Foundations of formal proof systems

Benjamin Werner

Ecole Polytechnique

MPRI

2-7-1

2023
How do we define mathematics?

All humans are mortal, Socrates is human, thus Socrate is mortal.

correction: *syntaxic* criterion

$$\vdash A \Rightarrow B \quad \vdash A \quad \vdash B$$

The stones to build mathematical proofs

$$\vdash \forall x. H(x) \Rightarrow M(x) \quad \vdash H(S)$$

$$\vdash H(s) \Rightarrow M(S)$$

$$\vdash M(S)$$

A mathematical proof is a *construction*
Birth of modern mathematical logic

Mathematical truth defined through totally objective rules

1872 : The *Begriffsschrift* of Frege

proof = tree structure
A century later

Mechanical verification becomes real

First proof system: Automath (1968)

N. G. de Bruijn

Formal proofs are *actually* built.

Today

A modern proof system: Coq

- Same principle
- More modern formalism
What do we want from a formalism

Before (informal proofs) : we want the formalism to be expressive (many theorems)

Now (formal proofs) we want also :
  ▶ Concise proofs
  ▶ Close to our intuition (no spurious syntactical hacking)
  ▶ ... 

This course : study formalisms with these aims in mind
First-order logic - language

A set of variables: $x, y, z, \ldots$

A set of function symbols: $f, g, h, \ldots$ each function symbol has an arity (number of arguments).
A set of predicate symbols: $A, B, C, P, R \ldots$ each with an arity.

Objects:

- a variable is a term,
- if $f$ is of arity $n$ and $t_1, \ldots, t_n$ are terms, then $f(t_1, \ldots, t_n)$ is a term.

Propositions:

- if $P$ is of arity $n$ then $P(t_1, \ldots, t_n)$ is a proposition
- is $A$ and $B$ are propositions,
  $A \land B, A \lor B, A \Rightarrow B, \bot, \forall x. A, \exists x. B$ are propositions.
Examples

**Arithmetic**
Function symbols: $0, S, +, \times$
Predicate symbol: $=$

**Set Theory**
Predicate symbols: $\in, =$
A theory is:

- A language (functions + predicate symbols)
- A set of axioms (propositions of the language)

Axioms of arithmetic:

\[
\begin{align*}
\forall x, \ 0 + x &= x \\
\forall x, \ y, \ S(x) + y &= S(x + y) \\
\forall x, \ 0 \times x &= 0 \\
\forall x, \ y, \ S(x) \times y &= y + x \times y \\
\forall x, \neg (0 = S(x)) \\
\forall x, \ y, \ S(x) = S(y) \Rightarrow x = y \\
\end{align*}
\]

\[
P(0) \land (\forall x, \ P(x) \Rightarrow P(S(x)))) \Rightarrow \forall x, \ P(x).
\]

\[
\begin{align*}
\forall x, \ x &= x \\
\forall x, \ y, \ P(x) \land x &= y \Rightarrow P(y).
\end{align*}
\]
Truth : natural deduction

\( \Gamma \) set of propositions
\( \Gamma \vdash A \)  \( A \) is provable unde hypothesises+axioms \( \Gamma \)

\[
\begin{align*}
\Gamma \vdash A & \quad \left( A x \right) \\
\frac{A \in \Gamma}{\Gamma \vdash A} & \\
\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \land B} & \left( \land-\text{I} \right) \\
\frac{\Gamma \vdash A \land B}{\Gamma \vdash A} & \left( \land-\text{E}_1 \right) \\
\frac{\Gamma \vdash A \land B}{\Gamma \vdash B} & \left( \land-\text{E}_2 \right) \\
\frac{\Gamma \vdash A}{\Gamma \vdash A \lor B} & \left( \lor-\text{I}_1 \right) \\
\frac{\Gamma \vdash B}{\Gamma \vdash A \lor B} & \left( \lor-\text{I}_2 \right) \\
\frac{\Gamma \vdash A \lor B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} & \left( \lor-\text{E} \right) \\
\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} & \left( \Rightarrow-\text{I} \right) \\
\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} & \left( \Rightarrow-\text{E} \right)
\end{align*}
\]
\[\Gamma \vdash A \quad (\forall-I) \quad \text{if } x \text{ not free in } \Gamma\]

\[\Gamma \vdash \forall x. A \quad (forall-E)\]

\[\Gamma \vdash A[x \backslash t] \quad (\forall-E)\]

\[\Gamma \vdash A[x \backslash t] \quad (\exists-I)\]

\[\Gamma \vdash \exists x. A \quad (\exists-E) \quad \text{if } x \text{ not free in } \Gamma, B\]
$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A} \quad (\bot\text{-E})$$

(this gives intuitionistic logic)

$$\frac{\Gamma \vdash A \lor \neg A}{(EM)}$$

(this gives classical logic)
Relating correctness and truth: models and semantics

A set $\mathcal{U}$ (universe)
For every $f$ of arity $n$, a function $|f| : \mathcal{U}^n \rightarrow \mathcal{U}$
For every $P$ of arity $n$, a function $|P| : \mathcal{U}^n \rightarrow \{0, 1\}$ (equivalently $|P| \subset \mathcal{P}(\mathcal{U}^n)$)
Given any $\mathcal{I}$ mapping variables $x$ to $\mathcal{U}$ we define $|t|_{\mathcal{I}} \in \mathcal{U}$ by :

$\begin{align*}
|x|_{\mathcal{I}} & \equiv \mathcal{I}(x) \\
|f(t_1, \ldots, t_n)|_{\mathcal{I}} & \equiv |f|(|t_1|_{\mathcal{I}}, \ldots |t_n|_{\mathcal{I}})
\end{align*}$

Given any $\mathcal{I}$ we define $|A| \in \{0, 1\}$ by :

$\begin{align*}
P(t_1, \ldots, t_n)|_{\mathcal{I}} & \equiv |P|(|t_1|_{\mathcal{I}}, \ldots |t_n|_{\mathcal{I}}) \\
|A \land B|_{\mathcal{I}} & \equiv |A|_{\mathcal{I}} \land |B|_{\mathcal{I}} \\
& \text{similar for } \lor, \Rightarrow, \bot, \ldots \\
|\forall x. A|_{\mathcal{I}} & \equiv \min_{\alpha \in \mathcal{U}} |A|_{\mathcal{I}; x \leftarrow \alpha} \\
|\exists x. A|_{\mathcal{I}} & \equiv \max_{\alpha \in \mathcal{U}} |A|_{\mathcal{I}; x \leftarrow \alpha} \text{ (this is very much classical logic)}
\end{align*}$
Model of a theory

A model is a triple: \( \mathcal{U} \), interpretation of \( f \)s, interpretation of \( P \)s. It is a model of a theory \( \mathcal{T} \) if for any \( A \in \mathcal{T} \), \( |A|_I = 1 \) (for any \( I \) since \( A \) is closed)

**Correctness**: If \( \Gamma \vdash A \), and \( \forall B \in \Gamma, |B|_I = 1 \), then \( |A|_I = 1 \).
proof: quite straightforward (good exercise)

**Coherence**: There is no proof of \( \mathcal{T} \vdash \bot \) (easy consequence of correctness)

**Completeness**: If for any model validating \( \Gamma \), \( |A|_I = 1 \), then \( \Gamma \vdash A \) is provable.
proof: more difficult (Gödel’s PhD)

- Relates correctness with truth
- incompleteness: limit of « truth » in math
An extension of first-order logic

*Deduction modulo*: we add rewrite rules to the language

\[
\begin{align*}
0 + x & \triangleright x \\
S(x) + y & \triangleright S(x + y) \\
O \times x & \triangleright 0 \\
S(x) \times y & \triangleright y + x \times y
\end{align*}
\]

we allow reasoning modulo the rewrite rules :

\[
\begin{array}{c}
\Gamma \vdash \phi \\
\hline
\Gamma \vdash \psi \text{ if } \phi =_R \psi
\end{array}
\]

How to prove \(2 + 2 = 4\) ?
Replacing more axioms by rewrite rules

How to ensure $0 \neq 1$?

$$\forall x. 0 \neq S(x)$$

Add a new predicate symbol EQZ

$$\begin{align*}
\text{EQZ}(0) & \triangleright \top \\
\text{EQZ}(S(x)) & \triangleright \bot
\end{align*}$$

Exercise: finish the proof

Important: avoiding messy rewrite rules ($A \land B \triangleright \bot \ldots$)
Replacing more axioms by rewrite rules (2)

How to ensure $\forall x. \forall y. S(x) = S(y) \Rightarrow x = y$?
(injectivity of $S$)
Add a new function symbol $\text{pred}$

\[
\begin{align*}
\text{pred}(S(x)) & \triangleright x \\
\text{pred}(0) & \triangleright 0 \quad \text{(or whatever)}
\end{align*}
\]

Exercise: finish the proof
A “simple” presentation of Arithmetic

Rules:

\[ 0 + x \triangleright x \]
\[ S(x) + y \triangleright S(x + y) \]
\[ O \times x \triangleright 0 \]
\[ S(x) \times y \triangleright y + x \times y \]
\[ \text{EQZ}(0) \triangleright \top \]
\[ \text{EQZ}(S(x)) \triangleright \bot \]
\[ \text{pred}(S(x)) \triangleright x \]
\[ \text{pred}(0) \triangleright 0 \]

Axioms:

\[ \forall x. x = x \]
\[ \forall x. \forall y. x = y \land P(x) \Rightarrow P(y) \]
\[ P(0) \land (\forall x. P(x) \Rightarrow P(S(x))) \Rightarrow \forall y. P(y) \]
Cuts in proofs

Another form of dynamics / computation / transformation in proofs

What is a cut?

1. Prove $\forall a. \forall b. (a + b)^2 = a^2 + b^2 + 2ab$ (ends with $\forall$-intro)
2. Deduces $\forall b. (3 + b)^2 = 9 + b^2 + 6b$ (use $\forall$-elim)

We could have proved (2) directly (following the same scheme as 1)
Logical Cut

An introduction rule followed by the corresponding elimination rule

\[ \begin{align*}
\sigma_1 & \quad \sigma_2 \\
\Gamma \vdash A & \quad \Gamma \vdash B \\
\hline
\Gamma \vdash A \land B & \quad \land\text{-i} \\
\hline
\Gamma \vdash A & \quad \land\text{-e1}
\end{align*} \]

Simplifies to:

\[ \sigma_1 \]

\[ \Gamma \vdash A \]

exercise: find the simplification for the other logical cuts
Cut Elimination

- Does this process terminate?
- If we have a proof of $\Gamma \vdash A$, can we find a cut-free proof?

Termination: a major point of this course
Cut-free proofs

Why does it matter to us?

In a cut-free proof, there are only axiom rules above elimination rules (or the EM)

If a proof is cut-free, without axiom and constructive, it ends with an introduction rule.

A proof of $\vdash A \vee B$ that is constructive and cut-free ends with $\vee - i1$ of $\vee - i2$.

A proof of $\vdash \exists x. A(x)$ that is constructive and cut-free contains a \textit{witness}.
Lemma: a cut free derivation (proof) of \[\vdash A\] always ends with an introduction rule.

Proof: by induction over the derivation (could be the length of the derivation, but not necessary).

Let us do a few cases.
Why "natural" deduction?

The ND rules aim at corresponding to actual (human) deduction steps.

Indeed:

Coq’s formalism includes / extends first-order logic with some rewrite/computation rules.

Proofs are built top-down (goal-driven) and basic tactics correspond to ND rules.

OK, now we can either:

➤ code
➤ stop
➤ play with a newer prototype

Next week: cuts and constructivity in Heyting Arithmetic