Proof theory of arithmetic

Lecture 3 – A consistency proof

Anupam Das

University of Birmingham

34th European Summer School
in Logic, Language and Information

Ljubljana, Slovenia
9 August 2023

These slides are available at http://www.anupamdas.com/esslli23.

Recap: the state of play

We want to reduce the consistency of PA to the consistency of a simple computational theory, in a finitistic manner.

We have formulated PA in sequent style, $\vdash_{\mathsf{PA}}$, and shown their equivalence finitistically, i.e. in PRA.

Almost every rule of $\vdash_{\mathsf{PA}}$ has the **subformula property** (up to substitutions): the only barrier to proving consistency is the cut rule:

$$\mathsf{cut}\ \frac{\vdash_{\mathsf{PA}} \Gamma, \varphi \qquad \vdash_{\mathsf{PA}} \Gamma, \overline{\varphi}}{\vdash_{\mathsf{PA}} \Gamma, \Gamma'}$$

NB: this viewpoint arguably hides the real culprit: induction.

(Blank slide)

Outline

1. A new system: up to ω!
2. Simulating PA
3. Cut-elimination for $\vdash_\omega$
4. Break: exercises and questions
5. Formalisation and ordinal analysis

System $\vdash_\omega$ (aka PA_ω)

We define a judgement $\vdash_\omega$ just like $\vdash_{\mathsf{PA}}$ except:

- Instead of id, $=$, $\neq$, Q rules, we simply admit all closed true (in)equations:

$$= \frac{}{\vdash_\omega n = n} \qquad \neq \frac{}{\vdash_\omega m \neq n}\; m \neq n$$

- Instead of $\forall$, ind rules, we have an ω-branching rule:

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

$$\omega \frac{\vdash_\omega \Gamma, \varphi(0) \quad \vdash_\omega \Gamma, \varphi(1) \quad \vdash_\omega \Gamma, \varphi(2) \quad \cdots}{\vdash_\omega \Gamma, \forall x \varphi(x)}$$

Conventions

- $\vdash_\omega$ is a judgement on only closed sequents.
- We *identify* closed terms t with their values $t^{\mathfrak{N}}$ (which are also numerals).

  NB: this is subtle, and important for formalisation; we will revisit it later.

(Blank slide)

Definition

The judgement $\vdash_\omega \Gamma$, for Γ closed, is defined by:

$$= \frac{}{\vdash_\omega n = n} \qquad \neq \frac{}{\vdash_\omega m \neq n}\, m \neq n$$

$$\mathsf{w}\, \frac{\vdash_\omega \Gamma}{\vdash_\omega \Gamma, \Gamma'} \qquad \mathsf{cut}\, \frac{\vdash_\omega \Gamma, \varphi \quad \vdash_\omega \Gamma', \overline{\varphi}}{\vdash_\omega \Gamma, \Gamma'}$$

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

$$\exists\, \frac{\vdash_\omega \Gamma, \exists x \varphi(x), \varphi(n)}{\vdash_\omega \Gamma, \exists x \varphi(x)} \qquad \omega\, \frac{\vdash_\omega \Gamma, \varphi(0) \quad \vdash_\omega \Gamma, \varphi(1) \quad \vdash_\omega \Gamma, \varphi(2) \quad \cdots}{\vdash_\omega \Gamma, \forall x \varphi(x)}$$

(Blank slide)

Similarly to $\vdash_{\mathsf{PA}}$, we can derive general identity:

Proposition (General identity)

$\vdash_\omega \varphi, \overline{\varphi}$

Proof.
By induction on the structure of φ.
The critical difference to the argument for $\vdash_{\mathsf{PA}}$ is for a quantified formula:

$$\omega\,\dfrac{\exists\,\dfrac{\dfrac{IH}{\vdash_\omega \overline{\varphi}(0), \varphi(0)}}{\vdash_\omega \overline{\varphi}(0), \exists x\varphi(x)} \qquad \exists\,\dfrac{\dfrac{IH}{\vdash_\omega \overline{\varphi}(1), \varphi(1)}}{\vdash_\omega \overline{\varphi}(1), \exists x\varphi(x)} \qquad \cdots}{\vdash_\omega \forall x\overline{\varphi}(x), \exists x\varphi(x)} \qquad \square$$

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

(Blank slide)

Example: consistency

Write $\mathrm{Prf}(x, y)$ for a formula stating "x codes a PA-proof of the formula coded by y".

It is not hard to see that:

Proposition ($\vdash_\omega$ *partial* consistency of PA)

For each $n \in \mathbb{N}$, we have $\vdash_\omega \neg \mathrm{Prf}(n, \ulcorner \bot \urcorner)$.

I.e. no *actual* proof concludes $\bot$ (of course, assuming PA is consistent).

However from here we immediately have from the ω rule:

Corollary ($\vdash_\omega$ consistency of PA)

$\vdash_\omega \forall x \neg \mathrm{Prf}(x, \ulcorner \bot \urcorner)$.

NB: there was nothing special about PA! We could have started from PA2, ZFC,...

$\vdash_\omega$ is not effectively presented, and so Gödel incompleteness does not apply.

Indeed we have achieved extreme power:

Proposition (Completeness)

If $\mathfrak{N} \models \varphi$ *then* $\vdash_\omega \varphi$.

NB: this argument does not even need cuts!

Proof idea.

By induction on the structure of φ. □

Just to be clear, we have a sanity check:

Proposition (Soundness)

If $\vdash_\omega \Gamma$ *then* $\mathfrak{N} \models [\Gamma]$.

Proof idea.

By induction on $\vdash_\omega$. □

NB: Obviously, this slide, and the previous one, work under a strong metatheory.

(Blank slide)

Outline

Another reduction

The main result of this section is:

Theorem

If $\vdash_{\mathsf{PA}} \varphi$, *for* φ *closed, then* $\vdash_{\omega} \varphi$.

More concretely, we shall prove the following Lemma:

Lemma (Simulation)

If $\vdash_{\mathsf{PA}} \Gamma(\vec{x})$, *with all free variables displayed, then* $\vdash_{\omega} \Gamma(\vec{n})$ *for all* $\vec{n} \in \mathbb{N}$.

Proof.

By induction on $\vdash_{\mathsf{PA}}$. The cases are given over the next few slides.

NB: we will typically suppress the substitution of numerals $\vec{n}$ for free variables $\vec{x}$.

(Blank slide) Equality

$$\overline{\vdash_{PA} t(\vec{x}) = t(\vec{x})}$$

$$\rightsquigarrow$$

$$\overline{\vdash_\omega t(\vec{n})^{\mathfrak{N}} = t(\vec{n})^{\mathfrak{N}}}$$

$$\frac{\vdash_{PA} \Gamma(t(\vec{x}))}{\vdash_{PA} t(\vec{x}) \neq u(\vec{x}), \Gamma(u(\vec{x}))}$$

$t(\vec{n})^{\mathfrak{N}} \neq u(\vec{n})^{\mathfrak{N}}$ then

$$\omega\ \frac{\overline{\vdash_\omega t(\vec{n})^{\mathfrak{N}} \neq u(\vec{n})^{\mathfrak{N}}}}{\vdash_\omega t(\vec{n})^{\mathfrak{N}} \neq u(\vec{n})^{\mathfrak{N}}, \Gamma(u(\vec{n}))}$$

$k = t(\vec{n})^{\mathfrak{N}} = u(\vec{n})^{\mathfrak{N}}$

$$\omega\ \frac{\vdash_\omega \Gamma(k)}{\vdash_\omega k \neq k, \Gamma(k)}$$

(Blank slide)

Simulation of quantifier rules

$$\exists\ \frac{\vdash_{\mathsf{PA}} \Gamma, \exists x \varphi(x), \varphi(t)}{\vdash_{\mathsf{PA}} \Gamma, \exists x \varphi(x)} \quad \rightsquigarrow \quad \exists\ \frac{\overset{IH}{\vdash_{\omega} \Gamma, \exists x \varphi(x), \varphi(t^{\mathfrak{N}})}}{\vdash_{\omega} \Gamma, \exists x \varphi(x)}$$

$$\forall\ \frac{\vdash_{\mathsf{PA}} \Gamma, \varphi(y)}{\vdash_{\mathsf{PA}} \Gamma, \forall x\, \varphi(x)} \quad \rightsquigarrow \quad \omega\ \frac{\overset{IH}{\vdash_{\omega} \Gamma, \varphi(0)} \quad \overset{IH}{\vdash_{\omega} \Gamma, \varphi(1)} \quad \overset{IH}{\vdash_{\omega} \Gamma, \varphi(2)} \quad \cdots}{\vdash_{\omega} \Gamma, \forall x\, \varphi(x)}$$

NB: notice here the utility of identifying closed terms with their values. This will facilitate the corresponding 'cut-reduction'.

Simulation of induction

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

We show that $\vdash_\omega \Gamma, \varphi(n)$ by (sub)induction on n:

- $\vdash_\omega \Gamma, \varphi(0)$ by *IH*.
- For the inductive step we have:

$$\mathsf{cut}\ \frac{\overset{\nabla\, ih}{\vdash_\omega \Gamma, \varphi(n)} \qquad \overset{\nabla\, IH}{\vdash_\omega \Gamma, \overline{\varphi}(n), \varphi(n+1)}}{\vdash_\omega \Gamma, \varphi(n+1)}$$

From here we indeed obtain $\vdash_\omega \Gamma, \varphi(t^{\mathfrak{N}})$, as required.

Simulation of induction, visually

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

$$\rightsquigarrow \quad \text{cut}\ \dfrac{\text{cut}\ \dfrac{\text{cut}\ \dfrac{\begin{array}{c}\text{cut}\ \dfrac{\text{cut}\ \dfrac{\overset{IH}{\Gamma, \varphi(0)} \qquad \overset{IH}{\Gamma, \overline{\varphi}(0), \varphi(1)}}{\vdash_\omega \Gamma, \varphi(1)}}{\ddots}\end{array}}{\vdash_\omega \Gamma, \varphi(t^{\mathfrak{N}} - 2)} \qquad \overset{IH}{\Gamma, \overline{\varphi}(t^{\mathfrak{N}} - 2), \varphi(t^{\mathfrak{N}} - 1)}}{\vdash_\omega \Gamma, \varphi(t^{\mathfrak{N}} - 1)} \qquad \overset{IH}{\Gamma, \overline{\varphi}(t^{\mathfrak{N}} - 1), \varphi(t^{\mathfrak{N}})}}{\vdash_\omega \Gamma, \varphi(t^{\mathfrak{N}})}$$

Outline

1. A new system: up to ω!
2. Simulating PA
3. Cut-elimination for $\vdash_\omega$
4. Break: exercises and questions
5. Formalisation and ordinal analysis

Our main result is:

Theorem (Cut-Elimination)
If $\vdash_\omega \Gamma$ *then we can derive* $\vdash_\omega \Gamma$ *without using the* cut *rule.*

By the subformula property of the non-cut rules, it is immediate that:

Corollary (Consistency of $\vdash_\omega$)
$\nvdash_\omega$

Since we have reduced $\vdash_{\mathsf{PA}}$ to $\vdash_\omega$, and also PA $\vdash$ to $\vdash_{\mathsf{PA}}$, we thus have:

Corollary (Consistency of PA)
PA *is consistent.*

NB: assuming *Cut-Elimination*, the corollaries are obtained finitistically, i.e. in PRA.

First, let us see some cut-reduction cases…

Cut-reduction cases: commutative

$$\mathsf{cut}\,\frac{\mathsf{r}\,\dfrac{\{\vdash_\omega \Gamma_i, \varphi\}_{i<\iota}}{\vdash_\omega \Gamma, \varphi} \qquad \vdash_\omega \Gamma', \overline{\varphi}}{\vdash_\omega \Gamma, \Gamma'} \quad \rightsquigarrow \quad \mathsf{r}\,\frac{\left\{\mathsf{cut}\,\dfrac{\vdash_\omega \Gamma_i, \varphi \qquad \vdash_\omega \Gamma', \overline{\varphi}}{\vdash_\omega \Gamma_i, \Gamma'}\right\}_{i<\iota}}{\vdash_\omega \Gamma, \Gamma'}$$

for an ι-ary inference step r, with $\iota \in \{0, 1, 2, \omega\}$.

$$\frac{\omega\,\dfrac{}{\forall x\,\psi(x), \Gamma, \varphi} \qquad \Gamma', \overline{\varphi}}{\forall x\,\psi(x), \Gamma, \Gamma'}$$

Cut-reduction case: quantifiers

$$
\textsf{cut}\;\dfrac{\exists\;\dfrac{\vdash_\omega \Gamma', \exists x\varphi(x), \varphi(k)}{\vdash_\omega \Gamma', \exists x\varphi(x)} \qquad \omega\;\dfrac{\{\vdash_\omega \Gamma, \overline{\varphi}(n)\}_{n<\omega}}{\vdash_\omega \Gamma, \forall x\overline{\varphi}(x)}}{\vdash_\omega \Gamma, \Gamma'}
$$

$$
\rightsquigarrow \qquad \textsf{cut}\;\dfrac{\textsf{cut}\;\dfrac{\vdash_\omega \Gamma', \exists x\varphi(x), \varphi(k) \qquad \omega\;\dfrac{\{\vdash_\omega \Gamma, \overline{\varphi}(n)\}_{n<\omega}}{\vdash_\omega \Gamma, \forall x\overline{\varphi}(x)}}{\vdash_\omega \Gamma, \Gamma', \varphi(k)} \qquad \vdash_\omega \Gamma, \overline{\varphi}(k)}{\vdash_\omega \Gamma, \Gamma'}
$$

(Blank slide)

Cut-elimination: the big idea, visually

To organise our overarching induction argument, let us set up some machinery.

Definition (Degrees)

- The **degree** of a formula φ, written $\deg(\varphi)$, is its number of logical symbols.
- The degree of a cut step is the degree of its cut formula.
- A d-cut is a cut of degree d.

Write $\vdash_{\overline{d}}$ for the restriction of $\vdash_{\omega}$ to only $< d$-cuts.

NB: Implicit here is that $\deg(\varphi) = \deg(\overline{\varphi})$.

NB: $\vdash_{\overline{0}}$ is just cut-free provability. Thus we have (in PRA):

Proposition (Cut-free consistency)

$\nvdash_{\overline{0}}$

d-cut-admissibility

Lemma (d-cut-admissibility)

$\vdash_{\overline{d}}$ *is closed under d*-cut.

I.e., when $\deg(\varphi) = d$, *if* $\vdash_{\overline{d}} \Gamma, \varphi$ *and* $\vdash_{\overline{d}} \Gamma', \overline{\varphi}$, *then* $\vdash_{\overline{d}} \Gamma, \Gamma'$.

Proof.

By induction on $\vdash_{\overline{d}} \Gamma, \varphi$ and $\vdash_{\overline{d}} \Gamma', \overline{\varphi}$. □

Lemma (Degree reduction)

$\vdash_{\overline{d}+1} \subseteq \vdash_{\overline{d}}$.
I.e. if $\vdash_{\overline{d}+1} \Gamma$ *then* $\vdash_{\overline{d}} \Gamma$.

Proof.

By induction on $\vdash_{\overline{d}+1}$. For the inductive step:

- By *IH* assume any premisses are already derivable by $\vdash_{\overline{d}}$.
- Now apply d-cut-admissibility. □

We can now complete the proof of cut-elimination:

Theorem (Cut-elimination for $\vdash_{\omega}$, restated)

If $\vdash_{\omega} \Gamma$ *then* $\vdash_{0} \Gamma$.

Proof.

We show $\vdash_{\overline{d}} \subseteq \vdash_{0}$ by induction on $d < \omega$. □

As mentioned before, this implies consistency of PA.

Outline

1. A new system: up to ω!
2. Simulating PA
3. Cut-elimination for $\vdash_\omega$
4. Break: exercises and questions
5. Formalisation and ordinal analysis

Exercises

1. Show, by induction on $\vdash_{\mathsf{PA}}$, that witness term t in the premiss of the $\exists$ rule can be restricted to contain only the variables occurring free in the lower sequent, without loss of provability.
2. Give a PA_ω proof of the *Drinkers Paradox*, i.e. show $\vdash_\omega \exists x\, (\varphi(x) \to \forall y\, \varphi(y))$.
3.
   - For the completeness argument for $\vdash_\omega$, write down the case for an existential formula and a disjunction.
   - What can you conclude about the size of sequents required to carry out the completeness argument?
   - **(Subtle.)** Why might we not want to impose such a restriction for the *Simulation Theorem*, embedding $\vdash_{\mathsf{PA}}$ into $\vdash_\omega$?
4. **(Hard.)** What do you think is the *closure ordinal* of, say, $\vdash_0$ (if you know what that is)?
5. For the simulation of $\vdash_{\mathsf{PA}}$ by $\vdash_\omega$, write down the cases of the missing rules id, $=$, $\neq$ and the ones for Q.
6.
   - What are the cut-reduction cases for $=$-$\neq$?
   - Write down the $\vee$-$\wedge$ cut-reduction case.

Outline

1. A new system: up to ω!
2. Simulating PA
3. Cut-elimination for $\vdash_\omega$
4. Break: exercises and questions
5. Formalisation and ordinal analysis

Taming the metatheory via ordinals

The metatheory required to show completeness of $\vdash_\omega$ for $\mathfrak{N}$ was ridiculously strong.

However, we can tame the metatheory required for the *Simulation Theorem* and the *Cut-Elimination Theorem*, by refining our inductions according to explicit order types.

Definition

ε_0 is the least ordinal α such that $\omega^\alpha = \alpha$.

Some observations

- $\varepsilon_0 = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \dots\} = \inf\{\alpha : \omega^\alpha \leqslant \alpha\}$ is a limit ordinal.
- Thus ε_0 is countable, and even recursive.
- We can naturally represent and compare ordinals $< \varepsilon_0$ in arithmetic. (More on this tomorrow).

(Blank slide)

Height of judgements

The **height** of a well-founded tree T is defined by induction on T as follows:

- If T has immediate subtrees $\{T_i\}_{i \in I}$, then $\mathrm{ht}(T) := \sup_{i \in I}(\mathrm{ht}(T_i) + 1)$.

So let us write $\vdash^{\alpha}_{\vec{d}} \Gamma$ if there is a derivation of $\vdash_{\vec{d}} \Gamma$ of height $\leqslant \alpha$.

(Blank slide)

Definition

The judgements $\vdash^{\alpha}_{d} \Gamma$, for $d < \omega$ and α an ordinal, are defined by:

$$= \frac{}{\vdash^{0}_{0} n = n} \qquad \neq \frac{}{\vdash^{0}_{0} m \neq n}\, m \neq n$$

$$\mathsf{w}\ \frac{\vdash^{\beta}_{d} \Gamma}{\vdash^{\alpha}_{d} \Gamma, \Gamma'}\, \beta < \alpha \qquad {<}d\text{-}\mathsf{cut}\ \frac{\vdash^{\beta}_{d} \Gamma, \varphi \quad \vdash^{\gamma}_{d} \Gamma', \overline{\varphi}}{\vdash^{\alpha}_{d} \Gamma, \Gamma'}\, \beta, \gamma < \alpha$$

$$\vee\ \frac{\vdash^{\beta}_{d} \Gamma, \varphi_0 \vee \varphi_1, \varphi_i}{\vdash^{\alpha}_{d} \Gamma, \varphi_0 \vee \varphi_1}\, \beta < \alpha \qquad \wedge\ \frac{\vdash^{\beta}_{d} \Gamma, \varphi \quad \vdash^{\gamma}_{d} \Gamma, \psi}{\vdash^{\alpha}_{d} \Gamma, \varphi \wedge \psi}\, \beta, \gamma < \alpha$$

$$\exists\ \frac{\vdash^{\beta}_{d} \Gamma, \exists x \varphi(x), \varphi(n)}{\vdash^{\alpha}_{d} \Gamma, \exists x \varphi(x)}\, \beta < \alpha \qquad \omega\ \frac{\vdash^{\beta_0}_{d} \Gamma, \varphi(0) \quad \vdash^{\beta_1}_{d} \Gamma, \varphi(1) \quad \vdash^{\beta_2}_{d} \Gamma, \varphi(2) \quad \cdots}{\vdash^{\alpha}_{d} \Gamma, \forall x \varphi(x)}\, \beta_i < \alpha$$

Theorem (Simulation, refined)

If $\vdash_{\mathsf{PA}} \varphi$, *for* φ *closed, then* $\vdash_d^\alpha \varphi$ *for some* $d < \omega$ *and* $\alpha < \omega 2$.

NB: for formalisation in PRA, we are implicitly using an **evaluator** for $\mathcal{L}_A$-terms.

Lemma (d-cut-admissibility, refined)

Let $\deg(\varphi) = d$. *If* $\vdash_d^\alpha \Gamma, \varphi$ *and* $\vdash_d^\beta \Gamma', \overline{\varphi}$, *then* $\vdash_d^{\alpha \sharp \beta} \Gamma, \Gamma'$.

NB: here $\sharp$ is the **symmetric sum** (or **natural sum**) of ordinals.

Lemma (Degree reduction)

If $\vdash_{d+1}^\alpha \Gamma$ *then* $\vdash_d^{\omega^\alpha} \Gamma$.

Putting this all together, we have:

Theorem (Cut-elimination for PA, refined)

If $\mathsf{PA} \vdash \varphi$, *then* $\vdash_0^\alpha \varphi$, *for some* $\alpha < \varepsilon_0$.

Corollary (Consistency, refined)

PA *is consistent, as long as "all* $\alpha < \varepsilon_0$ *are well-founded"...*

Some remarks on formalisation

The only parts of the refinements of the previous slide *not* available in PRA are the various inductions on ordinals $< \varepsilon_0$.

We can fix some appropriate recursive representation of ordinals $\alpha, \beta, \dots < \varepsilon_0$ and their comparison in $\mathcal{L}_A$ (more on this tomorrow).

Now define ε_0-ind for the schema of axioms for each $\varphi(x)$:

$$\forall \alpha < \varepsilon_0 (\forall \beta < \alpha \, \varphi(\beta) \to \varphi(\alpha)) \to \forall \alpha < \varepsilon_0 \, \varphi(\alpha)$$

We can now formalise our entire consistency argument:

Theorem (Formalised consistency)

PRA $+ \varepsilon_0$-ind *proves the consistency of* PA.

NB. We have finitistically reduced the entire consistency of PA to a 'simple' computational principle: induction up to ε_0.

NB. It is immediate that PA cannot prove well-foundedness of (any appropriate representation of) ε_0.