Proofs in theories
Why do proofs matter to computer scientists?

Church’s theorem: undecidability of provability (1936)

Proofs and algorithms are two completely different things

Method to judge a proposition true: build a proof
Algorithms can only be used for very specific decidable problems

But...
1. Computers are truth judgment machines

The 100th decimal of $\pi$ is a 9
2. Proof-checking and proof-search algorithms

Provability undecidable
But correctness of proof decidable: proof-checking algorithms
and provability semi-decidable: proof-search semi-algorithms
3. Proofs of algorithms and programs

Critical systems: transportation, energy, medicine...
A way to avoid bugs

Prove your programs correct

Programs: do, do, do... what for?
4. Constructivity and Brouwer-Heyting-Kolmogorov interpretation

Constructive proofs are algorithms

The language of (constructive) proofs is a programming language where all programs terminate
5. Theories

Proofs are not purely logical objects

Theories: arithmetic, set theory, type theory, etc.

Theories: sets of axioms, some theories algorithms
This course: proofs in theories

$2 + 2 = 4 \Rightarrow 2 + 2 = 4$

$n + 1 = p + 1 \Rightarrow n = p$

Proof theory: proofs in pure logic
Then proofs in some specific theories (Arithmetic, Simple type theory...)

Here: an arbitrary theory as long as we can
This course: proof-reduction and models

Two notions of truth: proofs, models
But (more and more) convergence

Key results in proof-theory: termination of proof-reduction
Proving termination of proof-reduction \( \simeq \) building a model
Structure of this course
(11 courses + 4 exercises sessions + 1 master class)

1, 2, 3: basic notions (proof, theory, many-valued model...)

4, 5, 6: examples of theories

7, 8: proof reduction

9, 10, 11: unified formalisms (λΠ-calculus, λΠ-calculus modulo theory, Martin-Löf type theory, the Calculus of Constructions)
Along the way: Proof-checking systems

Simple type theory: \textsc{HOL}, \textsc{HOL-light}, \textsc{Isabelle/HOL}, \textsc{PVS}

$\lambda\Pi$-calculus: \textsc{Twelf}

$\lambda\Pi$-calculus modulo theory: \textsc{Dedukti}

Martin-Löf’s type theory: \textsc{Agda}

The Calculus of constructions: \textsc{Coq}
What you are supposed to know

The notion of inductive definition

The notions of free and bound variable, alphabetic equivalence, and substitution

The syntax of (many-sorted) predicate logic

The natural deduction

The untyped and simply typed lambda-calculi

The expression of computable functions in arithmetic, in the language of rewrite rules and in the lambda-calculus
The Natural Deduction
I. The Natural Deduction Rules
The set of provable proposition

An inductive definition

\[
\begin{align*}
A \implies B & \quad A \\
\implies B & \\
\end{align*}
\]

\[
\begin{align*}
P \implies Q & \implies R \\
\implies R & \\
\end{align*}
\]

\[
\begin{align*}
\neg P & \\
\neg Q & \\
\end{align*}
\]
But not so comfortable

To prove $A \Rightarrow B$, assume $A$ and prove $B$

Do not deduce propositions but pairs formed with hypotheses and a conclusion, sequents, $\Gamma \vdash A$

\[
\frac{
\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A
}{
\Gamma \vdash B
}\]

\[
\frac{
\Gamma, A \vdash B
}{
\Gamma \vdash A \Rightarrow B
}\]

\[
\frac{
\Gamma, A \vdash A
}{
\Gamma \vdash A
}\]
An exercise

Prove $P \vdash Q \Rightarrow P$
\[
\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \land B} \quad \text{\textit{\&-intro}}
\]

\[
\frac{\Gamma \vdash A \land B}{\Gamma \vdash A} \quad \text{\textit{\&-elim}}
\]

\[
\frac{\Gamma \vdash A \land B}{\Gamma \vdash B} \quad \text{\textit{\&-elim}}
\]
The classification of the rules

These three rules mention only the connective $\land$
Most rules mention only one connective: the rules of $\land$, the rules of $\lor$, etc.
Either in the conclusion or in the premises

\[
\begin{align*}
\Gamma \vdash A & \quad \Gamma \vdash B \\
\hline
\Gamma \vdash A \land B & \quad \land\text{-intro}
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash A \land B \\
\hline
\Gamma \vdash A & \quad \land\text{-elim}
\end{align*}
\]
introduction / elimination
\[
\frac{\Gamma \vdash A}{\Gamma \vdash A \lor B} \quad \lor\text{-intro}
\]

\[
\frac{\Gamma \vdash B}{\Gamma \vdash A \lor B} \quad \lor\text{-intro}
\]

\[
\frac{\Gamma \vdash A \lor B}{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \quad \lor\text{-elim}
\]
\[ \Gamma, A \vdash B \quad \Rightarrow \text{-intro} \]

\[ \frac{\Gamma \vdash A \Rightarrow B}{\Gamma \vdash \Gamma \vdash A \quad \Gamma \vdash A}{\frac{\frac{\Gamma \vdash A \Rightarrow B}{\Gamma \vdash B}}{\Gamma \vdash B}} \Rightarrow \text{-elim} \]
$\Gamma \vdash A \quad \forall\text{-intro if } x \not\in \text{FV}(\Gamma)$

$\Gamma \vdash \forall x \ A \quad \forall\text{-elim}$

$\Gamma \vdash (t/x)A$
\[
\frac{\Gamma \vdash (t/x)A}{\Gamma \vdash \exists x A} \quad \exists\text{-intro}
\]

\[
\frac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash B}{\Gamma \vdash B} \quad \exists\text{-elim if } x \not\in FV(\Gamma, B)
\]
\[
\begin{align*}
\Gamma & \vdash \top & \text{T-intro} \\
\Gamma & \vdash \bot & \text{\bot-elim} \\
\Gamma & \vdash A & \text{\bot-elim}
\end{align*}
\]
\[ \Gamma \vdash A \text{ axiom if } A \in \Gamma \]

\[ \Gamma \vdash A \lor \neg A \text{ excluded-middle} \]
No rules for ¬ and ⇔

¬A abbreviation for $A \Rightarrow \bot$
$A \leftrightarrow B$ abbreviation for $(A \Rightarrow B) \land (B \Rightarrow A)$
Proofs

A sequent $\Gamma \vdash A$ is provable iff it has a derivation (proof)

A tree where nodes are labelled with sequents

Root labelled by $\Gamma \vdash A$

If node labelled by $\Delta \vdash B$ and children labelled by $\Sigma_1 \vdash C_1$, ..., $\Sigma_n \vdash C_n$ then a Natural deduction rule deduces $\Delta \vdash B$ from $\Sigma_1 \vdash C_1, \ldots, \Sigma_n \vdash C_n$
Proof of a proposition, proof in an axiomatic theory

A proposition $A$ is provable (without any axioms), if $\vdash A$ is

Axiomatic theory $\mathcal{T}$: set of closed propositions (axioms)
$A$ provable in $\mathcal{T}$ if finite subset $\Gamma$ of $\mathcal{T}$, $\Gamma \vdash A$ provable
II. Constructive proofs
$0 \in P$ and $2 \not\in P$

Does there exist $n$ such that $n \in P$ and $n + 1 \not\in P$?
\[ P(0), \neg P(S(S(0))) \vdash \exists x \ (P(x) \land \neg P(S(x))) \]

where \( \pi_1 \)

\[
\begin{align*}
&\frac{\Gamma, P(S(0)) \vdash P(S(0)) \quad \Gamma, P(S(0)) \vdash \neg P(S(S(0)))}{\Gamma, P(S(0)) \vdash P(S(0)) \land \neg P(S(S(0)))} \\
&\frac{\Gamma, P(S(0)) \vdash \exists x \ (P(x) \land \neg P(S(x)))}{\Gamma, P(S(0)) \vdash \exists x \ (P(x) \land \neg P(S(x)))}
\end{align*}
\]

where \( \Gamma = \{ P(0), \neg P(S(S(0))) \} \)
\[
\pi_2
\]

\[
\begin{array}{c}
\Gamma, \neg P(S(0)) \vdash P(0) \\
\hline
\Gamma, \neg P(S(0)) \vdash \neg P(S(0)) \\
\hline
\Gamma, \neg P(S(0)) \vdash P(0) \land \neg P(S(0)) \\
\hline
\Gamma, \neg P(S(0)) \vdash \exists x \left( P(x) \land \neg P(S(x)) \right)
\end{array}
\]

Finally

\[
\begin{array}{c}
\Gamma \vdash P(S(0)) \lor \neg P(S(0)) \\
\hline
\Gamma, P(S(0)) \vdash A \\
\hline
\Gamma, \neg P(S(0)) \vdash A
\end{array}
\]

\[
\begin{array}{c}
\pi_1 \\
\pi_2
\end{array}
\]

\[
\Gamma \vdash A
\]

where \( A = \exists x \left( P(x) \land \neg P(S(x)) \right) \)
We can prove
\[ \exists x \ (P(x) \land \neg P(x)) \]

Can we prove
\[ P(n) \land \neg P(S(n)) \]
for some natural number \( n \)?

No: easy to prove that for each number \( n \)
\[ P(0), \neg P(S(S(0))) \vdash P(n) \land \neg P(S(n)) \]
not provable
Without any axioms

We can prove

$$\exists x \ (P(0) \Rightarrow \neg P(S(S(0)))) \Rightarrow (P(x) \land \neg P(S(x))))$$

We can prove

$$P(0) \Rightarrow \neg P(S(S(0))) \Rightarrow (P(n) \land \neg P(S(n)))$$

for no natural number $n$
The notion of witness

$E$ has the witness property if
when $\exists x \ A$ is in $E$, there exists $t$ such that $(t/x)A$ is in $E$

The set of provable propositions: no witness property
How is this possible?

Only one possibility to prove $\exists x \ A$: prove $(t/x)A$ and then use the $\exists$-intro rule.

Example $\pi_1$ and $\pi_2$
Then a proof by case

$\pi_1$

\[
\frac{\pi_1}{\Gamma, P(S(0)) \vdash A}
\]

$\pi_2$

\[
\frac{\pi_2}{\Gamma, \neg P(S(0)) \vdash A}
\]

$\Gamma \vdash A$

0 or $S(0)$?
But still needs to prove $P(S(0)) \lor \neg P(S(0))$

The excluded-middle rule

$(A \lor \neg A)$ without knowing which of $A$ or $\neg A$ holds
The notion of constructive proof

A proof that does not use the excluded-middle rule

As we shall see: if a proposition $\exists x \ A$ has a constructive proof, without any axioms, then there exists a term $t$ such that $(t/x)A$ has a proof

Algorithm to extract witness from proof: proof reduction

Extends to many theories
A constructive proof $\pi$ of

$$\forall x \exists y \ (x = 2 \times y \lor x = 2 \times y + 1)$$

A proof of the proposition

$$\exists y \ (25 = 2 \times y \lor 25 = 2 \times y + 1)$$

Extract a witness from this proof
By construction, correct with respect to specification

$$x = 2 \times y \lor x = 2 \times y + 1$$
III. Cuts and proof reduction
Cuts

A proof ending with an elimination rule whose main premise is proved by an introduction rule on the same symbol. For instance:

\[
\begin{align*}
\pi & \quad \pi' \\
\Gamma \vdash A & \quad \Gamma \vdash B \\
\Gamma \vdash A \land B & \quad \land\text{-intro} \\
\Gamma \vdash A & \quad \land\text{-elim}
\end{align*}
\]
Seven cases

\[
\pi \\
\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow\text{-intro} \quad \pi' \\
\frac{\Gamma \vdash A}{\Gamma \vdash B} \Rightarrow\text{-elim}
\]
Proof reduction

Contains a cut: a sub-tree of the proof is a cut

Proof reduction: replace this sub-tree with another

\[ \frac{\pi}{\Gamma \vdash A} \quad \frac{\pi'}{\Gamma \vdash B} \quad \frac{\Gamma \vdash A \land B}{\Gamma \vdash A} \quad \land\text{-intro} \quad \land\text{-elim} \]
Eliminating a cut is easy
Eliminating a cut may create others: termination?

Technically: a major topic of this course
Why do we care?

**Cut-free:** contains no cut

A proof $\pi$ that is (1.) constructive, (2.) cut-free, and (3.) without any axioms **ends with an introduction rule.**

A proof $\pi$ of $\exists x A$ that is (1.) constructive, (2.) cut-free, and (3.) without any axioms ends with a $\exists$-intro rule: **witness property**
After the break

The notion of theory