

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

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

Introduction

- **Inductive and coinductive definitions**

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

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

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

Introduction

- **Inductive and coinductive definitions**

$$N = \mu X. 1 \oplus X$$

$$S = \nu X. N \otimes X$$

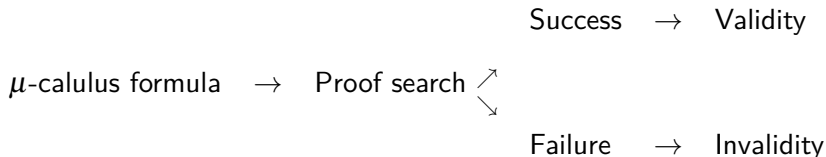
- **Proofs-programs over these data types**

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

$$\begin{array}{c} \Pi_{\text{double}} = \frac{\frac{\frac{\frac{1 \vdash 1}{1 \vdash 1 \oplus N} \text{ (}\oplus_1\text{)}}{1 \vdash N} \text{ (}\mu_l\text{)}}{1 \oplus N \vdash N} \text{ (}\oplus_l\text{)}}{N \vdash N} \text{ (}\mu_l\text{)}}{\frac{\frac{\frac{N \vdash N}{N \vdash 1 \oplus N} \text{ (}\oplus_2\text{)}}{N \vdash 1 \oplus N} \text{ (}\mu_r\text{)}}{N \vdash N} \text{ (}\oplus_2\text{)}}{N \vdash 1 \oplus N} \text{ (}\mu_r\text{)}} \text{ (}\oplus_2\text{)}}{\frac{N \vdash N}{N \vdash N} \text{ (}\oplus_2\text{)}} \text{ (}\oplus_2\text{)}} \text{ (}\oplus_2\text{)}} \end{array}$$

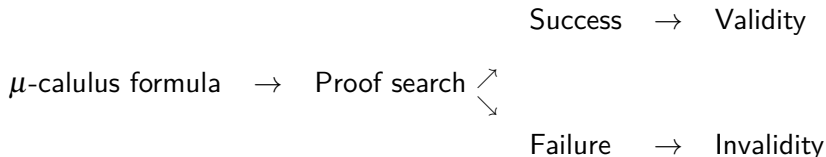
Infinitary (circular) proofs in the literature

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



Infinitary (circular) proofs in the literature

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

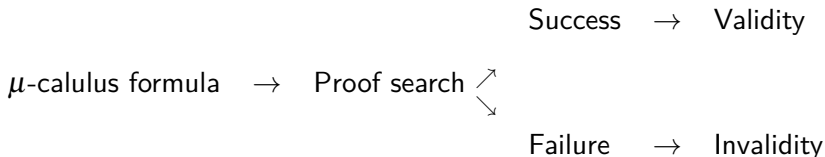


- **Completeness arguments:** Intermediate objects between syntax and semantics (Kozen, Kaivola, Walukiewicz)

μ -calculus formula \rightarrow Circular proof \rightarrow Finite axiomatization

Infinitary (circular) proofs in the literature

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



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

μ -calculus formula \rightarrow Circular proof \rightarrow 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 strategy 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 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 strategy based on the notion of polarity
 - **State of art:** Nothing
 - **Contribution:** Not in this talk

Infinitary proof system $\mu MALL^\infty$

Formulas

μ MALL $^\infty$ formulas

$F ::= \top \mid \perp \mid 0 \mid 1 \mid F \otimes F \mid F \wp F \mid F \& F \mid F \oplus F$ MALL formulas
| $\mu X.F$ least fixed point
| $\nu X.F$ greatest fixed point

- μ and ν are dual.

Example: $\neg(\nu X.X \otimes X) = \mu X.X \wp X$.

- Data types encoding

Nat := $\mu X.1 \oplus X$

Stream(A) := $\nu X.A \otimes X$

Sequent calculus

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

Usual logical rules

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

Identity rules

$$\frac{}{\vdash F, \neg F} \quad (\text{ax}) \quad \frac{\vdash \Gamma, F \quad \vdash \Delta, \neg F}{\vdash \Gamma, \Delta} \quad (\text{cut})$$

Rules for μ and ν

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

Sequent calculus - Example

$$\frac{\frac{\vdots}{\vdash \mu X.X} (\mu) \quad \frac{\vdots}{\vdash \nu X.X, F} (\nu)}{\vdash \mu X.X} (\mu) \quad \frac{\vdots}{\vdash \nu X.X, F} (\nu)}{\vdash F} (\text{cut})$$

Sequent calculus - Example

$$\frac{\frac{\vdots}{\vdash \mu X.X} (\mu) \quad \frac{\vdots}{\vdash \nu X.X, F} (\nu)}{\frac{\vdash \mu X.X \quad \vdash \nu X.X, F}{\vdash F} (\text{cut})} (\mu)$$

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**.

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

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

$$\begin{array}{c}
 \vdots \\
 \hline
 \vdash F, G \quad (\oplus_1) \\
 \hline
 \vdash F, G \oplus I \quad (\oplus_1) \\
 \hline
 \vdash F, I \quad (\mu) \\
 \hline
 \vdash F, G \quad (\nu) \\
 \hline
 \vdash F \oplus H, G \quad (\oplus_1) \\
 \hline
 \vdash H, G \quad (\nu) \\
 \hline
 \vdash F, G \quad (\mu)
 \end{array}$$

Cut elimination

Cut elimination procedure

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

$$\frac{\frac{\frac{\vdash \Gamma, F \quad \vdash \neg F, \Delta, G}{\vdash \Gamma, \Delta, G} \text{ (cut)}}{\vdash \Gamma, \Delta, \Sigma} \text{ (cut)}}{\vdash \Gamma, \Delta, \Sigma} \text{ (cut)}}{\vdash \Gamma, \Delta, \Sigma} \text{ (cut)}$$

\updownarrow

$$\frac{\frac{\vdash \Gamma, F}{\vdash \Gamma, \Delta, \Sigma} \text{ (cut)}}{\vdash \Gamma, \Delta, \Sigma} \text{ (cut)} \quad \frac{\frac{\vdash \neg F, \Delta, G \quad \vdash \neg G, \Sigma}{\vdash \neg F, \Delta, \Sigma} \text{ (cut)}}{\vdash \Gamma, \Delta, \Sigma} \text{ (cut)}$$

Cut elimination procedure

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

$$\frac{\frac{\frac{\vdash \Gamma, F \quad \vdash \neg F, \Delta, G}{\vdash \Gamma, \Delta, G} \text{ (cut)}}{\vdash \Gamma, \Delta, \Sigma} \text{ (cut)}}{\vdash \Gamma, \Delta, \Sigma} \text{ (cut)}$$

↓

$$\frac{\vdash \Gamma, F \quad \vdash \neg F, \Delta, G \quad \vdash \neg G, \Sigma}{\vdash \Gamma, \Delta, \Sigma} \text{ (m-cut)}$$

Cut elimination procedure - External operations

$$\frac{\frac{\vdash \Delta, F, G}{\vdash \Delta, F \wp G} (\wp) \quad \dots}{\vdash \Sigma, F \wp G} (m\text{-cut}) \quad \Rightarrow \quad \frac{\frac{\vdash \Delta, F, G}{\vdash \Sigma, F, G} \dots}{\vdash \Sigma, F \wp G} (m\text{-cut}) (\wp)$$

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

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

External operations are productive

Cut elimination procedure - Internal operations

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

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

$$\frac{\dots \quad \frac{\frac{\vdash \Delta, F[\mu X.F/X]}{\vdash \Delta, \mu X.F} \text{ (\mu)}}{\vdash \Sigma} \quad \frac{\frac{\vdash \Gamma, F^\perp[vX.F^\perp/X]}{\vdash \Gamma, vX.F^\perp} \text{ (v)}}{\vdash \Sigma} \text{ (m-cut)}}{\vdash \Sigma}$$

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

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 $\bar{\theta}$ be the proof obtained from θ by dropping all the formulas from Δ .
- $\bar{\theta}$ 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 π^* be the pre-proof obtained from $\pi \vdash \Delta$ by cut elimination. Suppose that a branch b of π^* 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 infinitary 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 infinitary proofs to finitary ones
 - Same question by preserving the computational content

Thank you for your attention!