \vee \bar{\psi}$.
- $\overline{\exists x \varphi} := \forall x \bar{\varphi}$
- $\overline{\forall x \varphi} := \exists x \bar{\varphi}$

Proposition

Every formula is *logically equivalent* to one in De Morgan form.

(Blank slide)

Logical complexity

While we are here we may as well strengthen the statement of Σ_1 -completeness.

Definition (Bounded quantification)

Write $t \leq u := \exists x t + x = u$. A **bounded quantifier** is $\exists x \leq t$ or $\forall x \leq t$, where:

- $\exists x \leq t \varphi := \exists x (x \leq t \wedge \varphi)$; and,
- $\forall x \leq t \varphi := \forall x (x \leq t \rightarrow \varphi)$.

A formula is **bounded** if it has only bounded quantifiers.

Definition (Arithmetical hierarchy)

- $\Delta_0 = \Sigma_0 = \Pi_0$ is the set of bounded formulas.
- $\Sigma_{n+1} := \{\exists \vec{x} \varphi : \varphi \in \Pi_n\}$
- $\Pi_{n+1} := \{\forall \vec{x} \varphi : \varphi \in \Sigma_n\}$.

$$\Delta_n := \Sigma_n \cap \Pi_n$$

$$\frac{\Sigma_n}{\exists \vec{x}_n \forall \vec{x}_{n-1} \dots \forall \vec{x}_1 \varphi_0}$$

bounded

e.g. $\exists x \varphi(x) \vee \exists y \psi(y)$
 $\equiv \exists z (\varphi(z) \vee \psi(z))$

Exercise

- Show that $\varphi \in \Sigma_n$ if and only if $\bar{\varphi} \in \Pi_n$.
- Show that Σ_n and Π_n are closed under \vee and \wedge , up to logical equivalence.
- Conclude that each formula is logically equivalent to one in some Σ_n or Π_n .

(Blank slide)

Σ_1 completeness, revisited

Lemma (Q decides bounded formulas)

If $\varphi \in \Delta_0$ is closed, then either $\mathbb{Q} \vdash \varphi$ or $\mathbb{Q} \vdash \bar{\varphi}$.

Proof idea.

By induction on the structure of φ .



Exercise

Complete this proof formally.

Theorem (Σ_1 -completeness)

If $\varphi \in \Sigma_1$ is closed and $\mathfrak{N} \models \varphi$, then $\mathbb{Q} \vdash \varphi$.

Proof.

- Write $\varphi = \exists \vec{x} \psi(\vec{x})$ for $\psi(\vec{x}) \in \Delta_0$.
- Since $\mathfrak{N} \models \varphi$ we have $\vec{n} \in \mathbb{N}$ such that $\mathfrak{N} \models \psi(\vec{n})$.
- By Lemma above, and Soundness of Q for \mathfrak{N} , we have $\mathbb{Q} \vdash \psi(\vec{n})$.
- Thus, by pure logic, $\mathbb{Q} \vdash \exists \vec{x} \psi(\vec{x})$, as required.



(Blank slide)

- 1 First-order arithmetic and Robinson's axioms
- 2 Induction and Peano's axioms**
- 3 Sequent calculus formulation
- 4 Break: exercises and questions
- 5 Digging deeper: formalisation and soundness

The **induction axiom** for a formula $\varphi(x)$ is:

$$\underline{\text{ind}(\varphi)} : \varphi(0) \rightarrow (\forall x(\varphi(x) \rightarrow \varphi(sx)) \rightarrow \forall x\varphi(x))$$

Definition (Peano Arithmetic)

PA is the theory axiomatised by Q and $\text{ind}(\varphi)$ for all formulas φ .

can have free vars.

We better state:

Proposition (Soundness)

$\mathfrak{N} \models \text{PA}$.

(We will discuss this further later.)

Exercise

Show that the axiom $x = 0 \vee \exists y x = sy$ of Q can be derived using induction and the other axioms of Q.

(Blank slide)

Example: addition is commutative

Lemma (Mirrored definition of +)

PA proves:

- $0 + y = y$
- $sx + y = s(x + y)$

Proof idea.

By induction on y . □

Proposition (Commutativity of +)

PA proves that + is commutative, i.e. $PA \vdash x + y = y + x$.

In particular, note that this means that $Q \subsetneq PA$.

Proof idea.

By induction on x . □

Exercise

Show furthermore that PA proves that \times is commutative. What about associativity? How logically complex are the induction instances needed to prove all these?

(Blank slide)

$$\textcircled{1} \quad \underline{PA \vdash 0 + y = y}$$

$$\begin{array}{l} \text{ind on } y \quad 0 + \underline{0} = 0 \quad \text{by } Q \\ \quad \quad \quad 0 + sy = s(0 + y) \quad \text{by } Q \\ \quad \quad \quad = sy \quad \text{by IH} \end{array}$$

$$\textcircled{2} \quad \underline{PA \vdash sx + y = s(x + y)}$$

$$\begin{array}{l} \text{ind on } y \quad sx + 0 = sx \quad \text{by } Q \\ \quad \quad \quad = s(x + 0) \quad \text{by } Q \\ \quad \quad \quad sx + sy = s(\underline{sx + y}) \quad \text{by } Q \\ \quad \quad \quad = ss(x + y) \quad \text{by IH} \\ \quad \quad \quad = s(x + sy) \quad \text{by } Q \end{array}$$

$$\underline{PA \vdash x + y = y + x}$$

$$\begin{array}{l} \text{ind on } x: \quad 0 + y = y \quad \text{by } \textcircled{1} \\ \quad \quad \quad = y + 0 \quad \text{by } Q \end{array}$$

$$sx + y =$$

(Blank slide)

- 1 First-order arithmetic and Robinson's axioms
- 2 Induction and Peano's axioms
- 3 Sequent calculus formulation**
- 4 Break: exercises and questions
- 5 Digging deeper: formalisation and soundness

We shall henceforth work exclusively with formulas in **De Morgan form**.

Definition (Sequents)

A **sequent**, written Γ, Δ etc., is a **set of formulas**.

For a sequent Γ with free variables \vec{x} , its **(formula) interpretation** is:

$$[\Gamma] := \forall \vec{x} \bigvee \Gamma$$

We will simply use commas ‘,’ for set union and omit braces, e.g. writing:

- Γ, Δ for $\Gamma \cup \Delta$; and,
- Γ, φ for $\Gamma \cup \{\varphi\}$.

We shall henceforth work exclusively with formulas in **De Morgan form**.

Definition (Sequents)

A **sequent**, written Γ, Δ etc., is a **set of formulas**.

For a sequent Γ with free variables \vec{x} , its **(formula) interpretation** is:

$$[\Gamma] := \forall \vec{x} \bigvee \Gamma$$

We will simply use commas ‘,’ for set union and omit braces, e.g. writing:

- Γ, Δ for $\Gamma \cup \Delta$; and,
- Γ, φ for $\Gamma \cup \{\varphi\}$.

Definition (Calculus for PA)

The **judgement** $\vdash_{\text{PA}} \Gamma$ is defined over the next few slides...

Rules for first-order logic (without equality)

The rules for first-order logic (without equality) are those of the usual **one-sided** sequent calculus:

$$\begin{array}{c} \text{id} \frac{}{\vdash_{\text{PA}} s = t, s \neq t} \quad \text{w} \frac{\vdash_{\text{PA}} \Gamma}{\vdash_{\text{PA}} \Gamma, \Gamma'} \quad \text{cut} \frac{\vdash_{\text{PA}} \Gamma, \varphi \quad \vdash_{\text{PA}} \Gamma', \bar{\varphi}}{\vdash_{\text{PA}} \Gamma, \Gamma'} \\ \\ \vee \frac{\vdash_{\text{PA}} \Gamma, \varphi_0 \vee \varphi_1, \varphi_i}{\vdash_{\text{PA}} \Gamma, \varphi_0 \vee \varphi_1} \quad i \in \{0, 1\} \quad \wedge \frac{\vdash_{\text{PA}} \Gamma, \varphi \quad \vdash_{\text{PA}} \Gamma, \psi}{\vdash_{\text{PA}} \Gamma, \varphi \wedge \psi} \\ \\ \exists \frac{\vdash_{\text{PA}} \Gamma, \exists x \varphi(x), \varphi(t)}{\vdash_{\text{PA}} \Gamma, \exists x \varphi(x)} \quad \forall \frac{\vdash_{\text{PA}} \Gamma, \varphi(y)}{\vdash_{\text{PA}} \Gamma, \forall x \varphi(x)} \quad y \text{ fresh} \end{array}$$

Exercise (η -expansion)

Using only the rules on this slide, show $\vdash_{\text{PA}} \varphi, \bar{\varphi}$ for any φ .

Exercise (Drinker's Paradox)

Using only the rules on this slide, show $\vdash_{\text{PA}} \exists x (\varphi(x) \rightarrow \forall y \varphi(y))$, for any $\varphi(x)$.

Rules for equality

We include rules for usual **Leibniz equality**:

$$= \frac{}{\vdash_{\text{PA}} t = t} \quad \neq \frac{\vdash_{\text{PA}} \Gamma(s)}{\vdash_{\text{PA}} s \neq t, \Gamma(t)}$$

These are directly induced from the usual axioms $x = x$ and:

$$x = y \rightarrow \varphi(x) \rightarrow \varphi(y) \tag{1}$$

Exercise

Show that $\vdash_{\text{PA}} (1)$. What about the 'mirrored' version:

$$x = y \rightarrow \varphi(y) \rightarrow \varphi(x)$$

We include rules for all **substitutional instances** of (almost all) Q axioms:

$${}^0 \frac{}{\vdash_{\text{PA}} st \neq 0} \quad {}^s \frac{}{\vdash_{\text{PA}} st \neq su, t = u}$$

$${}^{+0} \frac{}{\vdash_{\text{PA}} t + 0 = t} \quad {}^{+s} \frac{}{\vdash_{\text{PA}} t + su = s(t + u)}$$

$${}^{\times 0} \frac{}{\vdash_{\text{PA}} t \times 0 = 0} \quad {}^{\times s} \frac{}{\vdash_{\text{PA}} t \times su = t \times u + t}$$

NB: Note that we have not included a rule for case analysis: $x = 0 \vee \exists y x = sy$.
Recall that this is derivable from the other axioms in the presence of induction...

Finally, and most importantly, we include the **induction rules**:

$$\text{ind} \frac{\vdash_{\text{PA}} \Gamma, \varphi(0) \quad \vdash_{\text{PA}} \Gamma, \bar{\varphi}(y), \varphi(sy)}{\vdash_{\text{PA}} \Gamma, \varphi(t)} \quad y \text{ fresh}$$

This completes the definition of \vdash_{PA} .

Example, and two-sided notation

We sometimes write, say, $\Gamma \vdash_{\text{PA}} \Delta$ for $\vdash_{\text{PA}} \bar{\Gamma}, \Delta$, where $\bar{\Gamma} := \{\bar{\varphi} : \varphi \in \Gamma\}$.

Example (Induction)

For each φ , we have $\vdash_{\text{PA}} \text{ind}(\varphi)$.

$$\frac{\frac{\text{id} \frac{}{\varphi(z) \vdash_{\text{PA}} \varphi(z)} \quad \text{id} \frac{}{\varphi(sz) \vdash_{\text{PA}} \varphi(sz)}}{\wedge \frac{}{\varphi(z) \rightarrow \varphi(sz), \varphi(z) \vdash_{\text{PA}} \varphi(sz)}}}{\exists \frac{}{\forall x(\varphi(x) \rightarrow \varphi(sx)), \varphi(z) \vdash_{\text{PA}} \varphi(sz)}}}{\text{ind} \frac{}{\varphi(0) \vdash_{\text{PA}} \varphi(0)}}}{2 \vee, \forall \frac{}{\vdash_{\text{PA}} \varphi(0) \rightarrow \forall x(\varphi(x) \rightarrow \varphi(sx)) \rightarrow \forall x \varphi(x)}}$$

NB: we omitted several instances of w , a convention we shall continue to employ.

(Blank slide)

Some properties

Proposition (Substitution)

$\vdash_{\text{PA}} \Gamma(x) \implies \vdash_{\text{PA}} \Gamma(t)$ for any term t .

Theorem (Adequacy)

$\text{PA} \vdash \varphi \iff \vdash_{\text{PA}} \varphi$.

Proof idea.

By induction on the judgements $\text{PA} \vdash$ and \vdash_{PA} . For \Leftarrow we must strengthen the invariant to *arbitrary sequents* under the **formula interpretation**. □

Exercise

Complete this proof formally.

Most importantly for this course:

Corollary

PA is consistent $\iff \not\vdash_{\text{PA}}$.

(Blank slide)

(Blank slide)

- 1 First-order arithmetic and Robinson's axioms
- 2 Induction and Peano's axioms
- 3 Sequent calculus formulation
- 4 Break: exercises and questions**
- 5 Digging deeper: formalisation and soundness

Exercises

- 1 We defined $t \leq u := \exists x t + x = u$. Give an alternative definition of the form $\forall x \varphi_0$ where φ_0 is quantifier-free.
(Harder) Show that PA proves the equivalence of these definitions. What is the logical complexity of induction that you used?
- 2 Show that $\vdash_{\text{PA}} \varphi, \overline{\varphi}$, for each formula φ .
- 3 Show that the *case analysis* axiom $x = 0 \vee \exists y x = sy$ of Q can be derived using induction and the **other** axioms of Q.
- 4 Show $\vdash_{\text{PA}} \exists x (\varphi(x) \rightarrow \forall y \varphi(y))$, for any $\varphi(x)$
- 5 Show that the following variants of Leibniz equality are already theorems of first-order logic with equality: $t = u \rightarrow \varphi(t) \rightarrow \varphi(s)$
- 6
 - Show that $\mathbb{N} \cup \{\infty\}$ with $s\infty = \infty$ extends to a model of Q.
 - Show that $\mathbb{N} \cup \{\infty_0, \infty_1\}$ with
 - $\infty_0 + n = \infty_0$ and $\infty_1 + n = \infty_1$, for all $n \in \mathbb{N}$; but,
 - $n + \infty_0 = \infty_1$ and $n + \infty_1 = \infty_0$, for all $n \in \mathbb{N}$.
 - Conclude that Q does **not prove commutativity** of $+$, i.e. $x + y = y + x$.
- 7
 - Show that $\varphi \in \Sigma_n$ if and only if $\overline{\varphi} \in \Pi_n$.
 - Show that Σ_n and Π_n are closed under \vee and \wedge , up to logical equivalence.
 - Conclude that each formula is logically equivalent to one in some Σ_n or Π_n .
- 8 Show that PA proves that \times is commutative.

- 1 First-order arithmetic and Robinson's axioms
- 2 Induction and Peano's axioms
- 3 Sequent calculus formulation
- 4 Break: exercises and questions
- 5 Digging deeper: formalisation and soundness**

Recalling Hilbert's program, let us point out that the reduction of PA to \vdash_{PA} can itself be proved in a **very weak system** N.

Definition (Primitive recursive arithmetic)

PRA is a (**quantifier-free**) first-order theory given by:

- PRA's language extends \mathcal{L}_A by a symbol for each primitive recursive function;
- PRA extends Q by the defining equations for each primitive recursive function.

(In fact, even PRA is overkill, but further optimisation is beyond scope.)

Proposition (Meta)

PRA *proves* (an appropriate formalisation of) all (metalogical) theorems thusfar *except...*

Recalling Hilbert's program, let us point out that the reduction of PA to \vdash_{PA} can itself be proved in a **very weak system** N.

Definition (Primitive recursive arithmetic)

PRA is a (**quantifier-free**) first-order theory given by:

- PRA's language extends \mathcal{L}_A by a symbol for each primitive recursive function;
- PRA extends Q by the defining equations for each primitive recursive function.

(In fact, even PRA is overkill, but further optimisation is beyond scope.)

Proposition (Meta)

PRA *proves* (an appropriate formalisation of) all (metalogical) theorems thusfar **except...**
...soundness.

(Blank slide)

Revisiting soundness

Of course, by *Tarski's Undefinability of Truth*, we cannot even state Soundness in \mathcal{L}_A . However, Soundness has a curious consequence:

Corollary (of Soundness)

PA is consistent.

Proof.

$0^{\text{st}} \neq 1^{\text{st}}$, so PA $\not\vdash 0 = 1$ by Soundness. □

Thus, by *Gödel's Second Incompleteness*, even frugal approximations of Soundness are not available, **already in PA**.

However, we can exploit this idea to obtain **partial consistency results**. For instance:

Theorem (Formalised Consistency)

PRA proves the consistency of Q.

Reformulating Q without quantifiers

First, we can reformulate Q in a **quantifier-free** manner by introducing a **predecessor** function p under the axioms:

- $p0 = 0$
- $psx = x$

The point of p is to compute **witnesses** to the *case analysis* axiom of Q:

$$x = 0 \vee \exists y x = sy$$

Replacing this axiom with,

$$x = 0 \vee x = spx$$

results in a theory *at least* as strong as Q (even provably in PRA), and which we shall simply refer to as Q henceforth (as abuse of terminology).

It is easy to define a primitive recursive **evaluator** $\text{Eval}(x, y)$ for terms of \mathcal{L}_A .
In particular, PRA can formalise its basic characteristic properties:

Proposition (Characteristic properties)

PRA *proves*:

- $\text{Eval}(\ulcorner 0 \urcorner, y) = 0$
- $\text{Eval}(\ulcorner x_i \urcorner, \langle y_0, \dots, y_{n-1} \rangle) = y_i$, when $n > i$.
- $\text{Eval}(\ulcorner st \urcorner, y) = s \text{Eval}(\ulcorner t \urcorner, y)$.
- $\text{Eval}(\ulcorner pt \urcorner, y) = p \text{Eval}(\ulcorner t \urcorner, y)$.
- $\text{Eval}(\ulcorner t + u \urcorner, y) = \text{Eval}(\ulcorner t \urcorner, y) + \text{Eval}(\ulcorner u \urcorner, y)$.
- $\text{Eval}(\ulcorner t \times u \urcorner, y) = \text{Eval}(\ulcorner t \urcorner, y) \times \text{Eval}(\ulcorner u \urcorner, y)$.

Consistency of Q, formalised

Lemma (Formalised Soundness)

$\text{PRA} \vdash \text{“Q} \vdash t = u\text{”} \implies \text{Eval}(\ulcorner t \urcorner, y) = \text{Eval}(\ulcorner u \urcorner, y)$.

In fact, to prove this we also need another metalogical result:

Proposition (Cut-elimination)

PRA proves the *cut-elimination* theorem for first-order logic.

Nonetheless from here, the consistency of Q in PRA follows immediately:

Proof of Formalised Consistency.

(INSIDE PRA). If $\text{Q} \vdash 0 = 1$ then $\text{Eval}(\ulcorner 0 \urcorner, y) = \text{Eval}(\ulcorner 1 \urcorner, y)$, and so $0 = 1$ by the characteristic properties. This contradicts $\neg 0 = sx$. \square

Remark

A similar proof can be employed to show that PA proves the consistency of PRA. For this, we need to show that PA can define an *evaluator for primitive recursive functions*, something we will see later in the course.

(Blank slide)