Proof Theory of Induction

Stefan Hetzl

Institute of Discrete Mathematics and Geometry
Vienna University of Technology

Summer School for Proof Theory in First-Order Logic
Funchal, Madeira

August 2017

Outline

- Gentzen's consistency proof
- The omega rule
- Cyclic proofs

Outline

- **Gentzen's consistency proof**
  - **Background**
  - Peano arithmetic
  - Reduction of cut and induction
  - Ordinals
  - The consistency proof
- The omega rule
- Cyclic proofs

Background

- Hilbert's programme (1920ies)
    - Formalisation of mathematics
    - Proof of consistency by finitary methods

Background

- Hilbert's programme (1920ies)
  - Formalisation of mathematics
  - Proof of consistency by finitary methods
- Gödel's (2nd) incompleteness theorem (1931)
  Theorem. For a (consistent, axiomatisable, and sufficiently strong) first-order theory T, $T \nvdash \mathrm{Con}_T$.

Background

- Hilbert's programme (1920ies)
  - Formalisation of mathematics
  - Proof of consistency by finitary methods

- Gödel's (2nd) incompleteness theorem (1931)
  Theorem. For a (consistent, axiomatisable, and sufficiently strong) first-order theory T, $T \nvdash \mathrm{Con}_T$.

- Gentzen's approach (1936-): split consistency proof for T into:
  1. A cut-elimination procedure (in weak theory)
  2. A termination assumption (transcends theory)

Cut-elimination and consistency

- Why is cut-elimination relevant for consistency?
- **Definition.** A theory T is inconsistent if there is some formula φ s.t. $T \vdash \varphi$ and $T \vdash \neg\varphi$.
- Suppose there are T-proofs π_1 of φ and π_2 of $\neg\varphi$, then

$$\pi \qquad = \qquad \dfrac{\overset{(\pi_2)}{\Rightarrow \neg\varphi} \qquad \dfrac{\overset{(\pi_1)}{\Rightarrow \varphi}}{\neg\varphi \Rightarrow}\,\neg l}{\Rightarrow}\,\mathsf{cut}$$

is a proof of $\Rightarrow$. By cut-elimination, there is a cut-free proof π^* of $\Rightarrow$. Contradiction.

Outline

- **Gentzen's consistency proof**
  - ✓ Background
  - **Peano arithmetic**
  - Reduction of cut and induction
  - Ordinals
  - The consistency proof
- The omega rule
- Cyclic proofs

Peano arithmetic

- The language $L = \{0, s, +, \cdot, =\}$
- Basic arithmetic BA consists of the axioms:

$$\begin{aligned}
&\forall x \forall y\, (s(x) = s(y) \to x = y)\\
&\quad \forall x\, 0 \neq s(x)\\
&\quad \forall x\, x + 0 = x\\
&\forall x \forall y\, x + s(y) = s(x + y)\\
&\quad \forall x\, x \cdot 0 = 0\\
&\forall x \forall y\, x \cdot s(y) = x \cdot y + x
\end{aligned}$$

- Peano arithmetic PA consists of the axioms of BA together with, for every formula $\varphi(x, \bar{z})$, the induction axiom

$$\forall \bar{z}\, \big((\varphi(0, \bar{z}) \wedge \forall y(\varphi(y, z) \to \varphi(s(y), z)) \to \forall x\, \varphi(x, z)\big).$$

A sequent calculus for PA

- A sequent calculus for FOL with equality in L plus inital sequents

$$\begin{aligned} s(t) = s(u) &\Rightarrow t = u \\ &\Rightarrow 0 \neq s(t) \\ &\Rightarrow t + 0 = t \\ &\Rightarrow t + s(u) = s(t+u) \\ &\Rightarrow t \cdot 0 = 0 \\ &\Rightarrow t \cdot s(u) = t \cdot u + t \end{aligned}$$

and the induction rule

$$\frac{\varphi(\alpha), \Gamma \Rightarrow \Delta, \varphi(s(\alpha))}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(t)}$$

where α does not appear in $\varphi(0), \Gamma \Rightarrow \Delta, \varphi(t)$.

Simple proofs

- **Definition.** A PA-proof is called *simple* if it consists of only of initial sequents, atomic cuts, and structural inference.

Simple proofs

- **Definition.** A PA-proof is called *simple* if it consists of only of initial sequents, atomic cuts, and structural inference.

- **Simple proof lemma.** There is no simple proof of $\Rightarrow$.
  Proof. Let π be a simple proof of $\Rightarrow$.
  - W.l.o.g. π is variable-free.
  - Every formula in π is of the form $s = t$ with s, t variable-free.
  - Evaluate formulas and sequents to $\top$ or $\bot$ "in $\mathbb{N}$".
  - Every inital sequent evaluates to $\top$.
  - Every rule preserves $\top$.
  - $\Rightarrow$ evaluates to $\bot$.

Outline

- **Gentzen's consistency proof**
  - ✓ Background
  - ✓ Peano arithmetic
  - **Reduction of cut and induction**
  - Ordinals
  - The consistency proof
- The omega rule
- Cyclic proofs

Interaction between induction and cut: example

$$\dfrac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \varphi(0)\end{matrix} \qquad \dfrac{\begin{matrix}\vdots\\ \Gamma, \varphi(\alpha) \Rightarrow \varphi(s(\alpha))\end{matrix}}{\Gamma, \varphi(0) \Rightarrow \varphi(t)}\ \text{ind}}{\Gamma \Rightarrow \varphi(t)}\ \text{cut}$$

Interaction between induction and cut: example

$$\dfrac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \varphi(0)\end{matrix} \qquad \dfrac{\begin{matrix}\vdots\\ \Gamma, \varphi(\alpha) \Rightarrow \varphi(s(\alpha))\end{matrix}}{\Gamma, \varphi(0) \Rightarrow \varphi(t)}\,\text{ind}}{\Gamma \Rightarrow \varphi(t)}\,\text{cut}$$

$\Longrightarrow$ eliminating cuts means eliminating inductions too

Numerals and evaluation

- **Definition.** For $n \in \mathbb{N}$ define the L-term $\overline{n} = s^n(0)$.
- A term of the form $s^n(0)$ is called *numeral*.
- **Evaluation lemma.** Let t is a variable free L-term. Then
  - there is an $n \in \mathbb{N}$ s.t. BA $\vdash t = \overline{n}$, and
  - for any formula $\varphi(x)$ there is an induction-free proof of $\varphi(\overline{n}) \Rightarrow \varphi(t)$

Cut-elimination and induction

$$\dfrac{\begin{array}{c}(\pi(\alpha))\\ \varphi(\alpha), \Gamma \Rightarrow \Delta, \varphi(s(\alpha))\end{array}}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(t)}\ \mathsf{ind}$$

Cut-elimination and induction

$$\dfrac{\begin{matrix}(\pi(\alpha))\\ \varphi(\alpha),\Gamma\Rightarrow\Delta,\varphi(s(\alpha))\end{matrix}}{\varphi(0),\Gamma\Rightarrow\Delta,\varphi(t)}\ \mathsf{ind}$$

If t is variable-free, there is $n\in\mathbb{N}$ s.t. $\mathsf{BA}\vdash t=\overline{n}$

Cut-elimination and induction

$$\dfrac{\begin{array}{c}(\pi(\alpha))\\ \varphi(\alpha), \Gamma \Rightarrow \Delta, \varphi(s(\alpha))\end{array}}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(t)}\ \text{ind}$$

If t is variable-free, there is $n \in \mathbb{N}$ s.t. $\mathrm{BA} \vdash t = \overline{n}$

$$\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}(\pi(0))\\ \varphi(0), \Gamma \Rightarrow \Delta, \varphi(\overline{1})\end{array} \quad \begin{array}{c}(\pi(\overline{1}))\\ \varphi(\overline{1}), \Gamma \Rightarrow \Delta, \varphi(\overline{2})\end{array}}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(\overline{2})}\ \text{cut}\\ \vdots\\ \varphi(0), \Gamma \Rightarrow \Delta, \varphi(\overline{n})\end{array} \qquad \begin{array}{c}\text{Eval. Lem.}\\ \varphi(\overline{n}) \Rightarrow \varphi(t)\end{array}}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(t)}\ \text{cut}$$

Cut-elimination and induction

$$\dfrac{\overset{(\pi(\alpha))}{\varphi(\alpha), \Gamma \Rightarrow \Delta, \varphi(s(\alpha))}}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(t)}\ \text{ind}$$

If t is variable-free, there is $n \in \mathbb{N}$ s.t. $\mathsf{BA} \vdash t = \overline{n}$

$$\dfrac{\begin{array}{c}\dfrac{\overset{(\pi(0))}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(\overline{1})} \quad \overset{(\pi(\overline{1}))}{\varphi(\overline{1}), \Gamma \Rightarrow \Delta, \varphi(\overline{2})}}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(\overline{2})}\ \text{cut} \\ \vdots \\ \varphi(0), \Gamma \Rightarrow \Delta, \varphi(\overline{n})\end{array} \qquad \overset{\text{Eval. Lem.}}{\varphi(\overline{n}) \Rightarrow \varphi(t)}}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(t)}\ \text{cut}$$

Under which conditions does this work?

The end-piece

- **Definition.** A logical inference ι in a PA-proof π is called
  - *explicit* if it is ancestor of the end-sequent, and
  - *implicit* if it is ancestor of a cut formula.

The end-piece

- **Definition.** A logical inference ι in a PA-proof π is called
  - *explicit* if it is ancestor of the end-sequent, and
  - *implicit* if it is ancestor of a cut formula.
- **Definition.** The *end-piece* of a PA-proof π:
  all sequents which are not above an implicit logical inference.

The end-piece

- **Definition.** A logical inference ι in a PA-proof π is called
  - *explicit* if it is ancestor of the end-sequent, and
  - *implicit* if it is ancestor of a cut formula.
- **Definition.** The *end-piece* of a PA-proof π:
  all sequents which are not above an implicit logical inference.
- *Example.*

$$\dfrac{\dfrac{\dfrac{\begin{matrix}\vdots\\ \Rightarrow \psi(0,0)\end{matrix}}{\Rightarrow \exists y\,\psi(0,y)}\,\exists_{\mathsf{r}} \qquad \dfrac{\dfrac{\begin{matrix}\vdots\\ \psi(\alpha,\beta) \Rightarrow \exists y\,\psi(s(\alpha),y)\end{matrix}}{\exists y\,\psi(\alpha,y) \Rightarrow \exists y\,\psi(s(\alpha),y)}\,\exists_{\mathsf{l}}}{\exists y\,\psi(0,y) \Rightarrow \exists y\,\psi(t,y)}\,\mathsf{ind}}{\Rightarrow \exists y\,\psi(t,y)}\,\mathsf{cut} \qquad \dfrac{\begin{matrix}\vdots\\ \psi(t,\alpha) \Rightarrow \exists y\,\varphi(t,y)\end{matrix}}{\exists y\,\psi(t,y) \Rightarrow \exists y\,\varphi(t,y)}\,\exists_{\mathsf{l}}}{\dfrac{\Rightarrow \exists y\,\varphi(t,y)}{\Rightarrow \exists x \exists y\,\varphi(x,y)}\,\exists_{\mathsf{r}}}\,\mathsf{cut}$$

The end-piece

- **Definition.** A logical inference ι in a PA-proof π is called
  - *explicit* if it is ancestor of the end-sequent, and
  - *implicit* if it is ancestor of a cut formula.
- **Definition.** The *end-piece* of a PA-proof π:
  all sequents which are not above an implicit logical inference.
- *Example.*

$$
\dfrac{
  \dfrac{
    \dfrac{\begin{array}{c}\vdots\\ \Rightarrow \psi(0,0)\end{array}}{\color{blue}\Rightarrow \exists y\,\psi(0,y)}\,\exists_{\mathrm{r}}
    \qquad
    \dfrac{
      \dfrac{\begin{array}{c}\vdots\\ \psi(\alpha,\beta) \Rightarrow \exists y\,\psi(s(\alpha),y)\end{array}}{\color{blue}\exists y\,\psi(\alpha,y) \Rightarrow \exists y\,\psi(s(\alpha),y)}\,\exists_{\mathrm{l}}
    }{\color{blue}\exists y\,\psi(0,y) \Rightarrow \exists y\,\psi(t,y)}\,\mathrm{ind}
  }{\color{blue}\Rightarrow \exists y\,\psi(t,y)}\,\mathrm{cut}
  \qquad
  \dfrac{\begin{array}{c}\vdots\\ \psi(t,\alpha) \Rightarrow \exists y\,\varphi(t,y)\end{array}}{\color{blue}\exists y\,\psi(t,y) \Rightarrow \exists y\,\varphi(t,y)}\,\exists_{\mathrm{l}}
}{
  \dfrac{\color{blue}\Rightarrow \exists y\,\varphi(t,y)}{\color{blue}\Rightarrow \exists x \exists y\,\varphi(x,y)}\,\exists_{\mathrm{r}}
}\,\mathrm{cut}
$$

Σ_1-sequents

- **Definition.** A Σ_1-sequent is a sequent of the form

$$\forall \overline{x_1}\, \varphi_1, \ldots, \forall \overline{x_k} \varphi_k \Rightarrow \exists \overline{x_{k+1}}\, \varphi_{k+1}, \ldots, \exists \overline{x_n}\, \varphi_n$$

s.t. $\varphi_1, \ldots, \varphi_n$ quantifier-free, φ_i contains only variables from $\overline{x_i}$.

Σ_1-sequents

- **Definition.** A Σ_1-sequent is a sequent of the form

$$\forall\overline{x_1}\,\varphi_1,\ldots,\forall\overline{x_k}\varphi_k \Rightarrow \exists\overline{x_{k+1}}\,\varphi_{k+1},\ldots,\exists\overline{x_n}\,\varphi_n$$

  s.t. $\varphi_1,\ldots,\varphi_n$ quantifier-free, φ_i contains only variables from $\overline{x_i}$.

- **Lemma.** Let π be a PA-proof of a Σ_1-sequent $\Gamma \Rightarrow \Delta$ and let

$$\frac{\varphi(\alpha),\Gamma \Rightarrow \Delta,\varphi(s(\alpha))}{\varphi(0),\Gamma \Rightarrow \Delta,\varphi(t)}\ \text{ind}$$

  be a lowermost induction in the end-piece of π. Then t is variable-free.

Σ_1-sequents

- **Definition.** A Σ_1-sequent is a sequent of the form

$$\forall\overline{x_1}\,\varphi_1, \ldots, \forall\overline{x_k}\varphi_k \Rightarrow \exists\overline{x_{k+1}}\,\varphi_{k+1}, \ldots, \exists\overline{x_n}\,\varphi_n$$

  s.t. $\varphi_1, \ldots, \varphi_n$ quantifier-free, φ_i contains only variables from $\overline{x_i}$.

- **Lemma.** Let π be a PA-proof of a Σ_1-sequent $\Gamma \Rightarrow \Delta$ and let

$$\frac{\varphi(\alpha), \Gamma \Rightarrow \Delta, \varphi(s(\alpha))}{\varphi(0), \Gamma \Rightarrow \Delta, \varphi(t)}\ \text{ind}$$

  be a lowermost induction in the end-piece of π. Then t is variable-free.

  Proof. W.l.o.g. all variables in π are eigenvariables.

  End-piece does not contain $\forall_r$, $\exists_l$.

  $\Rightarrow$ End-piece contains only eigenvariables of inductions.

  $\Rightarrow$ The term of a lowermost induction is variable-free. □

Termination

- Let π be a proof of a Σ_1-sequent $\Gamma \Rightarrow \Delta$.
  - If end-piece of π contains ind:
    $\Longrightarrow$ reduce lowermost ind
  - If end-piece of π contains non-atomic cut:
    $\Longrightarrow$ reduce suitable non-atomic cut
  - Otherwise: π contains only atomic cuts
    (Then $\Gamma = \Delta = \emptyset$ implies that π is simple)

Termination

- Let π be a proof of a Σ_1-sequent $\Gamma \Rightarrow \Delta$.
  - If end-piece of π contains ind:
    $\Longrightarrow$ reduce lowermost ind
  - If end-piece of π contains non-atomic cut:
    $\Longrightarrow$ reduce suitable non-atomic cut
  - Otherwise: π contains only atomic cuts
    (Then $\Gamma = \Delta = \emptyset$ implies that π is simple)
- Have:

$$\pi_1 \quad \mapsto \quad \pi_2 \quad \mapsto \quad \pi_3 \quad \mapsto \quad \cdots$$

Do we ever enter the "Otherwise"-case?

Termination

- Let π be a proof of a Σ_1-sequent $\Gamma \Rightarrow \Delta$.
  - If end-piece of π contains ind:
    $\Longrightarrow$ reduce lowermost ind
  - If end-piece of π contains non-atomic cut:
    $\Longrightarrow$ reduce suitable non-atomic cut
  - Otherwise: π contains only atomic cuts
    (Then $\Gamma = \Delta = \emptyset$ implies that π is simple)
- Have:

$$\pi_1 \quad \mapsto \quad \pi_2 \quad \mapsto \quad \pi_3 \quad \mapsto \quad \cdots$$

  Do we ever enter the "Otherwise"-case?

- Want: well-founded $(X, <)$ and mapping o s.t.

$$\mathsf{o}(\pi_1) \;>\; \mathsf{o}(\pi_2) \;>\; \mathsf{o}(\pi_3) \;>\; \cdots$$

Outline

- **Gentzen's consistency proof**
  - ✓ Background
  - ✓ Peano arithmetic
  - ✓ Reduction of cut and induction
  - **Ordinals**
  - The consistency proof
- The omega rule
- Cyclic proofs

Ordinals, informally

- The order of the natural numbers

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots$$

Ordinals, informally

- Add limit element ω, i.e., $\forall n \in \mathbb{N} : n < \omega$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega$$

Ordinals, informally

- Add another successor element after that

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1}$$

Ordinals, informally

- and so on

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots$$

Ordinals, informally

- Add a new limit element again

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

- Repeat the above

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega\cdot 2} \quad \cdots \quad \bullet_{\omega\cdot 3} \quad \cdots\cdots$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

- And add a new limit element again

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega\cdot 2} \quad \cdots \quad \bullet_{\omega\cdot 3} \quad \cdots\cdots \quad \bullet_{\omega\cdot\omega=\omega^2}$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

- The ordinals $\leq \omega^2$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega\cdot 2} \quad \cdots \quad \bullet_{\omega\cdot 3} \quad \cdots\cdots \quad \bullet_{\omega\cdot\omega=\omega^2}$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

- The ordinals $\leq \omega^2$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega\cdot 2} \quad \cdots \quad \bullet_{\omega\cdot 3} \quad \cdots\cdots \quad \bullet_{\omega\cdot\omega=\omega^2}$$

- Repeat the repetition

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega^2} \quad \cdots \quad \bullet_{\omega^3} \quad \cdots\cdots$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

- The ordinals $\leq \omega^2$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega\cdot 2} \quad \cdots \quad \bullet_{\omega\cdot 3} \quad \cdots\cdots \quad \bullet_{\omega\cdot\omega=\omega^2}$$

- And add a new limit element again

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega^2} \quad \cdots \quad \bullet_{\omega^3} \quad \cdots\cdots \quad \bullet_{\omega^\omega}$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

- The ordinals $\leq \omega^2$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega\cdot 2} \quad \cdots \quad \bullet_{\omega\cdot 3} \quad \cdots\cdots \quad \bullet_{\omega\cdot\omega=\omega^2}$$

- The ordinals $\leq \omega^\omega$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega^2} \quad \cdots \quad \bullet_{\omega^3} \quad \cdots\cdots \quad \bullet_{\omega^\omega}$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

- The ordinals $\leq \omega^2$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega\cdot 2} \quad \cdots \quad \bullet_{\omega\cdot 3} \quad \cdots\cdots \quad \bullet_{\omega\cdot\omega=\omega^2}$$

- The ordinals $\leq \omega^\omega$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega^2} \quad \cdots \quad \bullet_{\omega^3} \quad \cdots\cdots \quad \bullet_{\omega^\omega}$$

- Iterate one more time

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega^\omega} \quad \cdots \quad \bullet_{\omega^{\omega^\omega}} \quad \cdots\cdots$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

- The ordinals $\leq \omega^2$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega\cdot 2} \quad \cdots \quad \bullet_{\omega\cdot 3} \quad \cdots\cdots \quad \bullet_{\omega\cdot\omega=\omega^2}$$

- The ordinals $\leq \omega^\omega$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega^2} \quad \cdots \quad \bullet_{\omega^3} \quad \cdots\cdots \quad \bullet_{\omega^\omega}$$

- And add a new limit element

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega^\omega} \quad \cdots \quad \bullet_{\omega^{\omega^\omega}} \quad \cdots\cdots \quad \bullet_{\varepsilon_0}$$

Ordinals, informally

- The ordinals $\leq \omega \cdot 2$

$$\bullet_0 \quad \bullet_1 \quad \bullet_2 \quad \cdots \quad \bullet_\omega \quad \bullet_{\omega+1} \quad \bullet_{\omega+2} \quad \cdots \quad \bullet_{\omega\cdot 2}$$

- The ordinals $\leq \omega^2$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega\cdot 2} \quad \cdots \quad \bullet_{\omega\cdot 3} \quad \cdots\cdots \quad \bullet_{\omega\cdot\omega=\omega^2}$$

- The ordinals $\leq \omega^\omega$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega^2} \quad \cdots \quad \bullet_{\omega^3} \quad \cdots\cdots \quad \bullet_{\omega^\omega}$$

- The ordinals $\leq \varepsilon_0$

$$\bullet_0 \quad \cdots \quad \bullet_\omega \quad \cdots \quad \bullet_{\omega^\omega} \quad \cdots \quad \bullet_{\omega^{\omega^\omega}} \quad \cdots\cdots \quad \bullet_{\varepsilon_0}$$

The ordinals $< \varepsilon_0$

- Ordinal arithmetic
  - addition $+$, multiplication $\cdot$, exponentiation
  - less-than $<$

The ordinals $< \varepsilon_0$

- Ordinal arithmetic
  - addition $+$, multiplication $\cdot$, exponentiation
  - less-than $<$
- Cantor normal form: if $0 < \alpha < \varepsilon_0$, then α can be written as

$$\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$$

where $\alpha_1 \geq \cdots \geq \alpha_n$, $0 < \alpha_i < \varepsilon_0$, α_i in normal form.
This normal form is unique.

The ordinals $< \varepsilon_0$

- Ordinal arithmetic
  - addition $+$, multiplication $\cdot$, exponentiation
  - less-than $<$
- Cantor normal form: if $0 < \alpha < \varepsilon_0$, then α can be written as

  $$\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$$

  where $\alpha_1 \geq \cdots \geq \alpha_n$, $0 < \alpha_i < \varepsilon_0$, α_i in normal form.
  This normal form is unique.
- The natural sum: for $\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$, $\beta = \omega^{\beta_1} + \cdots + \omega^{\beta_m}$ let

  $$\alpha \# \beta = \omega^{\lambda_1} \cdots \omega^{\lambda_{m+n}}$$

  $\lambda_1 \geq \cdots \geq \lambda_{m+n}$, $\{\lambda_1, \ldots, \lambda_{m+n}\} = \{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m\}$.

The ordinals $< \varepsilon_0$

- Ordinal arithmetic
  - addition $+$, multiplication $\cdot$, exponentiation
  - less-than $<$
- Cantor normal form: if $0 < \alpha < \varepsilon_0$, then α can be written as

  $$\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$$

  where $\alpha_1 \geq \cdots \geq \alpha_n$, $0 < \alpha_i < \varepsilon_0$, α_i in normal form.
  This normal form is unique.
- The natural sum: for $\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$, $\beta = \omega^{\beta_1} + \cdots + \omega^{\beta_m}$ let

  $$\alpha \# \beta = \omega^{\lambda_1} \cdots \omega^{\lambda_{m+n}}$$

  $\lambda_1 \geq \cdots \geq \lambda_{m+n}$, $\{\lambda_1, \ldots, \lambda_{m+n}\} = \{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m\}$.
- Formalisation
  - Term signature $O = \{0/0, \omega/1, +/2\}$
  - Modulo equality
  - Operations $+, \cdot, \exp, \#$ and relation $<$

Outline

- **Gentzen's consistency proof**
  - ✓ Background
  - ✓ Peano arithmetic
  - ✓ Reduction of cut and induction
  - ✓ Ordinals
  - **The consistency proof**
- The omega rule
- Cyclic proofs

The height of a sequent

- **Definition.** *Logical complexity* of a formula, cut, induction.

The height of a sequent

- **Definition.** *Logical complexity* of a formula, cut, induction.
- **Definition.** *Height* of a sequent S in a proof π, $\mathrm{h}(S, \pi)$, is maximum of log. complexities of cut or induction below S in π.

The height of a sequent

- **Definition.** *Logical complexity* of a formula, cut, induction.
- **Definition.** *Height* of a sequent S in a proof π, $\mathsf{h}(S, \pi)$, is maximum of log. complexities of cut or induction below S in π.
- **Observation.** If S_1 and S_2 are premises of a binary inference, then $\mathsf{h}(S_1, \pi) = \mathsf{h}(S_2, \pi)$.

The height of a sequent

- **Definition.** *Logical complexity* of a formula, cut, induction.
- **Definition.** *Height* of a sequent S in a proof π, $\mathsf{h}(S, \pi)$, is maximum of log. complexities of cut or induction below S in π.
- **Observation.** If S_1 and S_2 are premises of a binary inference, then $\mathsf{h}(S_1, \pi) = \mathsf{h}(S_2, \pi)$.
- **Notation.** $\mathsf{h}(S)$ for $\mathsf{h}(S, \pi)$ if π is clear

The ordinal assignment

- **Definition.** Let S be a sequent in a proof π. Define $\mathsf{o}(S)$:
  - Initial sequent S: $\mathsf{o}(S) = 1$
  - Structural inference $\dfrac{S'}{S}$: $\mathsf{o}(S) = \mathsf{o}(S')$
  - Unary logical inference $\dfrac{S'}{S}$: $\mathsf{o}(S) = \mathsf{o}(S') + 1$
  - Binary logical inference $\dfrac{S_1 \quad S_2}{S}$: $\mathsf{o}(S) = \mathsf{o}(S_1) \# \mathsf{o}(S_2)$
  - $\dfrac{S_1 \quad S_2}{S}$ cut : $\mathsf{o}(S) = \omega_{\mathsf{h}(S_i)-\mathsf{h}(S)}(\mathsf{o}(S_1) \# \mathsf{o}(S_2))$
  - $\dfrac{S'}{S}$ ind : $\mathsf{o}(S) = \omega_{\mathsf{h}(S')-\mathsf{h}(S)+1}(\alpha_1 + 1)$

    where $\mathsf{o}(S') = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$ with $\alpha_1 \geq \cdots \geq \alpha_n$.

The ordinal assignment

- **Definition.** Let S be a sequent in a proof π. Define $\mathsf{o}(S)$:
  - Initial sequent S: $\mathsf{o}(S) = 1$
  - Structural inference $\dfrac{S'}{S}$: $\mathsf{o}(S) = \mathsf{o}(S')$
  - Unary logical inference $\dfrac{S'}{S}$: $\mathsf{o}(S) = \mathsf{o}(S') + 1$
  - Binary logical inference $\dfrac{S_1 \quad S_2}{S}$: $\mathsf{o}(S) = \mathsf{o}(S_1) \# \mathsf{o}(S_2)$
  - $\dfrac{S_1 \quad S_2}{S}$ cut : $\mathsf{o}(S) = \omega_{\mathsf{h}(S_i)-\mathsf{h}(S)}(\mathsf{o}(S_1) \# \mathsf{o}(S_2))$
  - $\dfrac{S'}{S}$ ind : $\mathsf{o}(S) = \omega_{\mathsf{h}(S')-\mathsf{h}(S)+1}(\alpha_1 + 1)$

    where $\mathsf{o}(S') = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$ with $\alpha_1 \geq \cdots \geq \alpha_n$.
- **Definition.** Let π be a proof of S, then $\mathsf{o}(\pi) = \mathsf{o}(S, \pi)$.

The consistency proof

- **Reduction Lemma.** Let $\Gamma \Rightarrow \Delta$ be a Σ_1-sequent, let π be a proof of $\Gamma \Rightarrow \Delta$ that contains a non-atomic cut or an induction. Then there is a proof π' of $\Gamma \Rightarrow \Delta$ with $\mathsf{o}(\pi') < \mathsf{o}(\pi)$.

The consistency proof

- **Reduction Lemma.** Let $\Gamma \Rightarrow \Delta$ be a Σ_1-sequent, let π be a proof of $\Gamma \Rightarrow \Delta$ that contains a non-atomic cut or an induction. Then there is a proof π' of $\Gamma \Rightarrow \Delta$ with $\mathrm{o}(\pi') < \mathrm{o}(\pi)$.

- **Theorem.** PA is consistent.
  Proof. Suppose PA is inconsistent, then there is a proof π of $\Rightarrow$.
  - $\Rightarrow$ is a Σ_1-sequent
  - $\mathrm{o}(\pi) < \varepsilon_0$
  - Induction on $\mathrm{o}(\pi)$ (reduction lemma): obtain π^* of $\Rightarrow$ s.t. π^* does not contain induction nor non-atomic cut
  - π^* is a simple proof of $\Rightarrow$
  - Contradiction.

The consistency proof

- **Reduction Lemma.** Let $\Gamma \Rightarrow \Delta$ be a Σ_1-sequent, let π be a proof of $\Gamma \Rightarrow \Delta$ that contains a non-atomic cut or an induction. Then there is a proof π' of $\Gamma \Rightarrow \Delta$ with $\mathrm{o}(\pi') < \mathrm{o}(\pi)$.

- **Theorem.** PA is consistent.
  Proof. Suppose PA is inconsistent, then there is a proof π of $\Rightarrow$.
  - $\Rightarrow$ is a Σ_1-sequent
  - $\mathrm{o}(\pi) < \varepsilon_0$
  - Induction on $\mathrm{o}(\pi)$ (reduction lemma): obtain π^* of $\Rightarrow$ s.t. π^* does not contain induction nor non-atomic cut
  - π^* is a simple proof of $\Rightarrow$
  - Contradiction.

- **Remark.** Formalisation in PRA:
  - $\mathrm{PRA} + \mathrm{TI}(\varphi(x), <_{\varepsilon_0}) \vdash \mathrm{Con}_{\mathrm{PA}}$ for quantifier-free $\varphi(x)$
  - In particular: PRA proves Reduction Lemma, Simple Proof Lemma

More general end-sequents (1/2)

- Let $\mathrm{Exp}(x, y)$ be a representation of $n \mapsto 2^n$, in particular:

$$\mathrm{PA} \vdash \mathrm{Exp}(0, \overline{1}) \qquad \mathrm{PA} \vdash \mathrm{Exp}(x, y) \rightarrow \mathrm{Exp}(s(x), y \cdot \overline{2})$$

- Then $\mathrm{PA} \vdash \forall x \exists y\, \mathrm{Exp}(x, y)$:

$$\dfrac{\dfrac{\dfrac{\begin{matrix}\vdots\\ \Rightarrow \mathrm{Exp}(0,\overline{1})\end{matrix}}{\Rightarrow \exists y\,\mathrm{Exp}(0,y)}\,\exists_{\mathrm{r}} \qquad \dfrac{\dfrac{\dfrac{\begin{matrix}\vdots\\ \mathrm{Exp}(\beta,\gamma)\Rightarrow \mathrm{Exp}(s(\beta),\gamma\cdot 2)\end{matrix}}{\mathrm{Exp}(\beta,\gamma)\Rightarrow\exists y\,\mathrm{Exp}(s(\beta),y)}\,\exists_{\mathrm{r}}}{\exists y\,\mathrm{Exp}(\beta,y)\Rightarrow\exists y\,\mathrm{Exp}(s(\beta),y)}\,\exists_{\mathrm{l}}}{\exists y\,\mathrm{Exp}(0,y)\Rightarrow\exists y\,\mathrm{Exp}(\alpha,y)}\,\mathrm{ind}}{\Rightarrow\exists y\,\mathrm{Exp}(\alpha,y)}\,\mathrm{cut}}{\Rightarrow\forall x\exists y\,\mathrm{Exp}(x,y)}\,\forall_{\mathrm{r}}$$

More general end-sequents (1/2)

- Let $\mathrm{Exp}(x,y)$ be a representation of $n \mapsto 2^n$, in particular:

$$\mathrm{PA} \vdash \mathrm{Exp}(0,\overline{1}) \qquad \mathrm{PA} \vdash \mathrm{Exp}(x,y) \rightarrow \mathrm{Exp}(s(x), y\cdot\overline{2})$$

- Then $\mathrm{PA} \vdash \forall x \exists y\, \mathrm{Exp}(x,y)$:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Rightarrow \mathrm{Exp}(0,\overline{1})\end{array}}{\Rightarrow \exists y\, \mathrm{Exp}(0,y)}\,\exists_{\mathrm{r}} \qquad \dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\\ \mathrm{Exp}(\beta,\gamma) \Rightarrow \mathrm{Exp}(s(\beta),\gamma\cdot 2)\end{array}}{\mathrm{Exp}(\beta,\gamma) \Rightarrow \exists y\, \mathrm{Exp}(s(\beta),y)}\,\exists_{\mathrm{r}}}{\exists y\, \mathrm{Exp}(\beta,y) \Rightarrow \exists y\, \mathrm{Exp}(s(\beta),y)}\,\exists_{\mathrm{l}}}{\exists y\, \mathrm{Exp}(0,y) \Rightarrow \exists y\, \mathrm{Exp}(\alpha,y)}\,\mathrm{ind}}{\Rightarrow \exists y\, \mathrm{Exp}(\alpha,y)}\,\mathrm{cut}}{\Rightarrow \forall x \exists y\, \mathrm{Exp}(x,y)}\,\forall_{\mathrm{r}}$$

- But cut-elimination procedure does not work
  (Eigenvariable α in end-piece not introduced by induction)

More general end-sequents (2/2)

- **Proposition.** Every PA-proof of $\forall x \exists y\, \mathrm{Exp}(x,y)$ contains an induction inference.

  Proof. Let π be a PA-proof of $\forall x \exists y\, \mathrm{Exp}(x,y)$. Then w.l.o.g. π ends with $\forall_{\mathrm{r}}$. Suppose there is induction-free proof of $\exists y\, \mathrm{Exp}(\alpha, y)$, then by cut-elimination / Herbrand's theorem, there are $t_1, \ldots, t_n \in L \cup \{\alpha\}$ s.t.

$$\mathrm{BA} \vdash \mathrm{Exp}(\alpha, t_1) \vee \cdots \vee \mathrm{Exp}(\alpha, t_n), \text{ i.e.,}$$
$$\mathrm{BA} \vdash \forall\alpha\big(\mathrm{Exp}(\alpha, t_1) \vee \cdots \vee \mathrm{Exp}(\alpha, t_n)\big).$$

Contradiction. □

Summary of 1st part

Gentzen's consistency proof of PA

- Sequent calculus with induction rule
- Cut- and induction-elimination
- Except termination formalisable in PRA
- Ordinals (up to ε_0 in Cantor normal form)
- Proof of Σ_1-sequent: lowermost induction has variable-free term.
- Impossible for Π_2-sequents

Outline

- ✓ Gentzen's consistency proof
- **The omega rule**
  - **Infinitary propositional logic**
  - Infinitary proofs
  - The consistency proof
- Cyclic proofs

Infinitary propositional logic

- Observation: $\mathbb{N} \models \forall x\, \varphi(x)$ iff $\mathbb{N} \models \bigwedge_{n \in \mathbb{N}} \varphi(\overline{n})$
  $\mathbb{N} \models \exists x\, \varphi(x)$ iff $\mathbb{N} \models \bigvee_{n \in \mathbb{N}} \varphi(\overline{n})$

Infinitary propositional logic

- Observation: $\mathbb{N} \models \forall x\, \varphi(x)$ iff $\mathbb{N} \models \bigwedge_{n \in \mathbb{N}} \varphi(\overline{n})$
  $\mathbb{N} \models \exists x\, \varphi(x)$ iff $\mathbb{N} \models \bigvee_{n \in \mathbb{N}} \varphi(\overline{n})$
- The ω-rule

$$\frac{\Gamma, \varphi(0) \quad \Gamma, \varphi(\overline{1}) \quad \Gamma, \varphi(\overline{2}) \quad \cdots}{\Gamma, \bigwedge_{n \in \mathbb{N}} \varphi(n)}$$

Infinitary propositional logic

- Observation: $\mathbb{N} \models \forall x\, \varphi(x)$ iff $\mathbb{N} \models \bigwedge_{n\in\mathbb{N}} \varphi(\overline{n})$
  $\mathbb{N} \models \exists x\, \varphi(x)$ iff $\mathbb{N} \models \bigvee_{n\in\mathbb{N}} \varphi(\overline{n})$
- The ω-rule

$$\frac{\Gamma, \varphi(0) \quad \Gamma, \varphi(\overline{1}) \quad \Gamma, \varphi(\overline{2}) \quad \cdots}{\Gamma, \bigwedge_{n\in\mathbb{N}} \varphi(n)}$$

- **Definition.** The formulas of infinitary propositional logic:
  - Variable-free atoms (in $L = \{0, s, +, \cdot, =\}$)
  - Negated variable-free atoms (in L)
  - If, for $i \in I$, φ_i is a formula, then $\bigwedge_{i\in I} \varphi_i$ is a formula
  - If, for $i \in I$, φ_i is a formula, then $\bigvee_{i\in I} \varphi_i$ is a formula

  Here: I countable

Translation of first-order L-sentences

- **Definition.** *Translation of first-order L-sentences*:

$$A^\infty = A \text{ for an atom } A$$

$$[\forall x\, \varphi(x)]^\infty = \bigwedge_{n\in\mathbb{N}} \varphi^\infty(\overline{n}) \qquad [\exists x\, \varphi(x)]^\infty = \bigvee_{n\in\mathbb{N}} \varphi^\infty(\overline{n})$$

$$[\varphi \wedge \psi]^\infty = \varphi^\infty \wedge \psi^\infty \qquad [\varphi \vee \psi]^\infty = \varphi^\infty \vee \psi^\infty$$

$$[\varphi \to \psi]^\infty = \overline{\varphi^\infty} \vee \psi^\infty \qquad [\neg\varphi]^\infty = \overline{\varphi^\infty}$$

Translation of first-order L-sentences

- **Definition.** *Translation of first-order L-sentences*:

$$\begin{aligned} A^\infty &= A \text{ for an atom } A \\ [\forall x\, \varphi(x)]^\infty &= \bigwedge_{n\in\mathbb{N}} \varphi^\infty(\overline{n}) & \qquad [\exists x\, \varphi(x)]^\infty &= \bigvee_{n\in\mathbb{N}} \varphi^\infty(\overline{n}) \\ [\varphi \wedge \psi]^\infty &= \varphi^\infty \wedge \psi^\infty & [\varphi \vee \psi]^\infty &= \varphi^\infty \vee \psi^\infty \\ [\varphi \to \psi]^\infty &= \overline{\varphi^\infty} \vee \psi^\infty & [\neg\varphi]^\infty &= \overline{\varphi^\infty} \end{aligned}$$

- Where dualisation $\overline{\cdot}$ is defined as:

$$\begin{aligned} \overline{A} &= \neg A & \qquad \overline{\neg A} &= A & \qquad &\text{for an atom } A \\ \overline{\bigwedge_{i\in I} \varphi_i} &= \bigvee_{i\in I} \overline{\varphi_i} & \overline{\bigvee_{i\in I} \varphi_i} &= \bigwedge_{i\in I} \overline{\varphi_i} & &\text{for a formula } \varphi \end{aligned}$$

Example: induction axiom

The translation of the induction axiom

$$[\mathsf{I}_x\varphi]^\infty = \left[\varphi(0) \wedge \forall y\,(\varphi(y) \to \varphi(s(y))) \to \forall x\,\varphi(x)\right]^\infty$$

Example: induction axiom

The translation of the induction axiom

$$\begin{aligned}[\mathsf{I}_x\varphi]^\infty &= \left[\varphi(0)\wedge\forall y\,(\varphi(y)\to\varphi(s(y)))\to\forall x\,\varphi(x)\right]^\infty\\ &= \overline{\left[\varphi(0)\wedge\forall y\,(\varphi(y)\to\varphi(s(y)))\right]^\infty}\vee\bigwedge_{n\in\mathbb{N}}\varphi^\infty(\overline{n})\end{aligned}$$

Example: induction axiom

The translation of the induction axiom

$$
\begin{aligned}
[\mathsf{I}_x\varphi]^\infty &= \left[\varphi(0) \land \forall y\,(\varphi(y) \to \varphi(s(y))) \to \forall x\,\varphi(x)\right]^\infty \\
&= \overline{\left[\varphi(0) \land \forall y\,(\varphi(y) \to \varphi(s(y)))\right]^\infty} \lor \bigwedge_{n\in\mathbb{N}} \varphi^\infty(\overline{n}) \\
&= \overline{\varphi^\infty}(0) \lor \overline{\bigwedge_{n\in\mathbb{N}} \overline{\varphi^\infty(\overline{n})} \lor \varphi^\infty(\overline{n+1})} \lor \bigwedge_{n\in\mathbb{N}} \varphi^\infty(\overline{n})
\end{aligned}
$$

Example: induction axiom

The translation of the induction axiom

$$
\begin{aligned}
[\mathsf{I}_x\varphi]^\infty &= \left[\varphi(0) \wedge \forall y\,(\varphi(y) \to \varphi(s(y))) \to \forall x\,\varphi(x)\right]^\infty \\
&= \overline{\left[\varphi(0) \wedge \forall y\,(\varphi(y) \to \varphi(s(y)))\right]^\infty} \vee \bigwedge_{n\in\mathbb{N}} \varphi^\infty(\overline{n}) \\
&= \overline{\varphi^\infty}(0) \vee \overline{\bigwedge_{n\in\mathbb{N}} \overline{\varphi^\infty(\overline{n})} \vee \varphi^\infty(\overline{n+1})} \vee \bigwedge_{n\in\mathbb{N}} \varphi^\infty(\overline{n}) \\
&= \overline{\varphi^\infty}(0) \vee \bigvee_{n\in\mathbb{N}} \varphi^\infty(\overline{n}) \vee \overline{\varphi^\infty}(\overline{n+1}) \vee \bigwedge_{n\in\mathbb{N}} \varphi^\infty(\overline{n})
\end{aligned}
$$

Outline

- ✓ Gentzen's consistency proof
- **The omega rule**
  - ✓ Infinitary propositional logic
  - **Infinitary proofs**
  - The consistency proof
- Cyclic proofs

Sequent calculus $\mathbf{LK}^\infty$

- **Definition.** The set of axioms is the smallest set which contains
  - $A, \overline{A}$ for any atom A,
  - S^∞ if S is an axiom of BA (as a sequent).

  and is closed under atomic cut, i.e.,
  - If Γ, A and $\Delta, \overline{A}$ are axioms, then so is a subset of Γ, Δ.

Sequent calculus $\mathbf{LK}^\infty$

- **Definition.** The set of axioms is the smallest set which contains
  - $A, \overline{A}$ for any atom A,
  - S^∞ if S is an axiom of BA (as a sequent).

  and is closed under atomic cut, i.e.,
  - If Γ, A and $\Delta, \overline{A}$ are axioms, then so is a subset of Γ, Δ.
- **Definition.** $\mathbf{LK}^\infty$ works on sequents of inf. prop. logic.

$$\frac{}{\Gamma, \Delta} \quad \text{if } \Delta \text{ is an axiom}$$

$$\frac{\Gamma, \varphi_j \quad \text{for a } j \in I}{\Gamma, \bigvee_{i\in I} \varphi_i} \qquad \frac{\Gamma, \varphi_j \quad \text{for all } j \in I}{\Gamma, \bigwedge_{i\in I} \varphi_i}$$

$$\frac{\Gamma, \varphi \quad \Gamma, \overline{\varphi}}{\Gamma} \text{ cut}$$

- Proofs of infinite width but finite height

Translation of BA-proofs

- **Def.** Translation of BA-proof of $\Gamma \Rightarrow \Delta$ to $\mathbf{LK}^{\infty}$-proof of $\overline{\Gamma^{\infty}}, \Delta^{\infty}$
  - Axioms ✓
  - $\wedge_{\mathsf{r}}$

$$\dfrac{\begin{matrix}(\pi_1)\\ \Gamma \Rightarrow \Delta, \varphi\end{matrix} \quad \begin{matrix}(\pi_2)\\ \Pi \Rightarrow \Lambda, \psi\end{matrix}}{\Gamma, \Pi \Rightarrow \Delta, \Lambda, \varphi \wedge \psi}\ \wedge_{\mathsf{r}} \qquad \mapsto \qquad \dfrac{\begin{matrix}(\pi_1^{\infty})\\ \overline{\Gamma^{\infty}}, \Delta^{\infty}, \varphi^{\infty}\end{matrix} \quad \begin{matrix}(\pi_2^{\infty})\\ \overline{\Pi^{\infty}}, \Lambda^{\infty}, \psi^{\infty}\end{matrix}}{\overline{\Gamma^{\infty}}, \overline{\Pi^{\infty}}, \Delta^{\infty}, \Lambda^{\infty}, \varphi^{\infty} \wedge \psi^{\infty}}$$

  - $\forall_{\mathsf{r}}$

$$\dfrac{\begin{matrix}(\pi(\alpha))\\ \Gamma \Rightarrow \Delta, \varphi(\alpha)\end{matrix}}{\Gamma \Rightarrow \Delta, \forall x\, \varphi(x)}\ \forall_{\mathsf{r}} \quad \mapsto \quad \dfrac{\begin{matrix}(\pi(\overline{n})^{\infty})\\ \overline{\Gamma^{\infty}}, \Delta^{\infty}, \varphi^{\infty}(\overline{n}) \quad \text{for all } n \in \mathbb{N}\end{matrix}}{\overline{\Gamma^{\infty}}, \Delta^{\infty}, \bigwedge_{n \in \mathbb{N}} \varphi^{\infty}(\overline{n})}$$

  - Similarily for other rules

Translation of BA-proofs

- **Def.** Translation of BA-proof of $\Gamma \Rightarrow \Delta$ to $\mathbf{LK}^\infty$-proof of $\overline{\Gamma^\infty}, \Delta^\infty$
  - Axioms ✓
  - $\wedge_\mathsf{r}$

$$\dfrac{\overset{(\pi_1)}{\Gamma \Rightarrow \Delta, \varphi} \qquad \overset{(\pi_2)}{\Pi \Rightarrow \Lambda, \psi}}{\Gamma, \Pi \Rightarrow \Delta, \Lambda, \varphi \wedge \psi}\ \wedge_\mathsf{r} \qquad \mapsto \qquad \dfrac{\overset{(\pi_1^\infty)}{\overline{\Gamma^\infty}, \Delta^\infty, \varphi^\infty} \qquad \overset{(\pi_2^\infty)}{\overline{\Pi^\infty}, \Lambda^\infty, \psi^\infty}}{\overline{\Gamma^\infty}, \overline{\Pi^\infty}, \Delta^\infty, \Lambda^\infty, \varphi^\infty \wedge \psi^\infty}$$

  - $\forall_\mathsf{r}$

$$\dfrac{\overset{(\pi(\alpha))}{\Gamma \Rightarrow \Delta, \varphi(\alpha)}}{\Gamma \Rightarrow \Delta, \forall x\, \varphi(x)}\ \forall_\mathsf{r} \quad \mapsto \quad \dfrac{\overset{(\pi(\overline{n})^\infty)}{\overline{\Gamma^\infty}, \Delta^\infty, \varphi^\infty(\overline{n})} \quad \text{for all } n \in \mathbb{N}}{\overline{\Gamma^\infty}, \Delta^\infty, \bigwedge_{n \in \mathbb{N}} \varphi^\infty(\overline{n})}$$

  - Similarily for other rules
- Formalisation: primitive recursive function

$\mathbf{LK}^{\infty}$ proves induction

- Informally: Assume $\varphi(0)$ and $\varphi(\overline{n}) \to \varphi(\overline{n+1})$, then

$$\dfrac{\varphi(0) \qquad \dfrac{\varphi(0) \quad \varphi(0) \to \varphi(1)}{\varphi(1)} \qquad \dfrac{\dfrac{\varphi(\bar{0}) \quad \varphi(\bar{0}) \to \varphi(\bar{1})}{\varphi(\bar{1})} \qquad \varphi(\bar{1}) \to \varphi(\bar{2})}{\varphi(\bar{2})} \qquad \cdots}{\bigwedge_{n \in \mathbb{N}} \varphi(\overline{n})}$$

$\mathbf{LK}^\infty$ proves induction

- Informally: Assume $\varphi(0)$ and $\varphi(\overline{n}) \to \varphi(\overline{n+1})$, then

$$\dfrac{\varphi(0) \qquad \dfrac{\varphi(0) \quad \varphi(0) \to \varphi(1)}{\varphi(1)} \qquad \dfrac{\dfrac{\varphi(\overline{0}) \quad \varphi(\overline{0}) \to \varphi(\overline{1})}{\varphi(\overline{1})} \qquad \varphi(\overline{1}) \to \varphi(\overline{2})}{\varphi(\overline{2})} \qquad \cdots}{\bigwedge_{n\in\mathbb{N}} \varphi(\overline{n})}$$

- Hence $\mathbf{LK}^\infty \vdash [\mathsf{I}_x\varphi(x)]^\infty$

$\mathbf{LK}^\infty$ proves induction

- Informally: Assume $\varphi(0)$ and $\varphi(\overline{n}) \to \varphi(\overline{n+1})$, then

$$\dfrac{\varphi(0) \qquad \dfrac{\varphi(0) \quad \varphi(0) \to \varphi(1)}{\varphi(1)} \qquad \dfrac{\dfrac{\varphi(\bar{0}) \quad \varphi(\bar{0}) \to \varphi(\bar{1})}{\varphi(\bar{1})} \qquad \varphi(\bar{1}) \to \varphi(\bar{2})}{\varphi(\bar{2})} \qquad \cdots}{\bigwedge_{n\in\mathbb{N}} \varphi(\overline{n})}$$

- Hence $\mathbf{LK}^\infty \vdash [\mathsf{I}_x \varphi(x)]^\infty$
    - One application of the ω-rule
    - Formalisation: prim. rec. function mapping $\mathsf{I}_x \varphi(x)$ to $\mathbf{LK}^\infty$-proof

Completeness of $\mathbf{LK}^{\infty}$

- **Obs.** For a first-order L-sentence σ: if $\mathbb{N} \models \sigma$, then $\mathbf{LK}^{\infty} \vdash \sigma^{\infty}$.

Completeness of $\mathbf{LK}^{\infty}$

- **Obs.** For a first-order L-sentence σ: if $\mathbb{N} \models \sigma$, then $\mathbf{LK}^{\infty} \vdash \sigma^{\infty}$.
  Proof. Induction on the logical complexity of σ:
  - If σ is atom, then $\mathrm{BA} \vdash \sigma$ with atomic cuts, so $\{\sigma\}$ is axiom.

Completeness of $\mathbf{LK}^\infty$

- **Obs.** For a first-order L-sentence σ: if $\mathbb{N} \models \sigma$, then $\mathbf{LK}^\infty \vdash \sigma^\infty$.

  Proof. Induction on the logical complexity of σ:

  - If σ is atom, then $\mathsf{BA} \vdash \sigma$ with atomic cuts, so $\{\sigma\}$ is axiom.
  - If $\sigma = \forall x\, \varphi(x)$, then $\mathbb{N} \models \varphi(\overline{n})$ for all $n \in \mathbb{N}$, so

$$\frac{\varphi^\infty(0) \quad \varphi^\infty(1) \quad \varphi^\infty(2) \quad \cdots}{\bigwedge_{n\in\mathbb{N}} \varphi^\infty(\overline{n})}$$

  by IH.

Completeness of $\mathbf{LK}^\infty$

- **Obs.** For a first-order L-sentence σ: if $\mathbb{N} \models \sigma$, then $\mathbf{LK}^\infty \vdash \sigma^\infty$.
  Proof. Induction on the logical complexity of σ:
  - If σ is atom, then $\mathrm{BA} \vdash \sigma$ with atomic cuts, so $\{\sigma\}$ is axiom.
  - If $\sigma = \forall x\, \varphi(x)$, then $\mathbb{N} \models \varphi(\overline{n})$ for all $n \in \mathbb{N}$, so

    $$\frac{\varphi^\infty(0) \quad \varphi^\infty(1) \quad \varphi^\infty(2) \quad \cdots}{\bigwedge_{n\in\mathbb{N}} \varphi^\infty(\overline{n})}$$

    by IH.
  - If $\sigma = \exists x\, \varphi(x)$, then there is a $k \in \mathbb{N}$ s.t. $\mathbb{N} \models \varphi(\overline{k})$, so

    $$\frac{\varphi^\infty(\overline{k})}{\bigvee_{n\in\mathbb{N}} \varphi^\infty(\overline{n})}$$

    by IH.
  - . . . □

Outline

✓ Gentzen's consistency proof

- **The omega rule**
  - ✓ Infinitary propositional logic
  - ✓ Infinitary proofs
  - **The consistency proof**

- Cyclic proofs

The height of a proof

- Proof height in a finite system, example:

$$\pi \quad = \quad \dfrac{\overset{(\pi_1)}{\Gamma \Rightarrow \Delta, A} \quad \overset{(\pi_2)}{\Pi \Rightarrow \Lambda, B}}{\Gamma, \Pi \Rightarrow \Delta, \Lambda, A \wedge B}\ \wedge_r$$

Then $\mathrm{h}(\pi) = 1 + \max\{\mathrm{h}(\pi_1), \mathrm{h}(\pi_2)\} = \sup\{\mathrm{h}(\pi_i) + 1 \mid i \in \{1, 2\}\}$.

The height of a proof

- Proof height in a finite system, example:

$$\pi \qquad = \qquad \cfrac{\overset{(\pi_1)}{\Gamma \Rightarrow \Delta, A} \quad \overset{(\pi_2)}{\Pi \Rightarrow \Lambda, B}}{\Gamma, \Pi \Rightarrow \Delta, \Lambda, A \wedge B} \; \wedge_{\mathrm{r}}$$

  Then $\mathrm{h}(\pi) = 1 + \max\{\mathrm{h}(\pi_1), \mathrm{h}(\pi_2)\} = \sup\{\mathrm{h}(\pi_i) + 1 \mid i \in \{1, 2\}\}$.

- **Definition.** For $\mathbf{LK}^\infty$-proof π with direct subproofs π_i, $i \in I$ define $\mathrm{h}(\pi) = \sup\{\mathrm{h}(\pi_i) + 1 \mid i \in I\}$

The cut rank of a proof

- **Definition.** For a formula φ with direct subformulas φ_i, $i \in I$ define the *depth of* φ as $\mathrm{d}(\varphi) = \sup\{\mathrm{d}(\varphi_i) + 1 \mid i \in I\}$.
- **Observation.** The depth of σ^∞ is $\leq$ the depth of σ.

The cut rank of a proof

- **Definition.** For a formula φ with direct subformulas φ_i, $i \in I$ define the *depth of* φ as $\mathrm{d}(\varphi) = \sup\{\mathrm{d}(\varphi_i) + 1 \mid i \in I\}$.
- **Observation.** The depth of σ^∞ is $\leq$ the depth of σ.
- **Definition.** For $\mathbf{LK}^\infty$-proof π with direct subproofs π_i, $i \in I$ and last inference ι define the *cut rank of* π:
  - If ι is cut on some φ, then $\rho(\pi) = \max\{\mathrm{d}(\varphi), \rho(\pi_1), \rho(\pi_2)\}$.
  - Otherwise, $\rho(\pi) = \sup\{\rho(\pi_i) \mid i \in I\}$.

The cut rank of a proof

- **Definition.** For a formula φ with direct subformulas φ_i, $i \in I$ define the *depth of* φ as $\mathrm{d}(\varphi) = \sup\{\mathrm{d}(\varphi_i) + 1 \mid i \in I\}$.
- **Observation.** The depth of σ^∞ is $\leq$ the depth of σ.
- **Definition.** For $\mathbf{LK}^\infty$-proof π with direct subproofs π_i, $i \in I$ and last inference ι define the *cut rank of* π:
  - If ι is cut on some φ, then $\rho(\pi) = \max\{\mathrm{d}(\varphi), \rho(\pi_1), \rho(\pi_2)\}$.
  - Otherwise, $\rho(\pi) = \sup\{\rho(\pi_i) \mid i \in I\}$.
- **Notation.** $\mathbf{LK}^\infty \vdash^\rho_\alpha S$ if there is an $\mathbf{LK}^\infty$-proof of S with cut rank $\leq \rho$ and height $\leq \alpha$.

The proof translation revisited

- **Lemma.** If PA $\vdash \sigma$, then there is an $r < \omega$ s.t. $\mathbf{LK}^{\infty} \vdash^{r}_{\omega \cdot 2} \sigma^{\infty}$.

  Proof. If PA $\vdash \sigma$, then there is a BA-proof π of $I_1, \ldots, I_n \Rightarrow \sigma$.

The proof translation revisited

- **Lemma.** If PA $\vdash \sigma$, then there is an $r < \omega$ s.t. $\mathbf{LK}^\infty \vdash^r_{\omega\cdot 2} \sigma^\infty$.

  Proof. If PA $\vdash \sigma$, then there is a BA-proof π of $I_1, \dots, I_n \Rightarrow \sigma$.

$$\psi \quad = \quad \cfrac{\overset{(\pi_n)}{I_n^\infty} \qquad \begin{array}{c} \cfrac{\overset{(\pi_1)}{I_1^\infty} \quad \overset{(\pi^\infty)}{\overline{I_1^\infty}, \dots, \overline{I_n^\infty}, \sigma^\infty}}{\overline{I_2^\infty}, \dots, \overline{I_n^\infty}, \sigma^\infty}\ \text{cut} \\ \vdots \\ \overline{I_n^\infty}, \sigma^\infty \end{array}}{\sigma^\infty}\ \text{cut}$$

$\mathrm{h}(\pi^\infty) < \omega$, $\mathrm{h}(\pi_i) = \omega$ for $1 \leq i \leq n$

The proof translation revisited

- **Lemma.** If PA $\vdash \sigma$, then there is an $r < \omega$ s.t. $\mathbf{LK}^\infty \vdash^r_{\omega\cdot 2} \sigma^\infty$.

  Proof. If PA $\vdash \sigma$, then there is a BA-proof π of $I_1, \dots, I_n \Rightarrow \sigma$.

$$\psi \qquad = \qquad \dfrac{\begin{array}{c}(\pi_n)\\ I_n^\infty\end{array} \qquad \begin{array}{c} \dfrac{\begin{array}{c}(\pi_1)\\ I_1^\infty\end{array} \qquad \begin{array}{c}(\pi^\infty)\\ \overline{I_1^\infty}, \dots, \overline{I_n^\infty}, \sigma^\infty\end{array}}{\overline{I_2^\infty}, \dots, \overline{I_n^\infty}, \sigma^\infty}\ \text{cut} \\ \vdots \\ \overline{I_n^\infty}, \sigma^\infty\end{array}}{\sigma^\infty}\ \text{cut}$$

$\mathrm{h}(\pi^\infty) < \omega$, $\mathrm{h}(\pi_i) = \omega$ for $1 \leq i \leq n$
$\Rightarrow \mathrm{h}(\psi) = w + n < w \cdot 2$. □

Cut-elimination in $\mathbf{LK}^\infty$

- **Theorem.** If $r < \omega$ and $\mathbf{LK}^\infty \vdash^r_\alpha S$, then $\mathbf{LK}^\infty \vdash^0_{2^\alpha_r} S$.

Cut-elimination in $\mathbf{LK}^\infty$

- **Theorem.** If $r < \omega$ and $\mathbf{LK}^\infty \vdash^r_\alpha S$, then $\mathbf{LK}^\infty \vdash^0_{2^\alpha_r} S$.
  Proof Sketch. "Standard" cut-elimination argument.

Cut-elimination in $\mathbf{LK}^{\infty}$

- **Theorem.** If $r < \omega$ and $\mathbf{LK}^{\infty} \vdash^{r}_{\alpha} S$, then $\mathbf{LK}^{\infty} \vdash^{0}_{2^{\alpha}_{r}} S$.
  Proof Sketch. “Standard” cut-elimination argument.
- **Corollary.** If PA $\vdash \sigma$, then $\mathbf{LK}^{\infty} \vdash^{0}_{\alpha} \sigma^{\infty}$ for some $\alpha < \varepsilon_0$.

Cut-elimination in $\mathbf{LK}^\infty$

- **Theorem.** If $r < \omega$ and $\mathbf{LK}^\infty \vdash^r_\alpha S$, then $\mathbf{LK}^\infty \vdash^0_{2^\alpha_r} S$.
  Proof Sketch. “Standard” cut-elimination argument.

- **Corollary.** If $\mathrm{PA} \vdash \sigma$, then $\mathbf{LK}^\infty \vdash^0_\alpha \sigma^\infty$ for some $\alpha < \varepsilon_0$.
  Proof. If $\mathrm{PA} \vdash \sigma$, then there is $r < \omega$ s.t. $\mathbf{LK}^\infty \vdash^r_{\omega\cdot 2} \sigma^\infty$. By the cut-elimination theorem, $\mathbf{LK}^\infty \vdash^0_{2^{\omega\cdot 2}_r} \sigma^\infty$ and $2^{\omega\cdot 2}_r < \omega_{r+2} < \varepsilon_0$.

Cut-elimination in $\mathbf{LK}^\infty$

- **Theorem.** If $r < \omega$ and $\mathbf{LK}^\infty \vdash^r_\alpha S$, then $\mathbf{LK}^\infty \vdash^0_{2^\alpha_r} S$.
  Proof Sketch. "Standard" cut-elimination argument.

- **Corollary.** If PA $\vdash \sigma$, then $\mathbf{LK}^\infty \vdash^0_\alpha \sigma^\infty$ for some $\alpha < \varepsilon_0$.
  Proof. If PA $\vdash \sigma$, then there is $r < \omega$ s.t. $\mathbf{LK}^\infty \vdash^r_{\omega\cdot 2} \sigma^\infty$. By the cut-elimination theorem, $\mathbf{LK}^\infty \vdash^0_{2^{\omega\cdot 2}_r} \sigma^\infty$ and $2^{\omega\cdot 2}_r < \omega_{r+2} < \varepsilon_0$.

- **Corollary.** PA is consistent.

Cut-elimination in $\mathbf{LK}^\infty$

- **Theorem.** If $r < \omega$ and $\mathbf{LK}^\infty \vdash^r_\alpha S$, then $\mathbf{LK}^\infty \vdash^0_{2^\alpha_r} S$.
  Proof Sketch. "Standard" cut-elimination argument.

- **Corollary.** If $\mathrm{PA} \vdash \sigma$, then $\mathbf{LK}^\infty \vdash^0_\alpha \sigma^\infty$ for some $\alpha < \varepsilon_0$.
  Proof. If $\mathrm{PA} \vdash \sigma$, then there is $r < \omega$ s.t. $\mathbf{LK}^\infty \vdash^r_{\omega \cdot 2} \sigma^\infty$. By the cut-elimination theorem, $\mathbf{LK}^\infty \vdash^0_{2^{\omega\cdot 2}_r} \sigma^\infty$ and $2^{\omega \cdot 2}_r < \omega_{r+2} < \varepsilon_0$.

- **Corollary.** PA is consistent.
  Proof. Suppose $\mathrm{PA} \vdash \bot$, then $\mathbf{LK}^\infty \vdash^0_\alpha \emptyset$ for some $\alpha < \varepsilon_0$, but there is not cut-free proof of $\emptyset$ in $\mathbf{LK}^\infty$.

Summary of 2nd part

- The ω-rule
- The calculus $\mathbf{LK}^{\infty}$
- Proofs of infinite width, no infinite branches
- Depth measured by ordinals
- Cut-elimination
- Consistency proof

Outline

✓ Gentzen's consistency proof

✓ The omega rule

- **Cyclic proofs**
  - **Infinite proofs**
  - Cyclic proofs
  - Proof by induction
  - Cyclic proofs vs. proofs by induction

Infinite descent

- Fermat: *descente infinie*
  There is no infinite descending chain $a_1 > a_2 > \cdots$ with $a_i \in \mathbb{N}$
- **Example.** $\sqrt{2}$ is irrational.
  Proof. Suppose there are $p, q \geq 1$ s.t. $\sqrt{2} = \frac{p}{q}$, i.e., $p^2 = 2q^2$.
  Then: $2 \mid p^2$,

Infinite descent

- Fermat: *descente infinie*
  There is no infinite descending chain $a_1 > a_2 > \cdots$ with $a_i \in \mathbb{N}$
- **Example.** $\sqrt{2}$ is irrational.
  Proof. Suppose there are $p, q \geq 1$ s.t. $\sqrt{2} = \frac{p}{q}$, i.e., $p^2 = 2q^2$.
  Then: $2 \mid p^2, \quad 4 \mid p^2,$

Infinite descent

- Fermat: *descente infinie*
  There is no infinite descending chain $a_1 > a_2 > \cdots$ with $a_i \in \mathbb{N}$
- **Example.** $\sqrt{2}$ is irrational.
  Proof. Suppose there are $p, q \geq 1$ s.t. $\sqrt{2} = \frac{p}{q}$, i.e., $p^2 = 2q^2$.
  Then: $2 \mid p^2, \quad 4 \mid p^2, \quad 4 \mid 2q^2,$

Infinite descent

- Fermat: *descente infinie*
  There is no infinite descending chain $a_1 > a_2 > \cdots$ with $a_i \in \mathbb{N}$
- **Example.** $\sqrt{2}$ is irrational.
  Proof. Suppose there are $p, q \geq 1$ s.t. $\sqrt{2} = \frac{p}{q}$, i.e., $p^2 = 2q^2$.
  Then: $2 \mid p^2, \quad 4 \mid p^2, \quad 4 \mid 2q^2, \quad 2 \mid q^2,$

Infinite descent

- Fermat: *descente infinie*
  There is no infinite descending chain $a_1 > a_2 > \cdots$ with $a_i \in \mathbb{N}$
- **Example.** $\sqrt{2}$ is irrational.
  Proof. Suppose there are $p, q \geq 1$ s.t. $\sqrt{2} = \frac{p}{q}$, i.e., $p^2 = 2q^2$.
  Then: $2 \mid p^2, \quad 4 \mid p^2, \quad 4 \mid 2q^2, \quad 2 \mid q^2, \quad 4 \mid q^2$

Infinite descent

- Fermat: *descente infinie*
  There is no infinite descending chain $a_1 > a_2 > \cdots$ with $a_i \in \mathbb{N}$

- **Example.** $\sqrt{2}$ is irrational.
  Proof. Suppose there are $p, q \geq 1$ s.t. $\sqrt{2} = \frac{p}{q}$, i.e., $p^2 = 2q^2$.
  Then: $2 \mid p^2, \quad 4 \mid p^2, \quad 4 \mid 2q^2, \quad 2 \mid q^2, \quad 4 \mid q^2$
  So $2 \mid p$, $2 \mid q$, let $p' = \frac{p}{2}$, $q' = \frac{q}{2}$.

Infinite descent

- Fermat: *descente infinie*
  There is no infinite descending chain $a_1 > a_2 > \cdots$ with $a_i \in \mathbb{N}$

- **Example.** $\sqrt{2}$ is irrational.
  Proof. Suppose there are $p, q \geq 1$ s.t. $\sqrt{2} = \frac{p}{q}$, i.e., $p^2 = 2q^2$.
  Then: $2 \mid p^2, \quad 4 \mid p^2, \quad 4 \mid 2q^2, \quad 2 \mid q^2, \quad 4 \mid q^2$
  So $2 \mid p$, $2 \mid q$, let $p' = \frac{p}{2}$, $q' = \frac{q}{2}$.
  Then $p'^2 = \frac{p^2}{4} = 2\frac{q^2}{4} = 2q'^2$.

Infinite descent

- Fermat: *descente infinie*
  There is no infinite descending chain $a_1 > a_2 > \cdots$ with $a_i \in \mathbb{N}$

- **Example.** $\sqrt{2}$ is irrational.
  Proof. Suppose there are $p, q \geq 1$ s.t. $\sqrt{2} = \frac{p}{q}$, i.e., $p^2 = 2q^2$.
  Then: $2 \mid p^2, \quad 4 \mid p^2, \quad 4 \mid 2q^2, \quad 2 \mid q^2, \quad 4 \mid q^2$
  So $2 \mid p$, $2 \mid q$, let $p' = \frac{p}{2}$, $q' = \frac{q}{2}$.
  Then $p'^2 = \frac{p^2}{4} = 2\frac{q^2}{4} = 2q'^2$.
  So there is an infinitely desceding sequence $p > p' > \dots$
  Contradiction. □

Infinite descent

- Fermat: *descente infinie*
  There is no infinite descending chain $a_1 > a_2 > \cdots$ with $a_i \in \mathbb{N}$

- **Example.** $\sqrt{2}$ is irrational.
  Proof. Suppose there are $p, q \geq 1$ s.t. $\sqrt{2} = \frac{p}{q}$, i.e., $p^2 = 2q^2$.
  Then: $2 \mid p^2, \quad 4 \mid p^2, \quad 4 \mid 2q^2, \quad 2 \mid q^2, \quad 4 \mid q^2$
  So $2 \mid p$, $2 \mid q$, let $p' = \frac{p}{2}$, $q' = \frac{q}{2}$.
  Then $p'^2 = \frac{p^2}{4} = 2\frac{q^2}{4} = 2q'^2$.
  So there is an infinitely desceding sequence $p > p' > \ldots$
  Contradiction. □

- 3rd part: formalisation of cyclic proofs [Brotherston, Simpson '11]

Inductive definitions

- First-order signature Σ
  Inductive predicate symbols $\Sigma_I \subseteq \Sigma$
- For each $P \in \Sigma_I$ a finite set of productions of the form

$$\frac{Q_1(\mathbf{u_1}) \quad \cdots \quad Q_k(\mathbf{u_k})}{P(\mathbf{t})}$$

  with $Q_1, \ldots, Q_k \in \Sigma$ and $\mathbf{t}, \mathbf{u_1}, \ldots, \mathbf{u_k}$ term vectors.
- *Example.*

$$\frac{}{N(0)} \qquad \frac{N(x)}{N(s(x))} \qquad \frac{}{L(\mathrm{nil})} \qquad \frac{N(x) \quad L(z)}{L(\mathrm{cons}(x,z))}$$

$$\frac{}{E(0)} \qquad \frac{E(x)}{O(s(x))} \qquad \frac{O(x)}{E(s(x))}$$

Case split rules

- For inductive predicate P, case split rule is:

$$\frac{\text{cases}}{P(\mathbf{u}), \Gamma \Rightarrow \Delta}\ \text{case}_P$$

where each production

$$\frac{Q_1(\mathbf{u_1}[\mathbf{x}]) \quad \cdots \quad Q_k(\mathbf{u_k}[\mathbf{x}])}{P(\mathbf{t}[\mathbf{x}])}$$

of P gives rise to a case (premise)

$$\Gamma, \mathbf{u} = \mathbf{t}[\mathbf{x}], Q_1(\mathbf{u_1}[\mathbf{x}]), \ldots, Q_k(\mathbf{u_k}[\mathbf{x}]) \Rightarrow \Delta$$

where $\mathbf{x}$ is fresh in each case.

Case split rules: examples

$$\frac{t = 0, \Gamma \Rightarrow \Delta \quad t = s(x), N(x), \Gamma \Rightarrow \Delta}{N(t), \Gamma \Rightarrow \Delta}\ \text{case}_N$$

Case split rules: examples

$$\frac{t = 0, \Gamma \Rightarrow \Delta \quad t = s(x), N(x), \Gamma \Rightarrow \Delta}{N(t), \Gamma \Rightarrow \Delta}\ \mathsf{case}_N$$

$$\frac{t = 0, \Gamma \Rightarrow \Delta \quad t = s(x), O(x), \Gamma \Rightarrow \Delta}{E(t), \Gamma \Rightarrow \Delta}\ \mathsf{case}_E$$

Case split rules: examples

$$\frac{t = 0, \Gamma \Rightarrow \Delta \quad t = s(x), N(x), \Gamma \Rightarrow \Delta}{N(t), \Gamma \Rightarrow \Delta} \text{ case}_N$$

$$\frac{t = 0, \Gamma \Rightarrow \Delta \quad t = s(x), O(x), \Gamma \Rightarrow \Delta}{E(t), \Gamma \Rightarrow \Delta} \text{ case}_E$$

$$\frac{t = s(x), E(x), \Gamma \Rightarrow \Delta}{O(t), \Gamma \Rightarrow \Delta} \text{ case}_O$$

Case split rules: examples

$$\frac{t = 0, \Gamma \Rightarrow \Delta \quad t = s(x), N(x), \Gamma \Rightarrow \Delta}{N(t), \Gamma \Rightarrow \Delta}\ \text{case}_N$$

$$\frac{t = 0, \Gamma \Rightarrow \Delta \quad t = s(x), O(x), \Gamma \Rightarrow \Delta}{E(t), \Gamma \Rightarrow \Delta}\ \text{case}_E$$

$$\frac{t = s(x), E(x), \Gamma \Rightarrow \Delta}{O(t), \Gamma \Rightarrow \Delta}\ \text{case}_O$$

$$\frac{t = \text{nil}, \Gamma \Rightarrow \Delta \quad t = \text{cons}(x, z), N(x), L(z), \Gamma \Rightarrow \Delta}{L(t), \Gamma \Rightarrow \Delta}\ \text{case}_L$$

Right-introduction rules

- **Definition.** Let P be inductive predicate and

  $$\frac{Q_1(\mathbf{u_1}[\mathbf{x}]) \quad \cdots \quad Q_k(\mathbf{u_k}[\mathbf{x}])}{P(\mathbf{t}[\mathbf{x}])}$$

  a production for P. Then

  $$\frac{\Gamma \Rightarrow \Delta, Q_1(\mathbf{u_1}[\mathbf{v}]) \quad \cdots \quad \Gamma \Rightarrow \Delta, Q_k(\mathbf{u_k}[\mathbf{v}])}{\Gamma \Rightarrow \Delta, P(\mathbf{t}[\mathbf{v}])} \; P_{\mathrm{r}}$$

  is a right-introduction rule for P, where $\mathbf{v}$ is a vector of terms.

Right-introduction rules: examples

$$\frac{}{\Gamma \Rightarrow \Delta, N(0)}\ N_r \qquad \frac{\Gamma \Rightarrow \Delta, N(t)}{\Gamma \Rightarrow \Delta, N(s(t))}\ N_r$$

Right-introduction rules: examples

$$\frac{}{\Gamma \Rightarrow \Delta, N(0)}\; N_{\mathrm{r}} \qquad \frac{\Gamma \Rightarrow \Delta, N(t)}{\Gamma \Rightarrow \Delta, N(s(t))}\; N_{\mathrm{r}}$$

$$\frac{}{\Gamma \Rightarrow \Delta, E(0)}\; E_{\mathrm{r}} \qquad \frac{\Gamma \Rightarrow \Delta, O(t)}{\Gamma \Rightarrow \Delta, E(s(t))}\; E_{\mathrm{r}} \qquad \frac{\Gamma \Rightarrow \Delta, E(t)}{\Gamma \Rightarrow \Delta, O(s(t))}\; O_{\mathrm{r}}$$

Right-introduction rules: examples

$$\frac{}{\Gamma \Rightarrow \Delta, N(0)}\ N_{\mathrm{r}} \qquad \frac{\Gamma \Rightarrow \Delta, N(t)}{\Gamma \Rightarrow \Delta, N(s(t))}\ N_{\mathrm{r}}$$

$$\frac{}{\Gamma \Rightarrow \Delta, E(0)}\ E_{\mathrm{r}} \qquad \frac{\Gamma \Rightarrow \Delta, O(t)}{\Gamma \Rightarrow \Delta, E(s(t))}\ E_{\mathrm{r}} \qquad \frac{\Gamma \Rightarrow \Delta, E(t)}{\Gamma \Rightarrow \Delta, O(s(t))}\ O_{\mathrm{r}}$$

$$\frac{}{\Gamma \Rightarrow \Delta, L(\mathrm{nil})}\ L_{\mathrm{r}} \qquad \frac{\Gamma \Rightarrow \Delta, N(t) \quad \Gamma \Rightarrow \Delta, L(u)}{\Gamma \Rightarrow \Delta, L(\mathrm{cons}(t, u))}\ L_{\mathrm{r}}$$

$\mathbf{LKID}^{\omega}$ pre-proofs

- **Definition.** Set D of inductive definitions, *rules of D-*$\mathbf{LKID}^{\omega}$ are:
  - usual **LK** for FOL with equality
  - the substitution rules

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma\sigma \Rightarrow \Delta\sigma}\ \text{subst}$$

  - The case split rules for ind. predicates of D
  - The right-introduction rules for ind. predicates of D

- **Notation.** $\mathbf{LKID}^{\omega}$ instead of D-$\mathbf{LKID}^{\omega}$.

$\mathbf{LKID}^\omega$ pre-proofs

- **Definition.** Set D of inductive definitions, *rules of* D-$\mathbf{LKID}^\omega$ are:
  - usual **LK** for FOL with equality
  - the substitution rules

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma\sigma \Rightarrow \Delta\sigma} \text{ subst}$$

  - The case split rules for ind. predicates of D
  - The right-introduction rules for ind. predicates of D
- **Notation.** $\mathbf{LKID}^\omega$ instead of D-$\mathbf{LKID}^\omega$.
- **Definition.** An $\mathbf{LKID}^\omega$ *pre-proof* is a (possibly infinite) tree built from these rules.

LKID$^\omega$ pre-proofs

- **Definition.** Set D of inductive definitions, *rules of D-***LKID**$^\omega$ are:
  - usual **LK** for FOL with equality
  - the substitution rules

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma\sigma \Rightarrow \Delta\sigma}\ \text{subst}$$

  - The case split rules for ind. predicates of D
  - The right-introduction rules for ind. predicates of D
- **Notation. LKID**$^\omega$ instead of D-**LKID**$^\omega$.
- **Definition.** An **LKID**$^\omega$ *pre-proof* is a (possibly infinite) tree built from these rules.
- **Remark. LKID**$^\omega$ pre-proofs are not sound.

LKID$^\omega$ proofs

- **Definition.** *Path* $(\Gamma_i \Rightarrow \Delta_i)_{1 \leq i < \alpha}$ of sequents (for some $\alpha \leq \omega$)

LKID$^\omega$ proofs

- **Definition.** *Path* $(\Gamma_i \Rightarrow \Delta_i)_{1 \leq i < \alpha}$ of sequents (for some $\alpha \leq \omega$)
- **Definition.** $(\tau_i)_{1 \leq i < \alpha}$ is a *trace* in $(\Gamma_i \Rightarrow \Delta_i)_{1 \leq i < \alpha}$ if
  - every τ_i is a $P\mathbf{t}$ in Γ_i for an inductive predicate P, and
  - τ_i is successor of τ_{i+1}.

LKID$^\omega$ proofs

- **Definition.** *Path* $(\Gamma_i \Rightarrow \Delta_i)_{1 \leq i < \alpha}$ of sequents (for some $\alpha \leq \omega$)
- **Definition.** $(\tau_i)_{1 \leq i < \alpha}$ is a *trace* in $(\Gamma_i \Rightarrow \Delta_i)_{1 \leq i < \alpha}$ if
  - every τ_i is a $P\mathbf{t}$ in Γ_i for an inductive predicate P, and
  - τ_i is successor of τ_{i+1}.
- **Definition.** i is a *progress point* in $(\tau_i)_{1 \leq i < \alpha}$ if τ_{i+1} obtained from τ_i by case split.

$\mathbf{LKID}^\omega$ proofs

- **Definition.** *Path* $(\Gamma_i \Rightarrow \Delta_i)_{1 \leq i < \alpha}$ of sequents (for some $\alpha \leq \omega$)
- **Definition.** $(\tau_i)_{1 \leq i < \alpha}$ is a *trace* in $(\Gamma_i \Rightarrow \Delta_i)_{1 \leq i < \alpha}$ if
  - every τ_i is a $P\mathbf{t}$ in Γ_i for an inductive predicate P, and
  - τ_i is successor of τ_{i+1}.
- **Definition.** i is a *progress point* in $(\tau_i)_{1 \leq i < \alpha}$ if τ_{i+1} obtained from τ_i by case split.
- **Definition.** An $\mathbf{LKID}^\omega$ *proof* is an $\mathbf{LKID}^\omega$ pre-proof that satisfies the *global trace condition*: every infinite path contains a trace with infinitely many progress points.

LKID$^{\omega}$: example

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{\Rightarrow E(0)}\;E_{\mathsf{r}}
}{x_0 = 0 \Rightarrow E(0), O(x_0)}\;\mathsf{w}^*
}{x_0 = 0 \Rightarrow E(x_0), O(x_0)}\;=
\qquad
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{\vdots}{N(x_1) \Rightarrow E(x_1), O(x_1)}\;\mathsf{case}_N
}{N(x_1) \Rightarrow O(x_1), O(s(x_1))}\;O_{\mathsf{r}}
}{N(x_1) \Rightarrow E(s(x_1)), O(s(x_1))}\;E_{\mathsf{r}}
}{x_0 = s(x_1), N(x_1) \Rightarrow E(s(x_1)), O(s(x_1))}\;\mathsf{w}_{\mathsf{l}}
}{x_0 = s(x_1), N(x_1) \Rightarrow E(x_0), O(x_0)}\;=
}{N(x_0) \Rightarrow E(x_0), O(x_0)}\;\mathsf{case}_N
$$

Properties of $\mathbf{LKID}^{\omega}$

- **Definition.** Standard model . . . inductive predicates are interpreted as least fixed points (of semantics of their productions)

Properties of $\textbf{LKID}^\omega$

- **Definition.** Standard model ... inductive predicates are interpreted as least fixed points (of semantics of their productions)
- **Theorem.** $\textbf{LKID}^\omega$ is sound w.r.t. standard models.

Properties of $\mathbf{LKID}^\omega$

- **Definition.** Standard model . . . inductive predicates are interpreted as least fixed points (of semantics of their productions)
- **Theorem.** $\mathbf{LKID}^\omega$ is sound w.r.t. standard models.
- **Theorem.** Cut-free $\mathbf{LKID}^\omega$ is complete w.r.t. standard models.
  Proof Sketch.
  - Construct proof search tree as $\mathbf{LKID}^\omega$ proof
  - If S not valid, search tree of S has infinite branch without progress

Outline

- ✓ Gentzen's consistency proof
- ✓ The omega rule
- **Cyclic proofs**
  - ✓ Infinite proofs
  - **Cyclic proofs**
  - Proof by induction
  - Cyclic proofs vs. proofs by induction

CLKID$^\omega$

- Consider derivation trees built from **LKID**$^\omega$-rules.
  (derivation tree: branch may end with non-axiom)
- **Definition.** A bud in $\mathcal{D}$ is a leaf which is not an axiom.

CLKID$^\omega$

- Consider derivation trees built from **LKID**$^\omega$-rules.
(derivation tree: branch may end with non-axiom)
- **Definition.** A bud in $\mathcal{D}$ is a leaf which is not an axiom.
- **Definition.** For a bud S in $\mathcal{D}$ an internal node S' in $\mathcal{D}$ is called *companion* of S if $S' = S$.

CLKID$^\omega$

- Consider derivation trees built from **LKID**$^\omega$-rules.
  (derivation tree: branch may end with non-axiom)
- **Definition.** A bud in $\mathcal{D}$ is a leaf which is not an axiom.
- **Definition.** For a bud S in $\mathcal{D}$ an internal node S' in $\mathcal{D}$ is called *companion* of S if $S' = S$.
- **Definition.** A **CLKID**$^\omega$ *pre-proof* is a pair $(\mathcal{D}, \gamma)$ where
  - $\mathcal{D}$ is a finite derivation tree, and
  - γ assigns a companion to each bud.

CLKID$^\omega$

- Consider derivation trees built from **LKID**$^\omega$-rules. (derivation tree: branch may end with non-axiom)
- **Definition.** A bud in $\mathcal{D}$ is a leaf which is not an axiom.
- **Definition.** For a bud S in $\mathcal{D}$ an internal node S' in $\mathcal{D}$ is called *companion* of S if $S' = S$.
- **Definition.** A **CLKID**$^\omega$ *pre-proof* is a pair $(\mathcal{D}, \gamma)$ where
  - $\mathcal{D}$ is a finite derivation tree, and
  - γ assigns a companion to each bud.
- **CLKID**$^\omega$ pre-proof unfolds to **LKID**$^\omega$-proof by identifying each bud with its companion.
- **Definition.** A **CLKID**$^\omega$ *proof* is a **CLKID**$^\omega$ pre-proof whose unfolding satisfies the global trace condition.

CLKID$^{\omega}$: Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Rightarrow N(0)}}{x = 0 \Rightarrow N(0)}\,\mathsf{w_l}}{x = 0 \Rightarrow N(x)}\,= \qquad \dfrac{\dfrac{\dfrac{\dfrac{O(x) \Rightarrow N(x)}{O(x') \Rightarrow N(x')}\,\text{subst}}{x = s(x'), O(x') \Rightarrow N(x')}\,\mathsf{w_l}}{x = s(x'), O(x') \Rightarrow N(s(x'))}\,N_r}{x = s(x'), O(x') \Rightarrow N(x)}\,=}{E(x) \Rightarrow N(x)}\,\text{case}_E \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{E(x) \Rightarrow N(x)}{E(x') \Rightarrow N(x')}\,\text{subst}}{x = s(x'), E(x') \Rightarrow N(x')}\,\mathsf{w_l}}{x = s(x'), E(x') \Rightarrow N(s(x'))}\,N_r}{x = s(x'), E(x') \Rightarrow N(x)}\,=}{O(x) \Rightarrow N(x)}\,\text{case}_O}{E(x) \vee O(x) \Rightarrow N(x)}\,\vee_l$$

Decidability

- **Theorem.** The following problem is decidable: given $\mathbf{CLKID}^{\omega}$ pre-proof $(\mathcal{D}, \gamma)$, is $(\mathcal{D}, \gamma)$ a $\mathbf{CLKID}^{\omega}$ proof?

Decidability

- **Theorem.** The following problem is decidable: given $\mathbf{CLKID}^\omega$ pre-proof $(\mathcal{D}, \gamma)$, is $(\mathcal{D}, \gamma)$ a $\mathbf{CLKID}^\omega$ proof?
- **Definition.** *Büchi automaton* is NFA accepting an infinite word $w \in \Sigma^\omega$ if w has a path visiting an accepting state infinitely often.

Decidability

- **Theorem.** The following problem is decidable: given **CLKID**$^\omega$ pre-proof $(\mathcal{D}, \gamma)$, is $(\mathcal{D}, \gamma)$ a **CLKID**$^\omega$ proof?
- **Definition.** *Büchi automaton* is NFA accepting an infinite word $w \in \Sigma^\omega$ if w has a path visiting an accepting state infinitely often.
- *Proof Sketch.* $P = (\mathcal{D}, \gamma)$ induces Büchi automata
  - B_{all} s.t. $\mathrm{L}(B_{\mathrm{all}})$ is set of all infinite paths, and
  - B_{acc} s.t. $\mathrm{L}(B_{\mathrm{acc}})$ is set of infinite paths satisfying prog. cond.

  $\mathrm{L}(B_{\mathrm{all}}) \subseteq \mathrm{L}(B_{\mathrm{acc}})$ is decidable. □

Outline

- ✓ Gentzen's consistency proof
- ✓ The omega rule
- **Cyclic proofs**
  - ✓ Infinite proofs
  - ✓ Cyclic proofs
  - **Proof by induction**
  - Cyclic proofs vs. proofs by induction

Induction rules

- **Definition.** Inductive predicate P, induction rule for P:

$$\frac{\text{minor premises} \qquad \Gamma, \varphi_P(\mathbf{u}) \Rightarrow \Delta}{\Gamma, P(\mathbf{u}) \Rightarrow \Delta}\ \text{ind}_P$$

  where

  - minor premises from productions of inductive predicates mutually dependent with P
  - one induction formula φ_Q for each such predicate Q

Induction rules: examples

$$\frac{\Gamma \Rightarrow \Delta, \varphi_N(0) \quad \varphi_N(x), \Gamma \Rightarrow \Delta, \varphi_N(s(x)) \quad \varphi_N(t), \Gamma \Rightarrow \Delta}{N(t), \Gamma \Rightarrow \Delta}\ \mathrm{ind}_N$$

Induction rules: examples

$$\frac{\Gamma \Rightarrow \Delta, \varphi_N(0) \quad \varphi_N(x), \Gamma \Rightarrow \Delta, \varphi_N(s(x)) \quad \varphi_N(t), \Gamma \Rightarrow \Delta}{N(t), \Gamma \Rightarrow \Delta}\ \mathrm{ind}_N$$

$$\frac{\Gamma \Rightarrow \Delta, \varphi_E(0) \quad \varphi_E(x), \Gamma \Rightarrow \Delta, \varphi_O(s(x)) \quad \varphi_O(x), \Gamma \Rightarrow \Delta, \varphi_E(s(x)) \quad \varphi_E(t), \Gamma \Rightarrow \Delta}{E(t), \Gamma \Rightarrow \Delta}\ \mathrm{ind}_E$$

Induction rules: examples

$$\frac{\Gamma \Rightarrow \Delta, \varphi_N(0) \quad \varphi_N(x), \Gamma \Rightarrow \Delta, \varphi_N(s(x)) \quad \varphi_N(t), \Gamma \Rightarrow \Delta}{N(t), \Gamma \Rightarrow \Delta}\ \mathrm{ind}_N$$

$$\frac{\Gamma \Rightarrow \Delta, \varphi_E(0) \quad \varphi_E(x), \Gamma \Rightarrow \Delta, \varphi_O(s(x)) \quad \varphi_O(x), \Gamma \Rightarrow \Delta, \varphi_E(s(x)) \quad \varphi_E(t), \Gamma \Rightarrow \Delta}{E(t), \Gamma \Rightarrow \Delta}\ \mathrm{ind}_E$$

$$\frac{\Gamma \Rightarrow \Delta, \varphi_L(\mathrm{nil}) \quad N(x), \varphi_L(z), \Gamma \Rightarrow \Delta, \varphi_L(\mathrm{cons}(x, z)) \quad \varphi_L(t), \Gamma \Rightarrow \Delta}{L(t), \Gamma \Rightarrow \Delta}\ \mathrm{ind}_L$$

Properties of **LKID**

- Henkin model . . . least fixed points formed in subset of power set

Properties of **LKID**

- Henkin model . . . least fixed points formed in subset of power set
- **Theorem. LKID** is sound w.r.t. Henkin models.

Properties of **LKID**

- Henkin model . . . least fixed points formed in subset of power set
- **Theorem. LKID** is sound w.r.t. Henkin models.
- **Theorem. LKID** without cut is complete w.r.t. Henkin models.

Properties of **LKID**

- Henkin model . . . least fixed points formed in subset of power set
- **Theorem. LKID** is sound w.r.t. Henkin models.
- **Theorem. LKID** without cut is complete w.r.t. Henkin models.
- **Lemma.** PA can be interpreted in **LKID** plus BA-axioms.

Properties of **LKID**

- Henkin model . . . least fixed points formed in subset of power set
- **Theorem. LKID** is sound w.r.t. Henkin models.
- **Theorem. LKID** without cut is complete w.r.t. Henkin models.
- **Lemma.** PA can be interpreted in **LKID** plus BA-axioms.
- **Corollary.** PA is consistent.

Outline

✓ Gentzen’s consistency proof

✓ The omega rule

▶ **Cyclic proofs**

  ✓ Infinite proofs

  ✓ Cyclic proofs

  ✓ Proof by induction

  ▶ **Cyclic proofs vs. proofs by induction**

Translation from **LKID** to **CLKID**$^\omega$ (1/2)

- **Theorem.** If **LKID** $\vdash \Gamma \Rightarrow \Delta$ then **CLKID**$^\omega \vdash \Gamma \Rightarrow \Delta$.

Translation from **LKID** to **CLKID**$^{\omega}$ (1/2)

- **Theorem.** If **LKID** $\vdash \Gamma \Rightarrow \Delta$ then **CLKID**$^{\omega}$ $\vdash \Gamma \Rightarrow \Delta$.

  Proof. Translate inductions into cycles. For example:

$$\dfrac{\overset{(\pi_{\mathsf{b}})}{\Gamma \Rightarrow \Delta, \varphi(0)} \quad \overset{(\pi_{\mathsf{s}})}{\varphi(x), \Gamma \Rightarrow \Delta, \varphi(s(x))} \quad \overset{(\pi_{\mathsf{c}})}{\varphi(t), \Gamma \Rightarrow \Delta}}{N(t), \Gamma \Rightarrow \Delta}\ \mathsf{ind}_N$$

Translation from **LKID** to **CLKID**$^\omega$ (1/2)

- **Theorem.** If **LKID** $\vdash \Gamma \Rightarrow \Delta$ then **CLKID**$^\omega \vdash \Gamma \Rightarrow \Delta$.
  Proof. Translate inductions into cycles. For example:

$$\dfrac{\overset{(\pi_{\mathrm{b}})}{\Gamma \Rightarrow \Delta, \varphi(0)} \quad \overset{(\pi_{\mathrm{s}})}{\varphi(x), \Gamma \Rightarrow \Delta, \varphi(s(x))} \quad \overset{(\pi_{\mathrm{c}})}{\varphi(t), \Gamma \Rightarrow \Delta}}{N(t), \Gamma \Rightarrow \Delta}\ \mathrm{ind}_N$$

Let $\mathcal{A} = \{\varphi(0), \forall x\,(\varphi(x) \to \varphi(s(x)))\}$, translate to

$$\dfrac{\dfrac{\dfrac{N(z), \mathcal{A} \Rightarrow \varphi(z)}{N(t), \mathcal{A} \Rightarrow \varphi(t)}\ \text{subst}}{N(t) \Rightarrow \bigwedge \mathcal{A} \to \varphi(t)} \qquad \dfrac{\overset{(\pi_{\mathrm{b}}, \pi_{\mathrm{s}})}{\Gamma \Rightarrow \bigwedge \mathcal{A}, \Delta} \quad \overset{(\pi_{\mathrm{c}})}{\varphi(t), \Gamma \Rightarrow \Delta}}{\Gamma, \bigwedge \mathcal{A} \to \varphi(t) \Rightarrow \Delta}\ \to_{\mathrm{l}}}{N(t), \Gamma \Rightarrow \Delta}\ \text{cut}$$

Translation from **LKID** to **CLKID**$^\omega$ (2/2)

- *Proof (cont.)* reminder: $\mathcal{A} = \{\varphi(0), \forall x\,(\varphi(x) \to \varphi(s(x)))\}$
  where

$$\dfrac{z = 0, \overset{\checkmark}{\mathcal{A}} \Rightarrow \varphi(z) \qquad \dfrac{\dfrac{\dfrac{\dfrac{\mathcal{A}, N(z) \Rightarrow \varphi(z)}{\mathcal{A}, N(y) \Rightarrow \varphi(y)}\ \text{subst} \qquad \varphi(s(y)) \Rightarrow \varphi(s(y))}{\mathcal{A}, N(y), \varphi(y) \to \varphi(s(y)) \Rightarrow \varphi(s(y))}\ \to_{\mathsf{l}}}{\mathcal{A}, N(y) \Rightarrow \varphi(s(y))}\ \mathsf{c}_{\mathsf{l}}, \forall_{\mathsf{l}}}{z = s(y), \mathcal{A}, N(y) \Rightarrow \varphi(z)}\ =, \mathsf{w}_{\mathsf{l}}}{\mathcal{A}, N(z) \Rightarrow \varphi(z)}\ \text{case}_N$$

□

- What about the other direction?

Brotherston/Simpson conjecture

- **Conjecture** [Brotherston/Simpson '11].

  If $\mathbf{CLKID}^{\omega} \vdash \Gamma \Rightarrow \Delta$ then $\mathbf{LKID} \vdash \Gamma \Rightarrow \Delta$.

Brotherston/Simpson conjecture

- **Conjecture** [Brotherston/Simpson '11].

  If $\mathbf{CLKID}^{\omega} \vdash \Gamma \Rightarrow \Delta$ then $\mathbf{LKID} \vdash \Gamma \Rightarrow \Delta$.

- **Theorem** [Simpson $\leq$ '17]. True for PA.

Brotherston/Simpson conjecture

- **Conjecture** [Brotherston/Simpson '11].

  If $\mathbf{CLKID}^{\omega} \vdash \Gamma \Rightarrow \Delta$ then $\mathbf{LKID} \vdash \Gamma \Rightarrow \Delta$.

- **Theorem** [Simpson $\leq$ '17]. True for PA.

- **Theorem** [Berardi/Tatsuta '17]. False in general.

Brotherston/Simpson conjecture

- **Conjecture** [Brotherston/Simpson '11].

  $$\text{If } \mathbf{CLKID}^{\omega} \vdash \Gamma \Rightarrow \Delta \text{ then } \mathbf{LKID} \vdash \Gamma \Rightarrow \Delta.$$

- **Theorem** [Simpson $\leq$ '17]. True for PA.
- **Theorem** [Berardi/Tatsuta '17]. False in general.
- **Theorem** [Berardi/Tatsuta '17]. True for calculi containing PA.

Cyclic arithmetic is equivalent to Peano arithmetic

- Let $L = \{0, s, +, \cdot, <\}$
- **Definition.** *Cyclic arithmetic (CA)* is set of first-order L-sentences σ s.t. σ has $\mathbf{CLKID}^{\omega}$ proof from basic arithmetic axioms where N is the only inductive predicate.

Cyclic arithmetic is equivalent to Peano arithmetic

- Let $L = \{0, s, +, \cdot, <\}$

- **Definition.** *Cyclic arithmetic (CA)* is set of first-order L-sentences σ s.t. σ has $\mathbf{CLKID}^{\omega}$ proof from basic arithmetic axioms where N is the only inductive predicate.

- **Theorem** [Simpson $\leq$'17]. CA = PA.

Cyclic arithmetic is equivalent to Peano arithmetic

- Let $L = \{0, s, +, \cdot, <\}$

- **Definition.** *Cyclic arithmetic (CA)* is set of first-order L-sentences σ s.t. σ has $\mathbf{CLKID}^{\omega}$ proof from basic arithmetic axioms where N is the only inductive predicate.

- **Theorem** [Simpson $\leq$'17]. CA = PA.
  Proof Sketch. PA $\subseteq$ CA ✓

Cyclic arithmetic is equivalent to Peano arithmetic

- Let $L = \{0, s, +, \cdot, <\}$
- **Definition.** *Cyclic arithmetic (CA)* is set of first-order L-sentences σ s.t. σ has $\mathbf{CLKID}^\omega$ proof from basic arithmetic axioms where N is the only inductive predicate.
- **Theorem** [Simpson $\leq$'17]. CA = PA.
  Proof Sketch. PA $\subseteq$ CA ✓
  CA $\subseteq$ PA:
  - Formalisation of unfolding $\mathbf{CLKID}^\omega \rightarrow \mathbf{LKID}^\omega$ in ACA_0 (incl. theory of Büchi automata)
  - Formalisation of soundness of $\mathbf{LKID}^\omega$ in ACA_0
  - Truth reflection principle for Σ_n-sentences
  - Conservativity of ACA_0 over PA

□

Extended equivalence

- **Definition.** Given set of inductive definitions D:
  - D-**LKID** $+$ PA: add basic arithmetic axioms and ind. pred. N
  - D-**CLKID**$^{\omega}$ $+$ PA: add basic arithmetic axioms and ind. pred. N

Extended equivalence

- **Definition.** Given set of inductive definitions D:
  - D-**LKID** + PA: add basic arithmetic axioms and ind. pred. N
  - D-$\mathbf{CLKID}^{\omega}$ + PA: add basic arithmetic axioms and ind. pred. N

- **Theorem** [Berardi/Tatsuta '17].

$$D\text{-}\mathbf{LKID} + \mathrm{PA} = D\text{-}\mathbf{CLKID}^{\omega} + \mathrm{PA}$$

Extended equivalence

- **Definition.** Given set of inductive definitions D:
  - D-**LKID** $+$ PA: add basic arithmetic axioms and ind. pred. N
  - D-**CLKID**$^{\omega}$ $+$ PA: add basic arithmetic axioms and ind. pred. N

- **Theorem** [Berardi/Tatsuta '17].

$$D\text{-}\mathbf{LKID} + \mathrm{PA} = D\text{-}\mathbf{CLKID}^{\omega} + \mathrm{PA}$$

Proof Sketch. D-**LKID** $+ \mathrm{PA} \subseteq D$-**CLKID**$^{\omega} + \mathrm{PA}$ ✓

Extended equivalence

- **Definition.** Given set of inductive definitions D:
  - D-**LKID** $+$ PA: add basic arithmetic axioms and ind. pred. N
  - D-**CLKID**$^{\omega}$ $+$ PA: add basic arithmetic axioms and ind. pred. N

- **Theorem** [Berardi/Tatsuta '17].

$$D\text{-}\mathbf{LKID} + \mathrm{PA} = D\text{-}\mathbf{CLKID}^{\omega} + \mathrm{PA}$$

Proof Sketch. D-**LKID** $+$ PA $\subseteq$ D-**CLKID**$^{\omega}$ $+$ PA ✓

D-**CLKID**$^{\omega}$ $+$ PA $\subseteq$ D-**LKID** $+$ PA:

1. Cut D-**CLKID**$^{\omega}$ $+$ PA proof π into cycle-free parts
2. Prove induction principle on order $<_{\pi}$ in PA
3. Combine 1. and 2. to D-**LKID** $+$ PA proof.

CLKID$^\omega$ is not equivalent to LKID (1/2)

- "2-Hydra statement“ provable in **CLKID**$^\omega$ but not in **LKID**
- Hydra: mythical monster: cut off one head, grows two new heads

CLKID$^\omega$ is not equivalent to **LKID** (1/2)

- "2-Hydra statement" provable in **CLKID**$^\omega$ but not in **LKID**
- Hydra: mythical monster: cut off one head, grows two new heads
- 2-Hydra: Let $a, b \in \mathbb{N}$, then

$$(a{+}1, b{+}2) \mapsto (a, b), \quad (0, b{+}2) \mapsto (b{+}1, b), \quad (a{+}2, 0) \mapsto (a{+}1, a)$$

Terminate if none of these rules apply.

CLKID$^\omega$ is not equivalent to LKID (1/2)

- "2-Hydra statement" provable in **CLKID**$^\omega$ but not in **LKID**
- Hydra: mythical monster: cut off one head, grows two new heads
- 2-Hydra: Let $a, b \in \mathbb{N}$, then

  $$(a+1, b+2) \mapsto (a, b), \quad (0, b+2) \mapsto (b+1, b), \quad (a+2, 0) \mapsto (a+1, a)$$

  Terminate if none of these rules apply.
- Formalisation: let $L = \{0/0, s/1, N/1, p/2\}$, N defined inductively

$$\begin{array}{rl}
(H) & H_1 \wedge H_2 \wedge H_3 \wedge H_4 \rightarrow \forall x, y \in N\, p(x, y) \\
(H_1) & p(0, 0) \wedge p(s(0), 0) \wedge \forall x \in N\, p(x, s(0)) \\
(H_2) & \forall x, y \in N\, \big(p(x, y) \rightarrow p(s(x), s(s(y)))\big) \\
(H_3) & \forall y \in N\, \big(p(s(y), y) \rightarrow p(0, s(s(y)))\big) \\
(H_4) & \forall x \in N\, \big(p(s(x), x) \rightarrow p(s(s(x)), 0)\big)
\end{array}$$

$\mathbf{CLKID}^\omega$ is not equivalent to **LKID** (2/2)

- **Lemma.** $\mathbf{CLKID}^\omega \vdash H$
  Proof. Short and straightforward cyclic proof.

$\textbf{CLKID}^\omega$ is not equivalent to **LKID** (2/2)

- **Lemma.** $\textbf{CLKID}^\omega \vdash H$
  Proof. Short and straightforward cyclic proof.

- **Theorem** [Berardi/Tatsuta '17]. $\textbf{LKID} \nvdash H$
  Proof Sketch. Counter-Henkin-structure:
  - Domain $\mathbb{N} \oplus \mathbb{Z}$
  - Suitable infinite sequence of pairs in $\mathbb{Z}$.

□

Summary of 3rd part

- Inductive definitions
- Infinitely deep proofs $\mathbf{LKID}^{\omega}$
  - Sound and complete w.r.t. standard models
- Cyclic subsystem $\mathbf{CLKID}^{\omega}$ of $\mathbf{LKID}^{\omega}$
  - Finite proofs
  - Sound and complete w.r.t. Henkin models
- Proofs by induction **LKID**
- $\mathbf{LKID} \subseteq \mathbf{CLKID}^{\omega}$
- $\mathbf{CLKID}^{\omega} \subseteq \mathbf{LKID}$ if PA is included

Summary

Three proof-theoretic approaches to induction:

- Induction rules
- The ω-rule
- Cyclic proofs

What this talk did not contain:

- The incompleteness theorems
- Program extraction
  (and consistency proofs based on that)
- Bounded arithmetic
  (and connections to computational complexity)
- Inductive theorem proving
- . . .