Introduction to Proof Theory

Lecture 1
Proof Theory and Proof Systems

Marianna Girlando, Sonia Marin

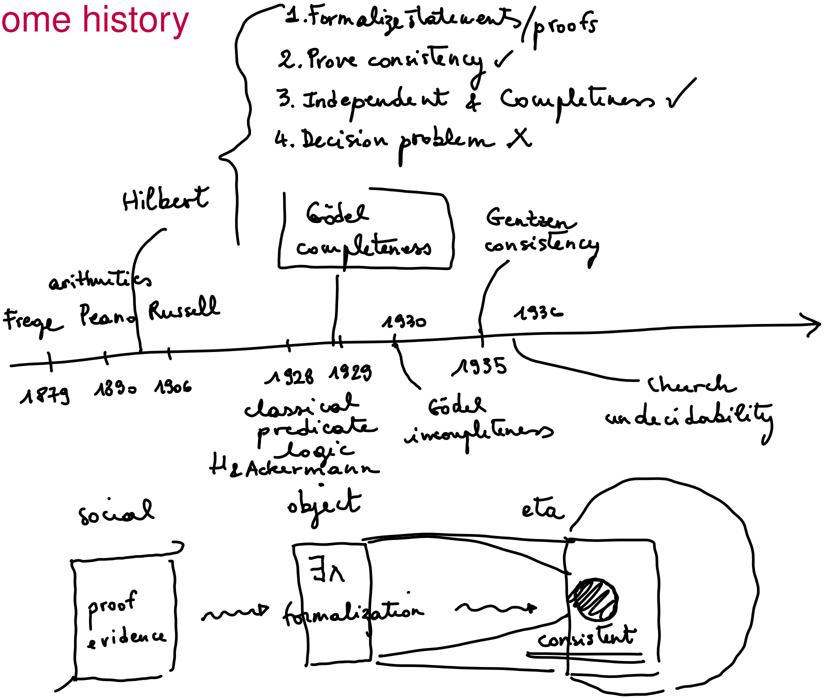
Universtiy of Amsterdam, University of Birmingham

OPLSS 2023

Eugene, Oregon, June 26 - July 8, 2023

Outline

Some history



Outline

1. History: Why it started?
   Formal language & First proof system
   Classical logic & Arithmetic

2. Intuitionistic / Constructive
   Related to prog lang theory

3. Natural Deduction
   Sequent calculus

4. Cut Elimination / Normalization

5. Back to arithmetics
   Etc.

Outline

Propositional logic: syntax

Language

- Countably many propositional variables:

$$\text{Var}_p = \{p, q, r, \dots\}$$

- Propositional constants: $\bot$ (*false*)
- Connectives: $\vee$ (*disjunction*), $\wedge$ (*conjunction*), $\rightarrow$ (*implication*)

Formulas (Form_p) $A, B, C, \dots$ are inductively generated as follows:

- Propositional variables and constants are formulas
- If A, B are formulas then $A \vee B$, $A \wedge B$, $A \rightarrow B$ are formulas.

$\neg A := A \rightarrow \bot$ $\qquad\qquad$ $\top := p \vee (p \rightarrow \bot)$

How do we interpret propositional formulas?

- Propositional assignment: assigns $\{0,1\}$ to propositional variables

$$\alpha : \mathrm{Var}_p \to \{0,1\}$$

- Extend the assignment to formulas

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

A	B	$A \to B$
1	1	1
1	0	0
0	1	1
0	0	1

Equivalently: Define $\alpha \models A$ "α satisfies A"

$\alpha \not\models \bot$

$\alpha \models p$ *iff* $\alpha(p) = 1$

$\alpha \models A \wedge B$ *iff* $\alpha \models A$ and $\alpha \models B$

$\alpha \models A \vee B$ *iff* $\alpha \models A$ or $\alpha \models B$

$\alpha \models A \to B$ *iff* $\alpha \not\models A$ or $\alpha \models B$

Predicate logic: language

We define a predicate language $\mathcal{L}^{=}$ as follows:

- Countably many variables: $\mathrm{Var} = \{x, y, z, \ldots\}$
- A set of function symbols: $\mathrm{Fun} = \{f, g, h, \ldots\}$

  Each function symbol has a fixed *arity* (n of arguments it takes)

  0-ary function symbols are called constants
- A set of predicate symbols: $\mathrm{Pred} = \{P, Q, R, \ldots\}$

  Each predicate symbol has a fixed *arity* (n of arguments it takes)

  Propositional variables are 0-ary predicates
- The equality symbol = (2-ary predicate)
- Propositional constants: $\bot$
- Connectives $\vee, \wedge, \rightarrow$.
- Quantifiers: $\exists$ (*existential*) and $\forall$ (*universal*)

Predicate logic: terms

$f: \mathbb{N}^n \to \mathbb{N}$

Terms (Ter) $s, t, u, \ldots$ are inductively generated as follows:

- Variables are terms
- If $f \in$ Fun is a k-ary function symbol and $t_1, \ldots, t_k$ are terms, then the following is a term:

$$f(t_1, \ldots, t_k)$$

Any constant is a term.

Informally, terms denote individual entities.

Predicate logic: formulas

Atomic formulas $P(t_1, \ldots, t_k)$ are inductively generated as follows:

- If s, t are terms, then $s = t$ is an atomic formula.
- If P is a predicate symbol or arity k and $t_1, \ldots, t_k$ are terms, then the following is an atomic formula:

$$P(t_1, \ldots, t_k)$$

Formulas (Form) $P, Q, R, \ldots$ are inductively generated as follows:

- Atomic formulas are formulas
- $\perp$ is a formula
- If A, B are formulas then $A \vee B$, $A \wedge B$ and $A \rightarrow B$ are formulas
- If A is a formula then $\exists x A$ and $\forall x A$ are formulas.

Outline

Introduction

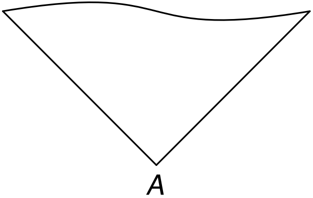
Propositional and first order syntax

Proof systems

Proof systems, informally

A proof system consists of:

- Set of axioms;
- Set of inference rules.



A proof of a formula A is constructed by chaining together axioms, inference rules, and objects generated from axioms and inference rules, until A is reached.

A logic can be identified with the set of provable formulas.

Various kinds of proof systems

- Hilbert-Frege proof systems, or axiom systems, or reductive systems (Prawitz, 1971)
- Gentzen-style proof systems

Today:

- Axiom system for propositional logic
- Axiom system for first-order logic
- First-order theories and Peano Arithmetic

An axiom system for classical propositional logic: $\mathcal{H}_{cp}$

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

PL1.	$A \to (B \to A)$
PL2.	$\big(A \to (B \to C)\big) \to \big((A \to B) \to (A \to C)\big)$
PL3.	$(A \land B) \to A$
PL4.	$(A \land B) \to B$
PL5.	$A \to \big(B \to (A \land B)\big)$
PL6.	$A \to (A \lor B)$
PL7.	$B \to (A \lor B)$
PL8.	$(A \to C) \to \big((B \to C) \to \big((A \lor B) \to C\big)\big)$
PL9.	$\bot \to A$
PL10.	$A \lor (A \to \bot)$

$$\text{mp}\,\frac{A \qquad\qquad A \to B}{B}$$

Examples

Prove the following:

- ☞ $\vdash_{\mathcal{H}_{cp}} A \rightarrow A$
- ☞ $\{A \rightarrow B, B \rightarrow C\} \vdash_{\mathcal{H}_{cp}} A \rightarrow C$

PL1. $A \rightarrow (B \rightarrow A)$

PL2. $\big(A \rightarrow (B \rightarrow C)\big) \rightarrow \big((A \rightarrow B) \rightarrow (A \rightarrow C)\big)$

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

1	$A \rightarrow ((B \rightarrow A) \rightarrow A)$	PL1
2	$(A \rightarrow ((B \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (B \rightarrow A)) \rightarrow (A \rightarrow A))$	PL2
3	$(A \rightarrow (B \rightarrow A)) \rightarrow (A \rightarrow A)$	mp 1, 2
4	$A \rightarrow (B \rightarrow A)$	PL1
5	$A \rightarrow A$	mp 3, 4

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

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

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

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

Classical propositional logic CPL is defined as $\{A \mid \vdash_{\mathcal{H}_{cp}} A\}$.

Deduction Theorem

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

$$\Gamma \vdash_{\mathcal{H}_{cp}} A \to B \quad \text{iff} \quad \Gamma \cup \{A\} \vdash_{\mathcal{H}_{cp}} B$$

$$\begin{array}{c} \Gamma \\ \vdots \\ A \to B \end{array} \quad \Longleftrightarrow \quad \begin{array}{c} \Gamma \cup \{A\} \\ \vdots \\ B \end{array}$$

$\Rightarrow)$

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

$\Rightarrow)$ MANCOSU, GALVAN, ZACH

An Introduction to Proof Theory

$\Leftarrow$