Introduction to Proof Theory

Lecture 2
Natural Deduction

Marianna Girlando, Sonia Marin

Universtiy of Amsterdam, University of Birmingham

OPLSS 2023

Eugene, Oregon, June 26 - July 8, 2023

Outline

First-order logic, Peano arithmetic

Intuitionistic logic

Natural deduction

What we saw yesterday

- propositional syntax
- first-order syntax
- proof systems
  - ↳ axiom system / Hilbert-Frege system
    - H_{cp}
    - H_{fo}
    - Peano Arithmetic

An axiom system for first-order logic: $\mathcal{H}_{fo}$

A, B, C formulas of $\mathcal{L}^=$

Axioms and inference rules of $\mathcal{H}_{cp}$, plus:

FO1. $\forall x(A(x)) \to A(t)$ term

FO2. $A(t) \to \exists x(A(x))$

FO3. $\forall x(A \to B(x)) \to \big(A \to \forall x(B(x))\big)$ where $x \notin FV(A)$

FO4. $\forall x(A(x) \to B) \to \big(\exists x(A(x)) \to B\big)$ where $x \notin FV(B)$

An axiom system for first-order logic: $\mathcal{H}_{fo}$

A, B, C formulas of $\mathcal{L}^{=}$

Axioms and inference rules of $\mathcal{H}_{cp}$, plus:

FO1. $\forall x(A(x)) \to A(t)$

FO2. $A(t) \to \exists x(A(x))$

FO3. $\forall x(A \to B(x)) \to \big(A \to \forall x(B(x))\big)$ where $x \notin FV(A)$

FO4. $\forall x(A(x) \to B) \to \big(\exists x(A(x)) \to B\big)$ where $x \notin FV(B)$

FO~~4~~5. $\forall x(x = x)$

FO~~5~~6. $\forall x \forall y\big(x = y \to (A(x) \to A(y))\big)$

$$\text{gen}\ \frac{A}{\forall x(A)}$$

Prove the following:

☞ $\{\forall x(A \to B), \forall x(A)\} \vdash_{\mathcal{H}_{fo}} \forall x(B)$

Proofs in $\mathcal{H}_{fo}$

A formula of $\mathcal{L}^=$, Γ set of formulas of $\mathcal{L}^=$:

A $\mathcal{H}_{fo}$ derivation of A from assumptions in Γ is a list of $\mathcal{L}^=$ formulas

$$\begin{array}{c} A_1 \\ A_2 \\ \vdots \\ A_n \end{array}$$

where $A_n = A$ and for each A_i, for $i \leq n$, we have that either:

- A_i is an axiom of $\mathcal{H}_{fo}$;
- $A_i \in \Gamma$;
- A_i is obtained by applying (mp) or (gen) to $A_1, \ldots, A_{i-1}$.

We write $\Gamma \vdash_{\mathcal{H}_{fo}} A$ if there is a derivation of A from formulas in Γ.

A proof of A is a derivation of A from $\emptyset$. We write $\vdash_{\mathcal{H}_{fo}} A$ if there is a proof of A.

First-order logic FOL is defined as $\{A \mid \vdash_{\mathcal{H}_{fo}} A\}$.

Peano Arithmetic (PA)

A first-order theory $\mathcal{T}$ consists of:

- A predicate language $\mathcal{L}^{=}_{\mathcal{T}}$;
- A set of formulas in the language $\mathcal{L}^{=}_{\mathcal{T}}$, the non-logical axioms of the theory.

Peano Arithmetic (PA) is a first-order theory

constant

unary function symbol

$x \mapsto x+1$

$$\mathcal{L}^{=}_{PA} = \{0, s, +, \cdot\}$$

binary function symbols

Peano Arithmetic (PA)

A first-order theory $\mathcal{T}$ consists of:

- A predicate language $\mathcal{L}^{=}_{\mathcal{T}}$;
- A set of formulas in the language $\mathcal{L}^{=}_{\mathcal{T}}$, the non-logical axioms of the theory.

Peano Arithmetic (PA) is a first-order theory

$(0 = s(x)) \to \bot$

$$\mathcal{L}^{=}_{PA} = \{0, s, +, \cdot\}$$

0

$s(0)$

$s(s(0))$

$\vdots$

$s(0) + 0 \leftarrow$

$s(s(0)) \cdot s(0)$

$\vdots$

PA1. $\forall x(0 \neq s(x))$

PA2. $\forall x \forall y(s(x) = s(y) \to x = y)$

PA3. $\forall x(x + 0 = x)$

PA4. $\forall x \forall y(x + s(y) = s(x + y))$

PA5. $\forall x(x \cdot 0 = 0)$

PA6. $\forall x \forall y(x \cdot s(y) = (x \cdot y) + x)$

PA7. $\big(A(0) \wedge \forall x(A(x) \to A(s(x)))\big) \to \forall x(A(x))$
where $A \in \mathcal{L}^{=}_{PA}, x \in FV(A)$

An example

Prove the following in *PA*:

- ☞ $\forall x\big(x \neq s(x)\big)$

  Set $A(x) := x \neq s(x)$

  To prove: $A(0) \wedge \forall x(A(x) \rightarrow A(s(x)))$

  Using (mp) and PA7. $\big(\underline{A(0)} \wedge \underline{\forall x(A(x) \rightarrow A(s(x)))}\big) \rightarrow \forall x(A(x))$

  conclude $\forall x(A(x))$

Proof of $A(0) := 0 \neq s(0)$

1 $\forall x\,(0 \neq s(x))$ PA1.

2 $\forall x\,(0 \neq s(x)) \rightarrow 0 \neq s(0)$ instance of FO1

3 $0 \neq s(x)$ mp on 1, 2

Proof of $\forall\ (A(x) \rightarrow A(s(x))) :=$

$:= \underbrace{\forall x\,(x \neq s(x) \rightarrow s(x) \neq s(s(x)))}$

this is an instance of the following:

$\leftarrow [\forall x \forall y\,(s(x) \neq s(y) \rightarrow x = y)$

(take $x := x$
$y := s(x)$)

and this is an instance of PA2,

- ☞ $\forall x\big(0 + x = x\big)$

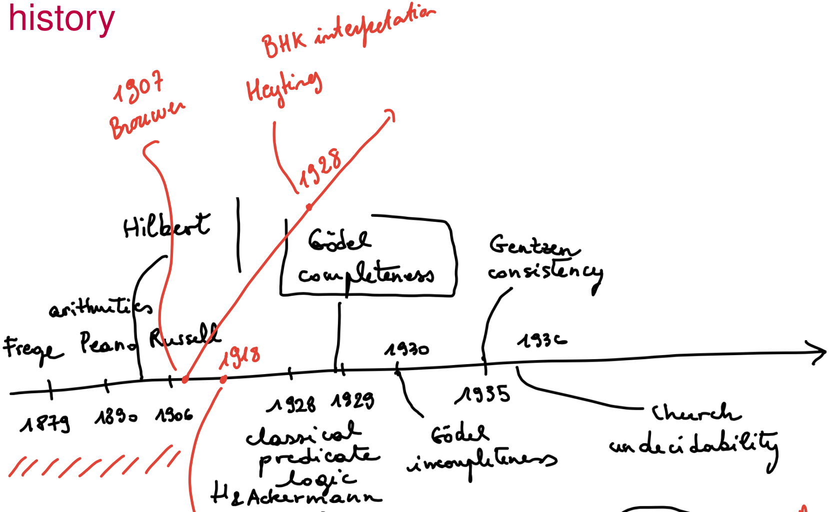
Outline

First-order logic, Peano arithmetic

Intuitionistic logic

Natural deduction

Some history



weyl "house built on sand"

$$\dfrac{\begin{matrix}A\\ \vdots\\ \bot\end{matrix}}{\neg A} \qquad \dfrac{\begin{matrix}\neg A\\ \vdots\\ \bot\end{matrix}}{A}$$

$A \vee \neg A$

⇒ rejection of the fact that there are 2 truth values

⇒ rejection of indirect reasoning

Constructive proofs?

??

Theorem. There exist irrational numbers a, b s.t. a^b is rational.

Proof # 1. Take $a = b = \sqrt{2}$. Then $\boxed{\sqrt{2}^{\sqrt{2}}}$ is either rational or irrational. If it is rational, the statement is proved. If it is irrational, take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Then $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$, and the statement is proved.

Proof # 2. Take $a = \sqrt{2}$ and $b = log_2 9$. Then $a^b = 3$.

An axiom system for intuitionistic propositional logic: $\mathcal{H}_{ip}$

Syntax of intuitionistic propositional logic: $\mathcal{L}_p$

- $\mathrm{Var}_p = \{p, q, r, \dots\}$
- $\bot, \wedge, \vee, \rightarrow$

A, B, C formulas of $\mathcal{L}_p$

PL1. $B \rightarrow (A \rightarrow B)$
PL2. $\big(A \rightarrow (B \rightarrow C)\big) \rightarrow \big((A \rightarrow B) \rightarrow (A \rightarrow C)\big)$
PL3. $(A \wedge B) \rightarrow A$
PL4. $(A \wedge B) \rightarrow B$
PL5. $A \rightarrow \big(B \rightarrow (A \wedge B)\big)$
PL6. $A \rightarrow (A \vee B)$
PL7. $B \rightarrow (A \vee B)$
PL8. $(A \rightarrow C) \rightarrow \big((B \rightarrow C) \rightarrow \big((A \vee B) \rightarrow C\big)\big)$
PL9. $\bot \rightarrow A$
PL10. $A \vee (A \rightarrow \bot)$

$$\text{mp}\ \frac{A \qquad\qquad A \rightarrow B}{B}$$

An axiom system for intuitionistic propositional logic: $\mathcal{H}_{ip}$

Syntax of intuitionistic propositional logic: $\mathcal{L}_p$

- $\mathrm{Var}_p = \{p, q, r, \dots\}$
- $\bot, \wedge, \vee, \rightarrow$

A, B, C formulas of $\mathcal{L}_p$

PL1. $B \rightarrow (A \rightarrow B)$
PL2. $\big(A \rightarrow (B \rightarrow C)\big) \rightarrow \big((A \rightarrow B) \rightarrow (A \rightarrow C)\big)$
PL3. $(A \wedge B) \rightarrow A$
PL4. $(A \wedge B) \rightarrow B$
PL5. $A \rightarrow \big(B \rightarrow (A \wedge B)\big)$
PL6. $A \rightarrow (A \vee B)$
PL7. $B \rightarrow (A \vee B)$
PL8. $(A \rightarrow C) \rightarrow \big((B \rightarrow C) \rightarrow \big((A \vee B) \rightarrow C\big)\big)$
PL9. $\bot \rightarrow A$

$$\mathrm{mp}\ \frac{A \qquad\qquad A \rightarrow B}{B}$$

Some examples

Formulas that are not provable in $\mathcal{H}_{ip}$:

- $A \vee \neg A$ (Excluded middle)
- $\neg\neg A \rightarrow A$ (Double negation)
- $((A \rightarrow B) \rightarrow A) \rightarrow A$ (Pierce's Law)
- $(A \rightarrow B) \rightarrow (\neg A \vee B)$

Formulas that are provable in $\mathcal{H}_{ip}$:

- $(\neg A \vee B) \rightarrow \cancel{(\neg A \vee B)}$ $A \rightarrow B$
- $(A \vee B) \rightarrow \neg(\neg A \wedge \neg B)$

Proofs in $\mathcal{H}_{ip}$

For A formula of $\mathcal{L}_p$, Γ set of formulas of $\mathcal{L}_p$:

A $\mathcal{H}_{ip}$ derivation of A from assumptions in Γ is a list of $\mathcal{L}_p$ formulas

$$\begin{array}{c} A_1 \\ A_2 \\ \vdots \\ A_n \end{array}$$

where $A_n = A$ and for each A_i, for $i \leq n$, we have that either:

- A_i is an axiom of $\mathcal{H}_{cp}$;
- $A_i \in \Gamma$;
- A_i is obtained by applying (mp) to formulas in $A_1, \ldots, A_{i-1}$.

We write $\Gamma \vdash_{\mathcal{H}_{ip}} A$ if there is a derivation of A from formulas in Γ.

A proof of A is a derivation of A from $\emptyset$. We write $\vdash_{\mathcal{H}_{ip}} A$ if there is a proof of A.

Intuitionistic propositional logic IPL is defined as $\{A \mid \vdash_{\mathcal{H}_{ip}} A\}$.

Outline

First-order logic, Peano arithmetic

Intuitionistic logic

Natural deduction

Pros and cons axioms

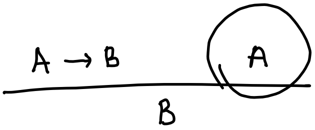
- **Pro:** make precise how connectives interact and the principles of mathematical reasoning
- **Con:** searching for a proof is painful because we can use only modus ponens
  - what about other common proof techniques?

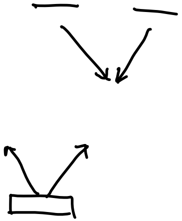
proof by cases e.g. X is finite or infinite

Let x be ....

Pros and cons axioms

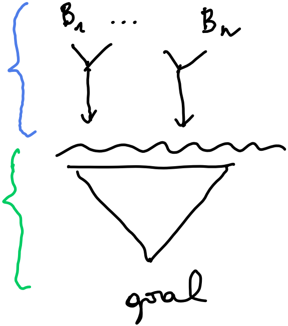
- **Pro:** make precise how connectives interact and the principles of mathematical reasoning
- **Con:** searching for a proof is painful because we can use only modus ponens
  - what about other common proof techniques?
  - what is A?





Natural deduction - informally

More proof techniques than MP
and use assumptions



elimination rules

introduction rules

analyse assumptions

meet $\longrightarrow$ proof

decompose goal

Introduction rules

give sufficient conditions for deriving statement depending on its form

$$\frac{A \qquad B}{A \wedge B}\ \wedge I \qquad \frac{A}{A \vee B}\ \vee I_1 \qquad \frac{B}{A \vee B}\ \vee I_2$$

$$\frac{\begin{array}{c}[A]^{\bullet} \\ \vdots \\ B\end{array}}{A \to B}\ \to I^{\bullet}$$

when temporary assumption has been used
it can be **discharged**
↳ indicated by $[\,\cdot\,]$

Elimination rules

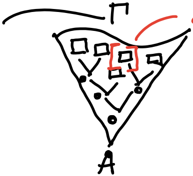
derive statements from assumptions that can be used

$$\frac{A \wedge B}{A}\,\wedge E_1 \qquad \frac{A \wedge B}{B}\,\wedge E_2 \qquad \frac{A \to B \qquad A}{B}\,\to_E$$

$$\frac{A \vee B \qquad \begin{array}{c}[A]\\ \vdots\\ C\end{array} \qquad \begin{array}{c}[B]\\ \vdots\\ C\end{array}}{C}\,\vee_E \qquad \frac{\perp}{C}\,\perp_E$$

Deduction trees

open assumptions



discharged assumptions

$\nvdash \Gamma$

$$\Gamma \vdash_{NJ} A$$

A derivation of formula $\underline{A}$ from $\underline{\text{set}}$ of assumptions (formulas) Γ is a tree of formulas in which each formula is

- either an assumption in Γ
- or the conclusion of a correct application of an inference rule.

If every assumption is discharged, it is a proof of A.

$$\emptyset \vdash_{NJ} A$$

N

Natural deduction for Intuitionistic Logic

J

$$\frac{\begin{array}{c}\bar{\ } \\ \vdots \\ B\end{array}}{A \to B}$$

Ass.

1: A