

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 π 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

A way to avoid bugs

Prove your programs correct

Critical systems: transportation, energy, medicine, ...

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 approaches to logic: 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 (16 weeks)

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

4, 5, 6: examples of theories

8, 9: proof reduction

10, 11, 12: unified formalisms ($\lambda\Pi$, $\lambda\Pi$ -modulo, Martin-Löf type theory, the Calculus of Constructions)

Along the way: Proof-checking systems

Simple type theory: **HOL**, **HOL-light**, **Isabelle/HOL**, **PVS**

$\lambda\Pi$: **Twelf**

$\lambda\Pi$ -modulo: **Dedukti**

Martin-Löf's type theory: **Agda**

The Calculus of constructions: **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

$$\frac{A \Rightarrow B \quad A}{B}$$

$$\overline{P \Rightarrow Q \Rightarrow R}$$

$$\overline{P}$$

$$\overline{Q}$$

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, $\Gamma \vdash A$

$$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$$

An exercise

Prove $P \vdash Q \Rightarrow P$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-intro}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-elim}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-elim}$$

The classification of the rules

These three rules mention only the connective \wedge

Most rules mention only one connective: the rules of \wedge , the rules of \vee , etc.

Either in the conclusion or in the premises

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-intro}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-elim}$$

introduction / elimination

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee\text{-intro}$$

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee\text{-intro}$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee\text{-elim}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow\text{-intro}$$

$$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \Rightarrow\text{-elim}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x A} \quad \forall\text{-intro if } x \notin FV(\Gamma)$$

$$\frac{\Gamma \vdash \forall x A}{\Gamma \vdash (t/x)A} \quad \forall\text{-elim}$$

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

$$\frac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash B}{\Gamma \vdash B} \exists\text{-elim if } x \notin FV(\Gamma, B)$$

$$\frac{}{\Gamma \vdash \top} \top\text{-intro}$$

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} \perp\text{-elim}$$

$\overline{\Gamma \vdash A}$ axiom if $A \in \Gamma$

$\overline{\Gamma \vdash A \vee \neg A}$ excluded-middle

\neg, \Leftrightarrow

No rules for \neg and \Leftrightarrow

$\neg A$ abbreviation for $A \Rightarrow \perp$

$A \Leftrightarrow B$ abbreviation for $(A \Rightarrow B) \wedge (B \Rightarrow A)$

Proofs

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

A tree where nodes are labelled by sequents

Root labelled by $\Gamma \vdash A$

If node labelled by $\Delta \vdash B$ and children labelled by $\Sigma_1 \vdash C_1, \dots, \Sigma_n \vdash C_n$ then a Natural deduction rule deduces $\Delta \vdash B$ from $\Sigma_1 \vdash C_1, \dots, \Sigma_n \vdash C_n$

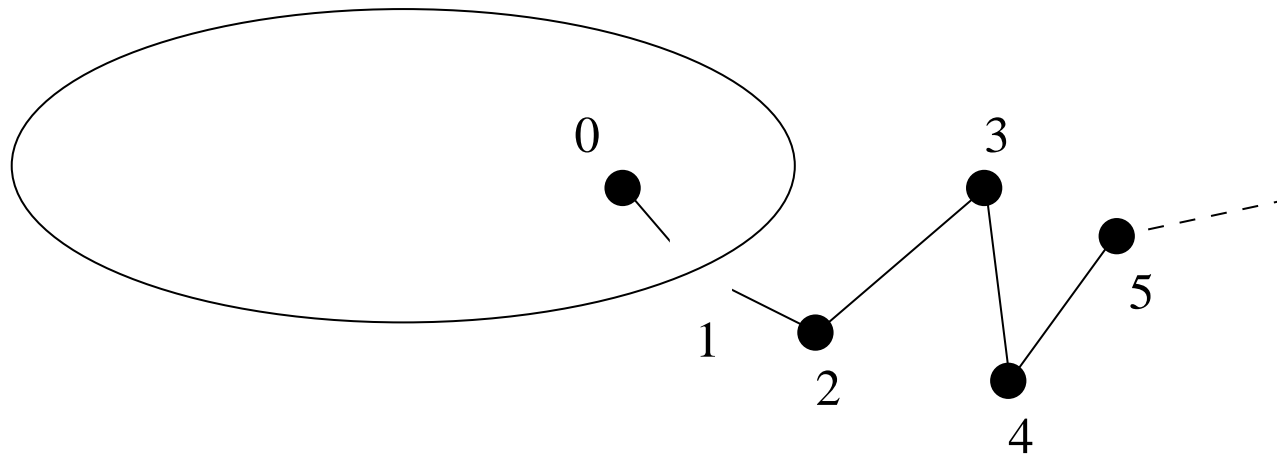
Proof of a proposition, proof in an axiomatic theory

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 Γ of \mathcal{T} , $\Gamma \vdash A$ provable

II. Constructive proofs



$0 \in P$ and $2 \notin P$

Does there exists n such that $n \in P$ and $n + 1 \notin P$?

$$P(0), \neg P(S(S(0))) \vdash \exists x (P(x) \wedge \neg P(S(x)))$$

π_1

$$\frac{\frac{\overline{\Gamma, P(S(0)) \vdash P(S(0))} \quad \overline{\Gamma, P(S(0)) \vdash \neg P(S(S(0)))}}{\Gamma, P(S(0)) \vdash P(S(0)) \wedge \neg P(S(S(0)))}}{\Gamma, P(S(0)) \vdash \exists x (P(x) \wedge \neg P(S(x)))}$$

where $\Gamma = \{P(0), \neg P(S(S(0)))\}$

π_2

$$\frac{\frac{\frac{\Gamma, \neg P(S(0)) \vdash P(0)}{\Gamma, \neg P(S(0)) \vdash P(0) \wedge \neg P(S(0))} \quad \frac{\Gamma, \neg P(S(0)) \vdash \neg P(S(0))}{\Gamma, \neg P(S(0)) \vdash \neg P(S(0))}}{\Gamma, \neg P(S(0)) \vdash \exists x (P(x) \wedge \neg P(S(x)))}$$

Finally

$$\frac{\Gamma \vdash P(S(0)) \vee \neg P(S(0)) \quad \frac{\pi_1}{\Gamma, P(S(0)) \vdash A} \quad \frac{\pi_2}{\Gamma, \neg P(S(0)) \vdash A}}{\Gamma \vdash A}$$

where $A = \exists x (P(x) \wedge \neg P(S(x)))$

We can prove

$$\exists x (P(x) \wedge \neg P(x))$$

Can we prove

$$P(n) \wedge \neg P(S(n))$$

for some natural number n ?

No: easy to prove that for each number n

$$P(0), \neg P(S(S(0))) \vdash P(n) \wedge \neg P(S(n))$$

not provable

Without any axioms

We can prove

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

We can prove

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

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 π_1 and π_2

Then a proof by case

$$\frac{\dots \quad \frac{\pi_1}{\Gamma, P(S(0)) \vdash A} \quad \frac{\pi_2}{\Gamma, \neg P(S(0)) \vdash A}}{\Gamma \vdash A}$$

0 or $S(0)$?

But still needs to prove $P(S(0)) \vee \neg P(S(0))$

The excluded-middle rule

$(A \vee \neg A)$ 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

Programming with proofs

A constructive proof π of

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

A proof of the proposition

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

Extract a witness from this proof

By construction, correct with respect to specification

$$x = 2 \times y \vee x = 2 \times y + 1$$

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

$$\frac{\frac{\frac{\pi}{\Gamma \vdash A} \quad \frac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B} \wedge\text{-intro}}{\Gamma \vdash A} \wedge\text{-elim}$$

Seven cases

$$\frac{\frac{\frac{\pi}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B} \Rightarrow\text{-intro} \quad \frac{\pi'}{\Gamma \vdash A}}{\Gamma \vdash B} \Rightarrow\text{-elim}$$

Proof reduction

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

Proof reduction: replace this sub-tree by another

$$\frac{\frac{\pi}{\Gamma \vdash A} \quad \frac{\pi'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B} \wedge\text{-intro}$$
$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-elim}$$

$$\frac{\frac{\frac{\pi}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B} \Rightarrow\text{-intro} \quad \frac{\pi'}{\Gamma \vdash A}}{\Gamma \vdash B} \Rightarrow\text{-elim}$$

Eliminating a cut is easy

Eliminating a cut may create others: termination?

Technically: one major topic of this course

Why do we care?

Cut free: contains no cut

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

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

Next time

The notion of theory