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/esslli23`.

Outline

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

Language of arithmetic

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

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

where:

- $\mathsf{0}$ 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 $\bot, \top, \vee, \wedge, \rightarrow, \leftrightarrow, \exists, \forall$ as usual.

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

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 $\mathbb{N}$.
- $0^{\mathfrak{N}} := 0 \in \mathbb{N}$.
- $s^{\mathfrak{N}} : \mathbb{N} \to \mathbb{N}$ by $n \mapsto n + 1$.
- $+^{\mathfrak{N}} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $(m, n) \mapsto m + n$.
- $\times^{\mathfrak{N}} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 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:

- $\neg \mathsf{s}x = 0$
- $\mathsf{s}x = \mathsf{s}y \rightarrow x = y$
- $x = 0 \vee \exists y\, x = \mathsf{s}y$

- $x + 0 = x$
- $x + \mathsf{s}y = \mathsf{s}(x + y)$
- $x \times 0 = 0$
- $x \times \mathsf{s}y = x \times y + x$

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.

Lower bounds for Q

Proposition (Soundness)

$\mathfrak{N} \models \mathsf{Q}$.

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

Exercise

- Show that $\mathbb{N} \cup \{\infty\}$ with $\mathsf{s}\infty = \infty$ 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)

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* $\mathsf{Q} \vdash \exists x \varphi(x)$*.*

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:

$$\varphi, \psi \quad ::= \quad s = t \quad | \quad s \neq t \quad | \quad \varphi \lor \psi \quad | \quad \varphi \land \psi \quad | \quad \exists x \varphi \quad | \quad \forall x \varphi$$

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

- $\overline{t = u} := t \neq u$
- $\overline{t \neq u} := t = u$
- $\overline{\varphi \lor \psi} := \overline{\varphi} \land \overline{\psi}$
- $\overline{\varphi \land \psi} := \overline{\varphi} \lor \overline{\psi}$.
- $\overline{\exists x \varphi} := \forall x \overline{\varphi}$
- $\overline{\forall x \varphi} := \exists x \overline{\varphi}$

Proposition

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

(Blank slide)

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

Definition (Bounded quantification)

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

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

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.
- $\Sigma_{n+1} := \{\exists \vec{x}\, \varphi : \varphi \in \Pi_n\}$
- $\Pi_{n+1} := \{\forall \vec{x}\, \varphi : \varphi \in \Sigma_n\}$.

Exercise

- 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.

(Blank slide)

Lemma (Q decides bounded formulas)

If $\varphi \in \Delta_0$ is closed, then either $\mathsf{Q} \vdash \varphi$ *or* $\mathsf{Q} \vdash \overline{\varphi}$*.*

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 $\mathsf{Q} \vdash \varphi$*.*

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 $\mathsf{Q} \vdash \psi(\vec{n})$.
- Thus, by pure logic, $\mathsf{Q} \vdash \exists \vec{x}\, \psi(\vec{x})$, as required. □

(Blank slide)

Outline

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:

$$\mathsf{ind}(\varphi) \quad : \quad \varphi(0) \to \forall x(\varphi(x) \to \varphi(\mathsf{s}x)) \to \forall x \varphi(x)$$

Definition (Peano Arithmetic)

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

We better state:

Proposition (Soundness)

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

(We will discuss this further later.)

Exercise

Show that the axiom $x = 0 \vee \exists y\, x = \mathsf{s}y$ 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:*

- $0 + y = y$
- $\mathsf{s}x + y = \mathsf{s}(x + y)$

Proof idea.

By induction on y. □

Proposition (Commutativity of $+$)

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

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

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)

(Blank slide)

Outline

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

Sequents

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

Definition (Sequents)

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

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

$$\lceil \Gamma \rceil := \forall \vec{x} \bigvee \Gamma$$

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

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

Sequents

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

Definition (Sequents)

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

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

$$\lceil \Gamma \rceil := \forall \vec{x} \bigvee \Gamma$$

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 $\vdash_{\mathsf{PA}} \Gamma$ 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:

$$\text{id}\ \frac{}{\vdash_{\mathsf{PA}} s = t, s \neq t} \qquad \text{w}\ \frac{\vdash_{\mathsf{PA}} \Gamma}{\vdash_{\mathsf{PA}} \Gamma, \Gamma'} \qquad \text{cut}\ \frac{\vdash_{\mathsf{PA}} \Gamma, \varphi \qquad \vdash_{\mathsf{PA}} \Gamma', \overline{\varphi}}{\vdash_{\mathsf{PA}} \Gamma, \Gamma'}$$

$$\vee\ \frac{\vdash_{\mathsf{PA}} \Gamma, \varphi_0 \vee \varphi_1, \varphi_i}{\vdash_{\mathsf{PA}} \Gamma, \varphi_0 \vee \varphi_1}\ i \in \{0, 1\} \qquad \wedge\ \frac{\vdash_{\mathsf{PA}} \Gamma, \varphi \qquad \vdash_{\mathsf{PA}} \Gamma, \psi}{\vdash_{\mathsf{PA}} \Gamma, \varphi \wedge \psi}$$

$$\exists\ \frac{\vdash_{\mathsf{PA}} \Gamma, \exists x \varphi(x), \varphi(t)}{\vdash_{\mathsf{PA}} \Gamma, \exists x \varphi(x)} \qquad \forall\ \frac{\vdash_{\mathsf{PA}} \Gamma, \varphi(y)}{\vdash_{\mathsf{PA}} \Gamma, \forall x \varphi(x)}\ y \text{ fresh}$$

Exercise (η-expansion)

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

Exercise (Drinker's Paradox)

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

Rules for equality

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

$$= \frac{}{\vdash_{\mathsf{PA}} t = t} \qquad \neq \frac{\vdash_{\mathsf{PA}} \Gamma(s)}{\vdash_{\mathsf{PA}} s \neq t, \Gamma(t)}$$

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

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

Exercise

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

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

Rules for Q

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

$$\mathsf{0}\,\frac{}{\vdash_{\mathsf{PA}} \mathsf{s}t \neq \mathsf{0}} \qquad \mathsf{s}\,\frac{}{\vdash_{\mathsf{PA}} \mathsf{s}t \neq \mathsf{s}u, t = u}$$

$$+\mathsf{0}\,\frac{}{\vdash_{\mathsf{PA}} t + \mathsf{0} = t} \qquad +\mathsf{s}\,\frac{}{\vdash_{\mathsf{PA}} t + \mathsf{s}u = \mathsf{s}(t + u)}$$

$$\times\mathsf{0}\,\frac{}{\vdash_{\mathsf{PA}} t \times \mathsf{0} = \mathsf{0}} \qquad \times\mathsf{s}\,\frac{}{\vdash_{\mathsf{PA}} t \times \mathsf{s}u = t \times u + t}$$

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

Rules for induction

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

$$\text{ind}\ \frac{\vdash_{\mathsf{PA}} \Gamma, \varphi(\mathsf{0}) \qquad \vdash_{\mathsf{PA}} \Gamma, \overline{\varphi}(y), \varphi(\mathsf{s}y)}{\vdash_{\mathsf{PA}} \Gamma, \varphi(t)}\ y \text{ fresh}$$

This completes the definition of $\vdash_{\mathsf{PA}}$.

Example, and two-sided notation

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

Example (Induction)

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

$$
\dfrac{
  \dfrac{}{\varphi(0) \vdash_{\mathsf{PA}} \varphi(0)}\,\mathsf{id}
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{}{\varphi(z) \vdash_{\mathsf{PA}} \varphi(z)}\,\mathsf{id}
      \qquad
      \dfrac{}{\varphi(\mathsf{s}z) \vdash_{\mathsf{PA}} \varphi(\mathsf{s}z)}\,\mathsf{id}
    }{\varphi(z) \to \varphi(\mathsf{s}z), \varphi(z) \vdash_{\mathsf{PA}} \varphi(\mathsf{s}z)}\,\wedge
  }{\forall x(\varphi(x) \to \varphi(\mathsf{s}x)), \varphi(z) \vdash_{\mathsf{PA}} \varphi(\mathsf{s}z)}\,\exists
}{
  \dfrac{\varphi(0), \forall x(\varphi(x) \to \varphi(\mathsf{s}x)) \vdash_{\mathsf{PA}} \varphi(y)}{\vdash_{\mathsf{PA}} \varphi(0) \to \forall x(\varphi(x) \to \varphi(\mathsf{s}x)) \to \forall x \varphi(x)}\,2\vee,\forall
}\,\mathsf{ind}
$$

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

(Blank slide)

Some properties

Proposition (Substitution)

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

Theorem (Adequacy)

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

Proof idea.

By induction on the judgements $\mathsf{PA} \vdash$ and $\vdash_{\mathsf{PA}}$. 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* $\iff \nvdash_{\mathsf{PA}}$.

(Blank slide)

(Blank slide)

Outline

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 $t \leqslant u := \exists x\, t + x = u$. 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 $\vdash_{\mathsf{PA}} \varphi, \overline{\varphi}$, for each formula φ.
3. Show that the *case analysis* axiom $x = 0 \vee \exists y\, x = \mathsf{s}y$ of Q can be derived using induction and the other axioms of Q.
4. Show $\vdash_{\mathsf{PA}} \exists x\, (\varphi(x) \to \forall y\, \varphi(y))$, for any $\varphi(x)$
5. Show that the following variants of Leibniz equality are already theorems of first-order logic with equality: $t = u \to \varphi(u) \to \varphi(t)$
6. - Show that $\mathbb{N} \cup \{\infty\}$ with $\mathsf{s}\infty = \infty$ 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. An alternative definition is $t \leqslant' u := \forall y\, u + \mathsf{s}y \neq t$.
2. By induction on the structure of φ. The most interesting case is when φ is quantified:

$$
\forall\ \dfrac{\exists\ \dfrac{\dfrac{IH}{\vdash_{\mathsf{PA}} \varphi(y), \overline{\varphi}(y)}}{\vdash_{\mathsf{PA}} \exists x\, \varphi(x), \overline{\varphi}(y)}}{\vdash_{\mathsf{PA}} \exists x\, \varphi(x), \forall x\, \overline{\varphi}(x)}
$$

3. **(Inside PA.)** By induction on x:
   - $x = 0$: we are done by left disjunct.
   - $x = \mathsf{s}x'$: set $y = x'$.

4.

$$
\exists\ \dfrac{\forall,\vee\ \dfrac{\exists\ \dfrac{\mathsf{w},\vee\ \dfrac{\mathsf{id}\ \dfrac{}{\vdash_{\mathsf{PA}} \overline{\varphi}(z), \varphi(z)}}{\vdash_{\mathsf{PA}} \varphi(z) \to \forall y\, \varphi(y), \varphi(z)}}{\vdash_{\mathsf{PA}} \exists x\, (\varphi(x) \to \forall y\, \varphi(y)), \overline{\varphi}(0), \varphi(z)}}{\vdash_{\mathsf{PA}} \exists x\, (\varphi(x) \to \forall y\, \varphi(y)), \varphi(0) \to \forall y\, \varphi(y)}}{\vdash_{\mathsf{PA}} \exists x\, (\varphi(x) \to \forall y\, \varphi(y))}
$$

5. By contraposition and usual Leibniz equality: $\varphi(u) \to \varphi(t)$ is logically equivalent to $\overline{\varphi}(t) \to \overline{\varphi}(u)$.
6.
   - We complete the definition of the structure by setting:
     - $\infty + a = a + \infty = \infty$, for all $a \in \mathbb{N} \cup \{\infty\}$
     - $\infty \times 0 = 0 \times \infty = 0$.
     - $\infty \times a = a \times \infty = a$ for $a \neq 0$.

     From here, verfiying that this is a Q-structure is routine.
   - We may complete the definition of the structure by setting:
     - $\mathsf{s}\infty_i = \infty_i$, for $i \in \{0, 1\}$;
     - $\infty_i + \infty_j = \infty_{1-j}$.
     - $\infty_i \times 0 = 0$
     - $\infty_i \times \alpha = \infty_{1-i}$ for $\alpha \neq 0$.
     - (It does not matter what values we set $\alpha \times \infty_j$, as long as they are consistent with above).

By construction, we have that $\mathsf{0}$ is no successor, s is injective, and that any non-$\mathsf{0}$ element is in the image of successor. It remains to check the recursive definitions of $+, \times$:

$$\begin{aligned} \infty_i + \mathsf{0} &= \infty_i \\ \infty_i + \mathsf{s}n &= \infty_i \\ &= \mathsf{s}\infty_i \\ &= \mathsf{s}(\infty_i + n) \\ \infty_i + \mathsf{s}\infty_j &= \infty_i + \infty_j \\ &= \infty_{1-j} \\ &= \mathsf{s}\infty_{1-j} \\ &= \mathsf{s}(\infty_i + \infty_{1-j}) \end{aligned}$$

$$\begin{aligned} \infty_i \times \mathsf{0} &= \mathsf{0} \\ \infty_i \times \mathsf{s}n &= \infty_{1-i} \\ &= \infty_i \times n + \infty_i \\ \infty_i \times \mathsf{s}\infty_j &= \infty_i \times \infty_j \\ &= \infty_{1-i} \\ &= (\infty_i \times \infty_j) + \infty_i \end{aligned}$$

7

- Follows directly from De Morgan duality.
- For Σ_n:
  - $\exists x\, \varphi(x) \lor \exists y\, \psi(y)$ is logically equivalent to $\exists x', y'\ (\varphi(x') \lor \psi(y'))$, where x, y have been renamed to distinct fresh ones x', y' to avoid conflicts with other occurrences.
  - $\exists x\, \varphi(x) \land \exists y\, \psi(y)$ is logically equivalent to $\exists x', y'\ (\varphi(x') \land \psi(y'))$ where x, y have been renamed to distinct fresh ones x', y' to avoid conflicts with other occurrences.

  The cases for Π_n are dual.
- By induction on the structure of a formula, applying one of the two previous bullet points at each step for, say, minimal n.

8. We proceed in the same way as for addition. First we show $0 \times y = 0$ by induction on y:
   - $0 \times 0 = 0$;
   - $0 \times sy = (0 \times y) + 0 = 0 + 0$ by IH, and so $= 0$ by Q.

   Then we show $sx \times y = x \times y + y$ by induction on y:
   - $sx \times 0 = 0$;
   - $sx \times sy = sx \times y + sx = (x \times y + y) + sx$ by IH, which $= (x \times y + x) + sy$ by associativity and commutativity of $+$ (proved earlier) and Q, and so again by Q, $= x \times sy + sy$.

   Now we show commutativity of $\times$, i.e. $x \times y = y \times x$, by induction on y:
   - $x \times 0 = 0 = 0 \times x$ by the first property above.
   - $x \times sy = x \times y + x = y \times x + x$ by IH, and so $= sy \times x$ by the second property above.

Outline

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 $\vdash_{\mathsf{PA}}$ 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*...

On formalisation

Recalling Hilbert's program, let us point out that the reduction of PA to $\vdash_{\mathsf{PA}}$ 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)

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.

$0^{\mathfrak{N}} \neq 1^{\mathfrak{N}}$, so PA $\nvdash 0 = 1$ 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 $\mathsf{p}x$ under the axioms:

- $\mathsf{p}0 = 0$
- $\mathsf{ps}x = x$

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

$$x = 0 \vee \exists y\, x = \mathsf{s}y$$

Replacing this axiom with,

$$x = 0 \vee x = \mathsf{sp}x$$

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** $\texttt{Eval}(x, y)$ for terms of $\mathcal{L}_A \cup \{\mathsf{p}\}$.

In particular, PRA can formalise its basic characteristic properties:

Proposition (Characteristic properties)

PRA *proves:*

- $\texttt{Eval}(\ulcorner 0 \urcorner, y) = 0$
- $\texttt{Eval}\left(\ulcorner x_i \urcorner, \langle y_0, \ldots y_{n-1} \rangle\right) = y_i \ \vee \ n \leqslant i.$
- $\texttt{Eval}(\ulcorner \mathsf{s}t \urcorner, y) = \mathsf{s}\,\texttt{Eval}(\ulcorner t \urcorner, y).$
- $\texttt{Eval}(\ulcorner \mathsf{p}t \urcorner, y) = \mathsf{p}\,\texttt{Eval}(\ulcorner t \urcorner, y).$
- $\texttt{Eval}(\ulcorner t + u \urcorner, y) = \texttt{Eval}(\ulcorner t \urcorner, y) + \texttt{Eval}(\ulcorner u \urcorner, y).$
- $\texttt{Eval}(\ulcorner t \times u \urcorner, y) = \texttt{Eval}(\ulcorner t \urcorner, y) \times \texttt{Eval}(\ulcorner u \urcorner, y).$

Lemma (Formalised Soundness)

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

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

Proposition (Formalised 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 $\mathsf{Q} \vdash 0 = 1$ then $\mathtt{Eval}(\ulcorner 0 \urcorner, y) = \mathtt{Eval}(\ulcorner 1 \urcorner, y)$, and so $0 = 1$ by the characteristic properties. This contradicts $\neg 0 = \mathsf{s}x$. □

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 might see later in the course.

(Blank slide)