Cut elimination for infinitary proofs

Amina Doumane
LSV-IRIF-Université Paris Diderot

March 2016 - Shonan meeting

Joint work with:
David Baelde & Alexis Saurin
LSV-ENS Cachan & IRIF-Université Paris 7
Introduction
Introduction

- Inductive and coinductive definitions

A natural number is either 0 or the successor of a natural number.
Introduction

- Inductive and coinductive definitions

\[ N = 1 \oplus N \]
Introduction

- Inductive and coinductive definitions

\[ N = \mu X.1 \oplus X \]
Introduction

- Inductive and coinductive definitions

\[ N = \mu X.1 \oplus X \]

A stream is made of a natural number (head) and a stream (tail).
Introduction

- Inductive and coinductive definitions

\[ N = \mu X.1 \oplus X \]
\[ S = N \otimes S \]
Introduction

- Inductive and coinductive definitions

\[
N = \mu X. 1 \oplus X \\
S = \nu X. N \otimes X
\]
Introduction

- Inductive and coinductive definitions

\[ N = \mu X. 1 \oplus X \]
\[ S = \nu X. N \otimes X \]
Introduction

- Inductive and coinductive definitions

\[ N = \mu X. 1 \oplus X \]
\[ S = \nu X. N \otimes X \]

- Proofs-programs over these data types

\[
\begin{align*}
\text{double}(n) &= 0 & \text{if } n = 0 \\
&= \text{succ}(\text{succ}(\text{double}(m))) & \text{if } n = \text{succ}(m)
\end{align*}
\]
Introduction

- Inductive and coinductive definitions

\[
\begin{align*}
N &= \mu X. 1 \oplus X \\
S &= \nu X. N \otimes X
\end{align*}
\]

- Proofs-programs over these data types

\[
\begin{align*}
double(n) &= 0 & \text{if } n = 0 \\
&= \text{succ(succ(double(m)))} & \text{if } n = \text{succ}(m)
\end{align*}
\]

\[
\Pi_{\text{double}} = \begin{array}{c}
\frac{N \vdash N}{1 \vdash 1} \\
(1) \\
\frac{1 \vdash 1 \oplus N}{N \vdash 1 \oplus N} \\
(\oplus_1) \\
\frac{N \vdash N}{N \vdash 1 \oplus N} \\
(\mu_r) \\
\frac{N \vdash 1 \oplus N}{N \vdash N} \\
(\oplus_2) \\
\frac{1 \oplus N \vdash N}{N \vdash N} \\
(\mu_l)
\end{array}
\]
Infinitary (circular) proofs in the literature

- Verification device: Complete deduction system giving algorithms for checking validity (Tableaux, sequent calculi)

\[ \mu \text{-calculus formula} \rightarrow \text{Proof search} \]

Success $\rightarrow$ Validity

Failure $\rightarrow$ Invalidity
Infinitary (circular) proofs in the literature

- **Verification device**: Complete deduction system giving algorithms for checking validity (Tableaux, sequent calculi)

  \[
  \begin{align*}
  \text{Success} & \quad \rightarrow \quad \text{Validity} \\
  \mu\text{-calculus formula} & \quad \rightarrow \quad \text{Proof search} \\
  \downarrow & \\
  \text{Failure} & \quad \rightarrow \quad \text{Invalidity}
  \end{align*}
  \]

- **Completeness arguments**: Intermediate objects between syntax and semantics (Kozen, Kaivola, Walukiewicz)

  \[
  \begin{align*}
  \mu\text{-calculus formula} & \quad \rightarrow \quad \text{Circular proof} \quad \rightarrow \quad \text{Finite axiomatization}
  \end{align*}
  \]
Infinitary (circular) proofs in the literature

- **Verification device**: Complete deduction system giving algorithms for checking validity (Tableaux, sequent calculi)

\[
\begin{align*}
\text{Success} & \quad \rightarrow \quad \text{Validity} \\
\mu\text{-calculus formula} & \quad \rightarrow \quad \text{Proof search} \\
\text{Failure} & \quad \rightarrow \quad \text{Invalidity}
\end{align*}
\]

- **Completeness arguments**: Intermediate objects between syntax and semantics (Kozen, Kaivola, Walukiewicz)

\[
\begin{align*}
\mu\text{-calculus formula} & \quad \rightarrow \quad \text{Circular proof} \quad \rightarrow \quad \text{Finite axiomatization}
\end{align*}
\]

- But rarely as proof/programm objects in themselves
Structural proof theory

Two main properties:

- Syntactic cut-elimination
Structural proof theory

Two main properties:

- **Syntactic cut-elimination**
  - **Motivation:** At the heart of proofs-as-programms viewpoint

- **Focalization**
  - **Motivation:** Proof search strategy based on the notion of polarity
Structural proof theory

Two main properties:

- Syntaxic cut-elimination
  - **Motivation:** At the heart of proofs-as-programmes viewpoint
  - **State of art:** Semantical cut elimination (Brotherstone), Additive fragment (Fortier-Santocanale)

- Focalization
  - **Motivation:** Proof search strategy based on the notion of polarity
  - **State of art:** Nothing
Structural proof theory

Two main properties:

- Syntactic cut-elimination
  - **Motivation:** At the heart of proofs-as-programms viewpoint
  - **State of art:** Semantical cut elimination (Brotherstone), Additive fragment (Fortier-Santocanale)
  - **Contribution:** See this talk

- Focalization
  - **Motivation:** Proof search startegy based on the notion of polarity
  - **State of art:** Nothing
  - **Contribution:** Not in this talk
Infinitary proof system $\mu MALL^\infty$
Formulas

**µ**\textit{MALL}\textsuperscript{∞} formulas

\[
F ::= \top | \bot | 0 | 1 | F \otimes F | F \bowtie F | F \& F | F \oplus F \quad \text{MALL formulas}
\]

\[
| \mu X.F \\
| \nu X.F
\]

- \(\mu\) and \(\nu\) are dual.

**Example:** \(\neg(\nu X. X \otimes X) = \mu X. X \bowtie X\).

- Data types encoding

\[
\text{Nat} ::= \mu X. 1 \oplus X
\]

\[
\text{Stream}(A) ::= \nu X. A \otimes X
\]
Sequent calculus

\( \mu \text{MALL}^\infty \) pre-proofs are the trees coinductively generated by:

**Usual logical rules**

\[
\frac{\Gamma, F}{\Gamma, \Delta, F \otimes G} \quad \frac{\Gamma, F, G}{\Gamma, F \otimes G} \quad \frac{\Gamma, F}{\Gamma, G} \quad \frac{\Gamma, F}{\Gamma, F \& G} \quad \frac{\Gamma, F}{\Gamma, F \oplus F} \quad \frac{\Gamma, F_i}{\Gamma, F_1 \oplus F_2}
\]

**Identity rules**

\[
\frac{\Gamma, F}{\Gamma, \neg F} \quad \frac{\Gamma, F}{\Gamma, \Delta, \neg F} \quad \frac{\Gamma, \Delta}{\Gamma}
\]

**Rules for \( \mu \) and \( \nu \)**

\[
\frac{\Gamma, F[\mu X.F/X]}{\Gamma, \mu X.F} \quad \frac{\Gamma, F[\nu X.F/X]}{\Gamma, \nu X.F}
\]
Sequent calculus - Example

\[
\vdash \mu X. X \quad \vdash \nu X. X, F \\
\vdash \mu X. X \quad \vdash \nu X. X, F \\
\vdash \mu X. X, F \\
\vdash F
\]

Pre-proofs are unsound, hence the need for a validity condition.
Sequent calculus - Example

\[
\vdash \mu X.X \quad (\mu) \\
\vdash \nu X.X, F \quad (\nu) \\
\vdash \nu X.X \quad (\nu) \\
\vdash F \quad \text{(cut)}
\]

Pre-proofs are unsound, hence the need for a validity condition.
Sequent calculus - Validity condition

- A **thread** in a branch is a sequence of formulas that traces the evolution of a given formula.
- A thread is **valid** if its outermost formula is a ν-formula.
- A pre-proof is **valid** if every branch contains a valid thread.
- A valid pre-proof is called **proof**.

\[
\begin{align*}
F & := \mu X. \nu Y. X \oplus Y \\
G & := \nu X. \mu Y. X \oplus Y \\
H & := \nu Y. F \oplus Y \\
I & := \mu Y. G \oplus Y
\end{align*}
\]

\[
\vdash F, G \quad (\oplus_1)
\]
\[
\vdash F, G \oplus I \quad (\oplus_1)
\]
\[
\vdash F, I \quad (\mu)
\]
\[
\vdash F, G \quad (\nu)
\]
\[
\vdash F \oplus H, G \quad (\oplus_1)
\]
\[
\vdash H, G \quad (\nu)
\]
\[
\vdash F, G \quad (\mu)
\]
Cut elimination
Cut elimination procedure

- **Strategy:** “push” the cuts away from the root.

- **Cut-Cut:**

\[
\begin{align*}
\vdash \Gamma, F & \quad \vdash \neg F, \Delta, G \\
\vdash \Gamma, \Delta, G & \quad \vdash \neg G, \Sigma \\
\vdash \Gamma, \Delta, \Sigma & \\
\vdash \neg F, \Delta, G & \quad \vdash \neg G, \Sigma \\
\vdash \Gamma, F & \quad \vdash \neg F, \Delta, \Sigma \\
\vdash \Gamma, \Delta, \Sigma & \\
\end{align*}
\]
Cut elimination procedure

- **Strategy:** “push” the cuts away from the root.

- **Cut-Cut:**

\[
\begin{align*}
\vdash \Gamma, F & \quad \vdash \neg F, \Delta, G \\
\quad & \quad \vdash \Gamma, \Delta, G \quad \text{(cut)} \quad \vdash \neg G, \Sigma \\
\quad & \quad \vdash \Gamma, \Delta, \Sigma \quad \text{(cut)} \quad \vdash \Gamma, \Delta, \Sigma \\
\downarrow \\
\vdash \Gamma, F & \quad \vdash \neg F, \Delta, G \\
\quad & \quad \vdash \neg G, \Sigma \quad \text{(m-cut)} \quad \vdash \Gamma, \Delta, \Sigma
\end{align*}
\]
Cut elimination procedure - External operations

\[
\frac{\vdash \Delta, F, G}{\vdash \Delta, F \otimes G \quad \text{(\otimes)}} \quad \frac{\vdash \Delta, F \otimes G}{\vdash \Sigma, F \otimes G \quad \text{(m-cut)}} \quad \Rightarrow \quad \frac{\vdash \Delta, F, G}{\vdash \Delta, F \otimes G \quad \text{(m-cut)}} \quad \frac{\vdash \Sigma, F, G}{\vdash \Sigma, F \otimes G \quad \text{(m-cut)}}
\]

\[
\frac{\vdash \Delta, F \quad \vdash \Delta, G}{\vdash \Delta, F \& G \quad \text{&(\&)}} \quad \frac{\vdash \Delta, F \& G}{\vdash \Sigma, F \& G \quad \text{(m-cut)}} \quad \Rightarrow \quad \frac{\vdash \Delta, F}{\vdash \Sigma, F \quad \text{(m-cut)}} \quad \frac{\vdash \Delta, G}{\vdash \Sigma, G \quad \text{(m-cut)}} \quad \frac{\vdash \Delta, G \quad \vdash \Delta, F}{\vdash \Sigma, F \& G \quad \text{(m-cut)}}
\]

\[
\frac{\vdash \Delta, F[\mu X.F/X]}{\vdash \Delta, \mu X.F \quad \text{\mu (\mu)}} \quad \Rightarrow \quad \frac{\vdash \Delta, \mu X.F}{\vdash \Sigma, \mu X.F \quad \text{(m-cut)}} \quad \frac{\vdash \Sigma, F[\mu X.F/X]}{\vdash \Sigma, \mu X.F \quad \text{\mu (\mu)}}
\]

External operations are productive
Cut elimination procedure - Internal operations

Internal operations are not productive
Cut elimination algorithm

- **Internal phase**: Perform internal transformations while you can’t do anything else.

- **External phase**: Build a part of the output tree whenever you can.
Cut elimination algorithm

- **Internal phase:** Perform internal transformations while you can’t do anything else.

- **External phase:** Build a part of the output tree whenever you can.

- Repeat.
Cut elimination algorithm

- **Internal phase:** Perform internal transformations while you can’t do anything else.

- **External phase:** Build a part of the output tree whenever you can.

- Repeat.
Cut elimination is productive

Theorem
Internal phase always halts.
Cut elimination is productive

Theorem
Internal phase always halts.

Proof: Suppose that the internal phase diverges for a proof $\pi \vdash \Delta$.

- Let $\theta$ be the sub-derivation of $\pi$ explored by the reduction.
- No rule is applied to a formula of $\Delta$ in $\theta$, as this would contradict the divergence of internal phase.
- Let $\overline{\theta}$ be the proof obtained from $\theta$ by dropping all the formulas from $\Delta$.
- $\overline{\theta}$ is then a proof for $\vdash$.
- We define a truth semantics for $\mu MALL^\infty$ formulas and show that the proof system is sound with respect to it.

Contradiction.
Cut elimination produces a proof

Theorem
The pre-proof obtained by the cut elimination algorithm is valid.
Theorem
The pre-proof obtained by the cut elimination algorithm is valid.

Proof: Let $\pi^*$ be the pre-proof obtained from $\pi \vdash \Delta$ by cut elimination. Suppose that a branch $b$ of $\pi^*$ is not valid.

- Let $\theta$ be the sub-derivation of $\pi$ explored by the reduction that produces $b$.
- **Fact:** Threads of $\theta$ are the threads of $b$, together with threads starting from cut formulas.
- The validity of $\theta$ cannot rely on the threads of $b$.
- $\theta^\mu$ is $\theta$ where we replace in $\Delta$ any $\nu$ by a $\mu$ and any $1, \top$ by $\bot, 0$.
- Show that formulas containing only $\mu, \bot, 0$ and $MALL$ connectives are false.
- $\theta^\mu$ proves a false sequent which contradicts soundness.
Conclusion
Conclusion

- Syntactic cut elimination with a new technique
- Focalisation

Future work:

- Go beyond Linear Logic and handle structural rules
- Translate infinitary proofs to finitary ones
- Same question by preserving the computational content

Thank you for your attention!
Conclusion

- Syntactic cut elimination with a new technique
- Focalisation

Future work:

- Go beyond Linear Logic and handle structural rules
- Translate infinitary proofs to finitary ones
- Same question by preserving the computational content

Thank you for your attention!