The termination of proof reduction
0. What we have seen so far
Proofs, constructive proof, theory, arithmetic

Simply typed lambda-calculus and its termination
I. Cuts and proof reduction
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

\[
\begin{align*}
\pi & \quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow\text{intro} \\
\pi' & \quad \frac{\Gamma \vdash A}{\Gamma \vdash B} \Rightarrow\text{elim}
\end{align*}
\]
Proof reduction

Contains a cut: a sub-tree of the proof is a cut
Proof reduction: replace this sub-tree with another

\[
\begin{align*}
\pi & \quad \pi' \\
\Gamma \vdash A & \quad \Gamma \vdash B \\
\Gamma \vdash A \land B & \quad \land\text{-intro} \\
\Gamma \vdash A & \quad \land\text{-elim}
\end{align*}
\]
Eliminating a cut is easy
Eliminating a cut may create others: termination?
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
II. Proof-terms
Notations for derivation trees

Inductive definition: smallest set closed by some functions
Example: $E$: smallest set containing $z = 0$ and closed by $f = x \mapsto x + 2$
$n$ in $E$ if and only is there exists a derivation (tree) of $E$

\[
\begin{array}{c}
\overline{0} \\
\overline{2} \\
\overline{4} \\
\overline{6} \\
\end{array}
\begin{array}{c}
\overline{z} \\
\overline{f} \\
\overline{f} \\
\overline{f} \\
\end{array}
\begin{array}{c}
\overline{0} \\
\overline{2} \\
\overline{4} \\
\overline{6} \\
\end{array}
\begin{array}{c}
\overline{z} \\
\overline{f} \\
\overline{f} \\
\overline{f} \\
\end{array}
\]
\[
\begin{array}{c}
\vdash T \quad \text{T-intro} \quad \vdash T \quad \text{T-intro} \\
\hline
\vdash T \land T \quad \text{\land-intro}
\end{array}
\]

Redundant: rule names only

\[
\begin{array}{c}
\text{T-intro} \quad \text{T-intro} \\
\hline
\text{\land-intro}
\end{array}
\]

Linear notation for trees: \(\text{\land-intro}(\text{T-intro}, \text{T-intro})\)
Shorthand for rule names: \(\langle I, I \rangle\)
The axiom rule

Natural deduction rules: functions from sequents to sequents
For each sequence of propositions $A_1, \ldots, A_n$ and each $A_i$: a different axiom rule
Name of axiom rule parametrized by $A_1, \ldots, A_n$ and $A_i$

\[
\begin{array}{c}
\text{axiom} \quad \text{axiom} \\
\wedge\text{-intro} \\
\end{array}
\quad
\begin{array}{c}
\text{axiom}_{P, Q \vdash P} \\
\wedge\text{-intro} \\
\end{array}
\quad
\begin{array}{c}
\text{axiom}_{P, Q \vdash Q} \\
\wedge\text{-intro} \\
\end{array}
\]
In a sequent: conclusion more important than context
Natural deduction rules: deduce propositions from propositions and context recalls which propositions can be used in axiom rule
Name hypotheses: $P, Q$ becomes $\alpha : P, \beta : Q$ and use these names as name of the axiom rule

\[
\begin{array}{c}
\alpha \\
\beta \\
\hline
\wedge \text{-intro}
\end{array}
\]

$\langle \alpha, \beta \rangle$
Some rules extend context: e.g.

\[
\frac{\pi}{A_1, \ldots, A_n, B \vdash C} \quad \Rightarrow\text{-intro}
\]

\(\lambda\) shorthand for \(\Rightarrow\text{-intro}\): not \(\lambda\pi\) or \(\lambda B \pi\) but name added hypothesis \(\lambda\beta : B \pi\)

\(\pi\) proof in context \(\alpha_1 : A_1, \ldots, \alpha_n : A_n, \beta : B\) and \(\lambda\beta : B \pi\) proof in context \(\alpha_1 : A_1, \ldots, \alpha_n : A_n\)

Hypotheses names like variables: \(\beta\) introduced by \(\lambda\), can be used in \(\pi\), not elsewhere: bound by \(\lambda\), scope \(\pi\)
Replacing an hypothesis

From \( \pi \) proof of \( \Gamma, A \vdash B \), remove the hypothesis \( A \) in all sequents, replace the axiom rules on this proposition by \( \pi' \) of \( \Gamma \vdash A \)

Substitute \( \pi' \) for \( \alpha \) (associated to \( A \)) in \( \pi \)
A proof of a sequent $A_1, ..., A_n \vdash B$ expressed as a term in the context $\alpha_1 : A_1, ..., \alpha_n : A_n$

$\Gamma \vdash A_i$ axiom

expressed as $\alpha_i$
\[
\frac{\pi}{\Gamma \vdash A} \quad \frac{\pi'}{\Gamma \vdash B} \quad \text{\land\text{-intro}}
\]
expressed as \(\langle \pi, \pi' \rangle\)

\[
\frac{\pi}{\Gamma \vdash A \land B} \quad \text{\land\text{-elim}}
\]
expressed as \(\text{fst}(\pi)\)

\[
\frac{\pi}{\Gamma \vdash A \land B} \quad \text{\land\text{-elim}}
\]
expressed as \(\text{snd}(\pi)\)
\[
\frac{\pi}{\Gamma, A \vdash B} \quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \quad \Rightarrow\text{-intro}
\]

expressed as \( \lambda \alpha : A \pi \)

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

expressed as \( \text{app}(\pi, \pi') \) also written \( (\pi \pi') \)

...
Proof-reduction on terms

\[
\begin{align*}
\frac{\pi_1}{\Gamma, A \vdash B} & \quad \Rightarrow\text{-intro} \\
\frac{\Gamma \vdash A \Rightarrow B}{\Gamma \vdash B} & \quad \Rightarrow\text{-elim} \\
\frac{\pi_2}{\Gamma \vdash A}
\end{align*}
\]

\((\lambda\alpha : A \, \pi_1) \, \pi_2)\) reduces to \((\pi_2/\alpha)\pi_1\)

\[((\lambda\alpha : A \, \pi_1) \, \pi_2) \rightarrow (\pi_2/\alpha)\pi_1\]

\[\text{fst}(\langle \pi_1, \pi_2 \rangle) \rightarrow \pi_1\]

\[\text{snd}(\langle \pi_1, \pi_2 \rangle) \rightarrow \pi_2\]
III. The Brouwer-Heyting-Kolmogorov interpretation
So far just changing notations: derivations labeled by rule names, a symbol for each rule, from sequents to propositions (variables)

Brouwer-Heyting-Kolmogorov interpretation: a completely different approach with same result
How do you build a proof of $A \land B$?
$\land$-intro rule: build a proof of $A$ and a proof of $B$

How do you use a proof of $A \land B$?
$\land$-elim rules: to build a proof of $A$ or a proof of $B$
How do you build an ordered pair formed with a proof of $A$ and a proof of $B$?

build a proof of $A$ and a proof of $B$

How do you use an ordered pair formed with a proof of $A$ and a proof of $B$?

to build a proof of $A$ or a proof of $B$
A proof of $A \land B$ **built** and **used** like an ordered pair formed with a proof of $A$ and a proof of $B$

A proof of $A \land B$ is an ordered pair formed with a proof of $A$ and a proof of $B$

A proof of $A \Rightarrow B$ is an algorithm mapping proofs of $A$ to proofs of $B$

$\langle \pi, \pi' \rangle$, $\lambda x \pi$
and also

- a proof of $\top$ is always the same object
- a proof of $\bot$, there is none
- a proof of $A \lor B$ is either a proof of $A$ or a proof of $B$
- a proof of $\forall x \ A$ is an algorithm mapping objects $t$ to proofs of $(t/x)A$
- a proof of $\exists x \ A$ is an ordered pair formed with an object $t$ and a proof of $(t/x)A$
IV. The Curry-de Bruijn-Howard correspondence
Types for proof-terms
\( \Phi(A) \) type of the proofs of \( A \)
Proof of \( A \Rightarrow B \): algorithm mapping proofs of \( A \) to proofs of \( B \)

\[ \Phi(A \Rightarrow B) = \Phi(A) \to \Phi(B) \]

\( \Phi \) isomorphism between propositions and types: the Curry-de Bruijn-Howard correspondence
Identify isomorphic object

\( \lambda \alpha : A \alpha \) has type \( A \Rightarrow A \)
\( \lambda \alpha : A \alpha \) is a proof of \( A \Rightarrow A \)
\[ \alpha_1 : A_1, \ldots, \alpha_n : A_n \vdash \pi : B \]

\[ \pi \text{ is a proof of the sequent } A_1, \ldots, A_n \vdash B \]

\[ (\alpha_1, \ldots, \alpha_n \text{ names given to the variables of standing for proofs of the propositions } A_1, \ldots, A_n) \]
Natural deduction rules turned into typing rules

\[
\Gamma \vdash \alpha : A \quad \text{axiom if } \alpha : A \in \Gamma
\]

\[
\frac{\Gamma \vdash \pi : A \quad \Gamma \vdash \pi' : B}{\Gamma \vdash \langle \pi, \pi' \rangle : A \land B} \quad \land\text{-intro}
\]

\[
\frac{\Gamma \vdash \pi : A \land B}{\Gamma \vdash \text{fst}(\pi) : A} \quad \land\text{-elim}
\]

\[
\frac{\Gamma \vdash \pi : A \land B}{\Gamma \vdash \text{snd}(\pi) : B} \quad \land\text{-elim}
\]
\[
\Gamma, \alpha : A \vdash \pi : B
\]
\[
\frac{\Gamma \vdash \lambda \alpha : A \pi : A \Rightarrow B}{\Gamma \vdash \pi : A \Rightarrow B \Rightarrow \text{-intro}}
\]
\[
\Gamma \vdash \pi : A \Rightarrow B \quad \Gamma \vdash \pi' : A
\]
\[
\frac{\Gamma \vdash (\pi \pi') : B}{\Rightarrow \text{-elim}}
\]
\[
\Gamma \vdash \pi : A
\]
\[
\frac{\Gamma \vdash \lambda x \pi : \forall x A}{\Rightarrow \text{-intro if } x \notin FV(\Gamma)}
\]
\[
\Gamma \vdash \pi : \forall x A
\]
\[
\frac{\Gamma \vdash (\pi \ t) : (t/x)A}{\Rightarrow \text{-elim}}
\]
A_1, \ldots, A_n \vdash B \text{ is derivable in Natural deduction if and only if}

there exists a proof-term \( \pi \) such that \( \alpha_1 : A_1, \ldots, \alpha_n : A_n \vdash \pi : B \)

is derivable in this system
Final rule

\[ \pi \] a closed and irreducible proof-term of type \( A \)
then it is an introduction, i.e. a term of the form
\[ I, \langle \pi_1, \pi_2 \rangle, i(\pi_1), j(\pi_1), \lambda \alpha : B \pi_1, \lambda x \pi_1, \text{ or } \langle t, \pi_1 \rangle \]

Corollary: Witness property
V. The termination of proof-term reduction
Follow the termination proof of simply typed $\lambda$-calculus

Instead of $\rightarrow$: $\Rightarrow$, $\top$, $\bot$, $\land$, $\lor$, $\forall$, $\exists$
By induction over $A$ a set of proof-terms $R_A$

- If $A$ atomic, then a proof-term is an element of $R_A$ if it strongly terminates

- A proof-term is an element of $R_{A \Rightarrow B}$ if it strongly terminates and when it reduces to $\lambda \alpha : A \, \pi_1$ (introduction) then for every $\pi'$ in $R_A$, $(\pi' / \alpha) \pi_1$ is an element of $R_B$

- A proof-term is an element of $R_{A \wedge B}$ if it strongly terminates and when it reduces to $\langle \pi_1, \pi_2 \rangle$ (introduction) then $\pi_1$ and $\pi_2$ are elements of $R_A$ and $R_B$

- etc.
Easy lemmas

If $A$ proposition and $\alpha$ variable, then $\alpha \in R_A$

If $\pi$ is an element of $R_A$ and $\pi \rightarrow^* \pi'$, then $\pi'$ is an element of $R_A$

If $A$ proposition and $\pi$ proof-term that is an elimination such that all one-step reducts of $\pi$ are in $R_A$, then $\pi$ is in $R_A$
The theorem

π a proof-term of type A in a context Γ
θ a substitution mapping the term-variables to terms of the same sort
σ a substitution mapping proof-term variables bound to a proposition B in Γ to elements of \( R_B \)
Then \( \sigma \theta \pi \) is an element of \( R_A \)
By induction over the structure of $\pi$

- **axiom** $\pi = \alpha$, $\sigma\theta\alpha = \sigma\alpha$ in $R_A$
\[ \Rightarrow \text{-intro } A = B \Rightarrow C \]

\[ \pi = \lambda \alpha : B \ \rho \text{ where } \rho \text{ proof-term of type } C \]

\[ \sigma \theta \pi = \lambda \alpha : \theta B \ \sigma \theta \rho \]

By induction hypothesis, \( \sigma \theta \rho \in R_C \)

Reduction sequence issued from \( \sigma \theta \pi \) reduces \( \sigma \theta \rho \), finite

\[ \lambda \alpha : \theta B \ \rho' \text{ reduct of } \sigma \theta \pi : \rho' \text{ reduct of } \sigma \theta \rho \]

\( \tau \) any proof-term of \( R_B \), \((\tau/\alpha)\rho' \) reduct of \( ((\tau/\alpha) \circ \sigma) \theta \rho \)

By induction hypothesis \(( (\tau/\alpha) \circ \sigma ) \theta \rho \) in \( R_C \)

Thus \(( (\tau/\alpha) \rho' \) \in \( R_C \)
\( \land\text{-intro} \ A = B \land C \)

\( \pi = \langle \rho_1, \rho_2 \rangle \) where \( \rho_1 \) of type \( B \) and \( \rho_2 \) of type \( C \)

\( \sigma\theta\pi = \langle \sigma\theta\rho_1, \sigma\theta\rho_2 \rangle \)

By induction hypothesis, \( \sigma\theta\rho_1 \in R_B \) and \( \sigma\theta\rho_2 \in R_C \)

Reduction sequence issued from \( \sigma\theta\pi \) reduces \( \sigma\theta\rho_1 \) and \( \sigma\theta\rho_2 \), finite

\( \langle \rho'_1, \rho'_2 \rangle \) reduct of \( \sigma\theta\pi \): \( \rho'_1 \) is reduct of \( \sigma\theta\rho_1 \) and \( \rho'_2 \) of \( \sigma\theta\rho_2 \)

\( \rho'_1 \in R_B \) and \( \rho'_2 \in R_C \)
\[ \Rightarrow\text{-elim} \]

\[ \pi = (\rho_1 \rho_2), \text{ where } \rho_1 \text{ of type } B \Rightarrow A \text{ and } \rho_2 \text{ of type } B \]

\[ \sigma \theta \pi = (\sigma \theta \rho_1 \sigma \theta \rho_2) \]

By induction hypothesis \( \sigma \theta \rho_1 \in R_{B \Rightarrow A} \) and \( \sigma \theta \rho_2 \in R_B \)

Termination: \( n \) (\( n' \)) max length seq. issued \( \sigma \theta \rho_1 \) (\( \sigma \theta \rho_2 \))

By induction on \( n + n' \), \( (\sigma \theta \rho_1 \sigma \theta \rho_2) \in R_A \)

Only need to prove every of its one step reducts is in \( R_A \)

If reduction in \( \sigma \theta \rho_1 \) or in \( \sigma \theta \rho_2 \) then induction hypothesis

Otherwise \( \sigma \theta \rho_1 = \lambda \alpha \rho' \) reduct is \( (\sigma \theta \rho_2/\alpha)\rho' \)

By definition of \( R_{B \Rightarrow A} \) is in \( R_A \)
\(\text{\&-elim}\)

\[ \pi = \text{fst}(\rho) \text{ where } \rho \text{ of type } A \land B \]

\[ \sigma \theta \pi = \text{fst}(\sigma \theta \rho) \]

By induction hypothesis \(\sigma \theta \rho \in R_{A \land B}\)

Termination: \(n\) max length seq. issued \(\sigma \theta \rho \in R_{A \land B}\)

By induction on \(n, \text{fst}(\sigma \theta \rho)\) in \(R_A\)

Only need to prove every of its one step reducts is in \(R_A\)

If reduction in \(\sigma \theta \rho\) then induction hypothesis

Otherwise \(\sigma \theta \rho = \langle \rho'_1, \rho'_2 \rangle\) reduct is \(\rho'_1\)

By definition of \(R_{A \land B}\) in \(R_A\)
Corollary

Every proof-term in Predicate logic strongly terminates

$\theta$: the substitution mapping each term variable to itself
$\sigma$: the substitution mapping each proof-term variables to itself
IV. Cuts in Deduction modulo
What is a cuts in Deduction modulo?

Same as in Predicate logic:

a proof ending with an elimination rule whose main premise is proved by an introduction rule on the same symbol
Failure of termination of proof reduction

For some theories: e.g. $P \implies (P \implies Q)$

\[
\begin{align*}
& P \vdash P \implies Q \quad \text{axiom} \\
& \quad \vdash P \implies Q \quad \text{\Rightarrow-elim} \\
& \quad \vdash P \implies Q \quad \text{\Rightarrow-intro} \\
& \quad \vdash Q \quad \text{\Rightarrow-elim}
\end{align*}
\]
An exercise

Prove that the sequent $\vdash Q$ has no cut-free proof
But when proof-reduction terminates

Cut-free proofs have the same properties than in Predicate logic.
A proof that is (1) constructive (2) cut-free and (3) in a purely computational theory ends with an introduction rule.

All (1) purely computational theories where (2) proof-reduction terminates have the witness property.
In particular

Proof reduction terminates in arithmetic
From a proof of

\[ \forall x \ (N(x) \Rightarrow \exists y \ (N(y) \land (x = 2 \times y \lor x = 2 \times y + 1))) \]

and 25 get a proof of

\[ \exists y \ (N(y) \land (25 = 2 \times y \lor 25 = 2 \times y + 1))) \]

witness: 12

\[ \forall x \ (N(x) \Rightarrow \exists y \ (N(y) \land (x = 2 \times y \lor x = 2 \times y + 1))) \]

More than simply typed lambda-calculus: all functions you can prove to exist in arithmetic
Proposition: specification = extended type of the program
Message to take home

Proofs are expressed in a (functional) programming language

The proved proposition is the type of the proof

Proof reduction is the execution mechanism of this language

A proof of $\forall x \exists y \ A$ when applied to $n$ yields a proof of $\exists y \ (n/x)A$

whose reduction (execution) yields a witness $p$ such that $(n/x, p/y)A$

More than the type, $A$ is the specification of the program
Tomorrow

Automated theorem proving