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**

$$\mathsf{N} = 1 \oplus \mathsf{N}$$

Introduction

- **Inductive and coinductive definitions**

$$\mathsf{N} = \mu X.1 \oplus X$$

Introduction

- **Inductive and coinductive definitions**

$$\mathsf{N} = \mu X.1 \oplus X$$

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

Introduction

- **Inductive and coinductive definitions**

$$\mathsf{N} = \mu X.1 \oplus X$$
$$\mathsf{S} = N \otimes \mathsf{S}$$

Introduction

- **Inductive and coinductive definitions**

$$\mathsf{N} = \mu X.1 \oplus X$$
$$\mathsf{S} = \nu X.N \otimes X$$

Introduction

- **Inductive and coinductive definitions**

$$\mathrm{N} = \mu X.1 \oplus X$$
$$\mathrm{S} = \nu X.N \otimes X$$

Introduction

- **Inductive and coinductive definitions**

$$\mathrm{N} = \mu X.1 \oplus X$$
$$\mathrm{S} = \nu X.N \otimes X$$

- **Proofs-programs over these data types**

$$\begin{array}{lcll} double(n) & = & 0 & \text{if } n = 0 \\ & = & succ(succ(double(m))) & \text{if } n = succ(m) \end{array}$$

Introduction

- **Inductive and coinductive definitions**

$$
\begin{aligned}
\mathsf{N} &= \mu X.1 \oplus X \\
\mathsf{S} &= \nu X.N \otimes X
\end{aligned}
$$

- **Proofs-programs over these data types**

$$
\begin{array}{lcll}
double(n) & = & 0 & \text{if } n = 0 \\
 & = & succ(succ(double(m))) & \text{if } n = succ(m)
\end{array}
$$

$$
\Pi_{double} =
\begin{prooftree}
\AxiomC{}
\RightLabel{(1)}
\UnaryInfC{$1 \vdash 1$}
\RightLabel{$(\oplus_1)$}
\UnaryInfC{$1 \vdash 1 \oplus N$}
\RightLabel{(μ_l)}
\UnaryInfC{$1 \vdash N$}
\AxiomC{Π_{double}}
\UnaryInfC{$N \vdash N$}
\RightLabel{$(\oplus_2)$}
\UnaryInfC{$N \vdash 1 \oplus N$}
\RightLabel{(μ_r)}
\UnaryInfC{$N \vdash N$}
\RightLabel{$(\oplus_2)$}
\UnaryInfC{$N \vdash 1 \oplus N$}
\RightLabel{(μ_r)}
\UnaryInfC{$N \vdash N$}
\RightLabel{$(\oplus_l)$}
\BinaryInfC{$1 \oplus N \vdash N$}
\RightLabel{(μ_l)}
\UnaryInfC{$N \vdash N$}
\end{prooftree}
$$

Infinitary (circular) proofs in the litterature

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

$$\mu\text{-calulus formula} \quad \rightarrow \quad \text{Proof search} \begin{array}{l} \nearrow \quad \text{Success} \quad \rightarrow \quad \text{Validity} \\ \searrow \quad \text{Failure} \quad \rightarrow \quad \text{Invalidity} \end{array}$$

Infinitary (circular) proofs in the litterature

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

$$\mu\text{-calulus formula} \quad \rightarrow \quad \text{Proof search} \begin{array}{l} \nearrow \quad \text{Success} \quad \rightarrow \quad \text{Validity} \\ \\ \searrow \quad \text{Failure} \quad \rightarrow \quad \text{Invalidity} \end{array}$$

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

$$\mu\text{-calulus formula} \quad \rightarrow \quad \text{Circular proof} \quad \rightarrow \quad \text{Finite axiomatization}$$

Infinitary (circular) proofs in the litterature

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

$$\mu\text{-calulus formula} \quad \rightarrow \quad \text{Proof search} \begin{array}{l} \nearrow \quad \text{Success} \quad \rightarrow \quad \text{Validity} \\ \searrow \quad \text{Failure} \quad \rightarrow \quad \text{Invalidity} \end{array}$$

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

$$\mu\text{-calulus formula} \quad \rightarrow \quad \text{Circular proof} \quad \rightarrow \quad \text{Finite axiomatization}$$

- **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 startegy based on the notion of polarity

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)
- Focalization
  - **Motivation:** Proof search startegy 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

$\mu MALL^\infty$ formulas

$$
\begin{array}{lcll}
F & ::= & \top \mid \bot \mid 0 \mid 1 \mid F \otimes F \mid F \parr F \mid F \& F \mid F \oplus F & MALL \textbf{ formulas} \\
 & \mid & \mu X.F & \textbf{least fixed point} \\
 & \mid & \nu X.F & \textbf{greatest fixed point}
\end{array}
$$

- μ and ν are dual.

  <u>Example:</u> $\neg(\nu X.X \otimes X) = \mu X.X \parr X$.

- Data types encoding

$$
\begin{array}{rcl}
\mathrm{Nat} & := & \mu X.1 \oplus X \\
\mathrm{Stream}(A) & := & \nu X.A \otimes X
\end{array}
$$

Sequent calculus

$\mu MALL^\infty$ pre-proofs are the trees coinductively generated by:

Usual logical rules

$$\frac{\vdash \Gamma, F \qquad \vdash \Delta, G}{\vdash \Gamma, \Delta, F \otimes G}\ (\otimes) \qquad \frac{\vdash \Gamma, F, G}{\vdash \Gamma, F \parr G}\ (\parr) \qquad \frac{\vdash \Gamma, F \qquad \vdash \Gamma, G}{\vdash \Gamma, F \& G}\ (\&) \qquad \frac{\vdash \Gamma, F_i}{\vdash \Gamma, F_1 \oplus F_2}\ (\oplus_i)$$

Identity rules

$$\frac{}{\vdash F, \neg F}\ (\mathrm{ax}) \qquad \frac{\vdash \Gamma, F \qquad \vdash \Delta, \neg F}{\vdash \Gamma, \Delta}\ (\mathrm{cut})$$

Rules for μ and ν

$$\frac{\vdash \Gamma, F[\mu X.F/X]}{\vdash \Gamma, \mu X.F}\ (\mu) \qquad \frac{\vdash \Gamma, F[\nu X.F/X]}{\vdash \Gamma, \nu X.F}\ (\nu)$$

Sequent calculus - Example

$$
\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\;(\mu)}{\vdash \mu X.X}\;(\mu) \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, F}\;(\nu)}{\vdash \nu X.X, F}\;(\nu)}{\vdash F}\;(\mathtt{cut})
$$

Sequent calculus - Example

$$
\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\;(\mu)}{\vdash \mu X.X}\;(\mu) \qquad \dfrac{\dfrac{\dfrac{\vdots}{\vdash \nu X.X, F}\;(\nu)}{\vdash \nu X.X, F}\;(\nu)}{}}{\vdash F}\;(\mathtt{cut})
$$

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**.

$$F := \mu X.\nu Y.X \oplus Y \qquad G := \nu X.\mu Y.X \oplus Y$$

$$H := \nu Y.F \oplus Y \qquad I := \mu Y.G \oplus Y$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\vdash F, G}\,(\oplus_1)}{\vdash F, G \oplus I}\,(\oplus_1)}{\vdash F, I}\,(\mu)}{\vdash F, G}\,(\nu)}{\vdash F \oplus H, G}\,(\oplus_1)}{\vdash H, G}\,(\nu)}{\vdash F, G}\,(\mu)$$

Cut elimination

Cut elimination procedure

- **Strategy:** "push" the cuts away from the root.
- **Cut-Cut:**

$$\dfrac{\dfrac{\vdash \Gamma, F \qquad \vdash \neg F, \Delta, G}{\vdash \Gamma, \Delta, G}\ (\mathtt{cut}) \qquad \vdash \neg G, \Sigma}{\vdash \Gamma, \Delta, \Sigma}\ (\mathtt{cut})$$

$$\updownarrow$$

$$\dfrac{\vdash \Gamma, F \qquad \dfrac{\vdash \neg F, \Delta, G \qquad \vdash \neg G, \Sigma}{\vdash \neg F, \Delta, \Sigma}\ (\mathtt{cut})}{\vdash \Gamma, \Delta, \Sigma}\ (\mathtt{cut})$$

Cut elimination procedure

- **Strategy:** "push" the cuts away from the root.
- **Cut-Cut:**

$$\dfrac{\dfrac{\vdash \Gamma, F \qquad \vdash \neg F, \Delta, G}{\vdash \Gamma, \Delta, G}\ (\mathtt{cut}) \qquad \vdash \neg G, \Sigma}{\vdash \Gamma, \Delta, \Sigma}\ (\mathtt{cut})$$

$$\downarrow$$

$$\dfrac{\vdash \Gamma, F \qquad \vdash \neg F, \Delta, G \qquad \vdash \neg G, \Sigma}{\vdash \Gamma, \Delta, \Sigma}\ (\mathtt{m\text{-}cut})$$

Cut elimination procedure - External operations

$$\dfrac{\dfrac{\vdash \Delta, F, G}{\vdash \Delta, F \parr G}\ (\parr) \qquad \ldots}{\vdash \Sigma, F \parr G}\ (\texttt{m-cut}) \quad \Rightarrow \quad \dfrac{\dfrac{\vdash \Delta, F, G \qquad \ldots}{\vdash \Sigma, F, G}\ (\texttt{m-cut})}{\vdash \Sigma, F \parr G}\ (\parr)$$

$$\dfrac{\dfrac{\vdash \Delta, F \qquad \vdash \Delta, G}{\vdash \Delta, F \& G}\ (\&) \qquad \ldots}{\vdash \Sigma, F \& G}\ (\texttt{m-cut}) \quad \Rightarrow \quad \dfrac{\dfrac{\vdash \Delta, F \qquad \ldots}{\vdash \Sigma, F}\ (\texttt{m-cut}) \qquad \dfrac{\vdash \Delta, G \qquad \ldots}{\vdash \Sigma, G}\ (\texttt{m-cut})}{\vdash \Sigma, F \& G}\ (\&)$$

$$\dfrac{\dfrac{\vdash \Delta, F[\mu X.F/X]}{\vdash \Delta, \mu X.F}\ (\mu) \qquad \ldots}{\vdash \Sigma, \mu X.F}\ (m - cut) \quad \Rightarrow \quad \dfrac{\dfrac{\vdash \Delta, F[\mu X.F/X] \qquad \ldots}{\vdash \Sigma, F[\mu X.F/X]}\ (m - cut)}{\vdash \Sigma, \mu X.F}\ (\mu)$$

External operations are productive

Cut elimination procedure - Internal operations

$$\dfrac{\dots \quad \dfrac{\vdash \Delta, F_2 \quad \vdash \Delta, F_1}{\vdash \Delta, F_2 \& F_1}\ (\&) \quad \dfrac{\vdash \Gamma, F_i^{\perp}}{\vdash \Gamma, F_1^{\perp} \oplus F_2^{\perp}}\ (\oplus_i)}{\vdash \Sigma}\ (\texttt{m-cut})$$

$$\Rightarrow \quad \dfrac{\dots \quad \vdash \Delta, F_i \quad \vdash \Gamma, F_i^{\perp}}{\vdash \Sigma}\ (\texttt{m-cut})$$

$$\dfrac{\dots \quad \dfrac{\vdash \Delta, F[\mu X.F/X]}{\vdash \Delta, \mu X.F}\ (\mu) \quad \dfrac{\vdash \Gamma, F^{\perp}[\nu X.F^{\perp}/X]}{\vdash \Gamma, \nu X.F^{\perp}}\ (\nu)}{\vdash \Sigma}\ (\texttt{m-cut})$$

$$\Rightarrow \quad \dfrac{\dots \quad \vdash \Delta, F[\mu X.F/X] \quad \vdash \Gamma, F^{\perp}[\nu X.F^{\perp}/X]}{\vdash \Sigma}\ (\texttt{m-cut})$$

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 θ be the sub-derivation of π explored by the reduction.
- No rule is applied to a formula of Δ in θ,
  as this would contradict the divergence of internal phase.
- Let $\overline{\theta}$ be the proof obtained from θ by dropping all the formulas from Δ.
- $\overline{\theta}$ 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.

Cut elimination produces a proof

Theorem

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

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

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

Conclusion

Conclusion

- Syntactic cut elimination with a new technique
- Focalisation
- Futur work:
  - Go beyond Linear Logic and handle structural rules
  - Translate infinitrary proofs to finitary ones
  - Same question by preserving the computational content

Conclusion

- Syntactic cut elimination with a new technique
- Focalisation
- Futur work:
  - Go beyond Linear Logic and handle structural rules
  - Translate infinitrary proofs to finitary ones
  - Same question by preserving the computational content

Thank you for your attention!