Introduction to linear logic

Emmanuel Beffara

IML, CNRS & Université d'Aix-Marseille

Summmer school on linear logic and geometry of interaction
Torino – 27th August 2013

Lecture notes are available at
`http://iml.univ-mrs.fr/~beffara/intro-ll.pdf`

The proof-program correspondence

Linear sequent calculus

A bit of semantics

A bit of proof theory

Proof nets

Plan

What are we doing here?

Proof theory in 3 dates:

1900 Hilbert: the question of foundations of mathematics

1930 Gödel: incompleteness theorem
Gentzen: sequent calculus and cut elimination

1960 Curry-Howard correspondence

What are we doing here?

Proof theory in 3 dates:

- 1900 Hilbert: the question of foundations of mathematics
- 1930 Gödel: incompleteness theorem
  Gentzen: sequent calculus and cut elimination
- 1960 Curry-Howard correspondence

The central question: **consistency**

- logic: is my logical system degenerate?
- computation: can my program go wrong?

Implies a search for *meaning*: semantics.

Curry-Howard: the setting

Definition

Formulas of propositional logic:

$A, B := \alpha$	propositional variables
$A \Rightarrow B$	implication
$A \wedge B$	conjunction

Definition

Terms of the simply-typed λ-calculus with pairs:

$t, u := x$	variable
$\lambda x^A.t$	abstraction, i.e. function
$(t)u$	application
$\langle t, u \rangle$	pairing
$\pi_i t$	projection, with $i = 1$ or $i = 2$

Curry-Howard: statics

Identity:

$$\frac{}{\Gamma, x : A \vdash x : A}\ \text{ax}$$

Implication:

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B}\ {\Rightarrow}\text{I} \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash (t)u : B}\ {\Rightarrow}\text{E}$$

Conjunction:

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B}{\Gamma \vdash \langle t, u \rangle : A \wedge B}\ {\wedge}\text{I} \quad \frac{\Gamma \vdash t : A \wedge B}{\Gamma \vdash \pi_1 t : A}\ {\wedge}\text{E1} \quad \frac{\Gamma \vdash t : A \wedge B}{\Gamma \vdash \pi_2 t : B}\ {\wedge}\text{E2}$$

Definition

Evaluation is the relation generated by the pair of rules

$$(\lambda x.t)u \rightsquigarrow t[u/x] \qquad \text{and} \qquad \pi_i\langle t_1, t_2\rangle \rightsquigarrow t_i \quad \text{for } i = 1 \text{ or } i = 2$$

The typed λ-calculus

Definition

Evaluation is the relation generated by the pair of rules

$$(\lambda x.t)u \rightsquigarrow t[u/x] \qquad \text{and} \qquad \pi_i\langle t_1, t_2\rangle \rightsquigarrow t_i \quad \text{for } i = 1 \text{ or } i = 2$$

Theorem (Subject reduction)

If $\Gamma \vdash t : A$ *holds and* $t \rightsquigarrow u$ *then* $\Gamma \vdash u : A$ *holds.*

Theorem (Termination)

A typable term has no infinite sequence of reductions.

The typed λ-calculus

Definition

Evaluation is the relation generated by the pair of rules

$$(\lambda x.t)u \rightsquigarrow t[u/x] \qquad \text{and} \qquad \pi_i\langle t_1, t_2\rangle \rightsquigarrow t_i \quad \text{for } i = 1 \text{ or } i = 2$$

Theorem (Subject reduction)

If $\Gamma \vdash t : A$ holds and $t \rightsquigarrow u$ then $\Gamma \vdash u : A$ holds.

Theorem (Termination)

A typable term has no infinite sequence of reductions.

Theorem (Confluence)

For any reductions $t \rightsquigarrow^* u$ and $t \rightsquigarrow^* v$,
there is a term w such that $u \rightsquigarrow^* w$ and $v \rightsquigarrow^* w$.

Curry-Howard: dynamics

What does evaluation mean, when considering proofs?

Curry-Howard: dynamics

What does evaluation mean, when considering proofs?

Theorem

A proof in natural deduction is normal *iff there is never an introduction rule followed by an elimination rule for the same connective.*

Curry-Howard: dynamics

What does evaluation mean, when considering proofs?

Theorem

A proof in natural deduction is normal *iff there is never an introduction rule followed by an elimination rule for the same connective.*

Theorem (Subformula property)

In a normal proof, any formula occurring in a sequent at any point in the proof is a subformula of one of the formulas in the conclusion.

Normal proofs are *direct*, *explicit*.

Denotational semantics

The search for invariants of reduction:

- *models* of the λ-calculus (as a theory of functions)
- structures for defining the *value* of proofs

The kind of objects we want is:

logic	computation	object
formula	type	space
proof	term	morphism
normalization	evaluation	equality

Example

Sets for types, arbitrary functions for terms.
It works but there are way too many functions!

Coherence spaces

Definition

A *coherence space* A is

- a set $|A|$ (the web),
- a symmetric and reflexive binary relation $\frown_A$ (the coherence).

A *clique* $a \in \mathcal{C}\ell(A)$ is a subset of $|A|$ of points pairwise related by $\frown_A$.

Intuition:

- points are bits of information about objects of A,
- cliques are consistent descriptions of objects

Example

A coherence space for words could have bits to say

- "at position i there is a letter a"
- "at position i there is the end-of-string symbol"

Stable functions

A definable function maps information about an object in A to information about an object of B.

Definition

A stable function from A to B is a function $f : \mathcal{Cl}(A) \to \mathcal{Cl}(B)$ that is

continuous: for a directed family $(a_i)_{i \in I}$ in $\mathcal{Cl}(A)$, $f(\bigcup_{i \in I} a_i) = \bigcup_{i \in I} f(a_i)$;

stable: for all $a, a' \in \mathcal{Cl}(A)$ such that $a \cup a' \in \mathcal{Cl}(A)$, $f(a \cap a') = f(a) \cap f(a')$.

Implies monotonicity.

- The value for an arbitrary input is deduced from finite approximations,
- For every bit of output, there is a minimum input needed to get it.

Stable functions – traces

Definition

The *trace* of a stable function $f : \mathcal{C}\ell(A) \to \mathcal{C}\ell(B)$ is

$$Tr\big(f\big) := \Big\{(a, \beta) \;\Big|\; a \in \mathcal{C}\ell(A),\ \beta \in f(a),\ \forall a' \subsetneq a, \beta \notin f(a')\Big\}.$$

Remarkable facts:

- Each stable function is uniquely defined by its trace.
- Traces are the cliques in a coherence space $A \Rightarrow B$.

Stable functions – linearity

Definition

A stable function f is *linear* if for all $(a, \beta) \in Tr(f)$, a is a singleton.

- For one bit of output, you need one bit of input.
- The function uses its argument exactly once.

Classical sequent calculus has *weakening* and *contraction* of formulas, which allows using any hypothesis any number of times:

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ \mathrm{wL} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\ \mathrm{wR} \qquad \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ \mathrm{cL} \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ \mathrm{cR}$$

These make the following rules equivalent:

$$\underset{\text{additive}}{\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}}\ \wedge\mathrm{Ra} \qquad \underset{\text{multiplicative}}{\frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \wedge B, \Delta, \Delta'}}\ \wedge\mathrm{Rm}$$

And similarly for other connectives, left rules, etc.

In the absence of weakening and contraction, these become different.

Sequents in intuitionistic logic:

$$A_1, \ldots, A_n \vdash B$$

"From hypotheses $A_1, \ldots, A_n$ deduce B."

A proof of this is interpreted as

- a way to make a proof of B from proofs of the A_i
- a function from $A_1 \times \ldots \times A_n$ to B

Contraction and weakening are allowed on the left.

Sequent calculi

Sequents in classical logic:

$$A_1, \dots, A_n \vdash B_1, \dots, B_p$$

"From hypotheses $A_1, \dots, A_n$ deduce B_1 or … or B_p ."

Contraction and weakening are allowed on both sides.

Sequent calculi

Sequents in linear logic:

$$A_1, \dots, A_n \vdash B_1, \dots, B_p$$

"From hypotheses $A_1, \dots, A_n$ deduce B_1 or … or B_p *linearly*."

A proof of this is interpreted as

- a way to make a proof of B from proofs of the A_i using each A_i exactly once
- a linear map from $A_1 \otimes \dots \otimes A_n$ to $B_1 \parr \dots \parr B_p$

Contraction and weakening are **not** allowed.

Plan

The proof-program correspondence

Linear sequent calculus

- Multiplicative linear logic
- One-sided presentation
- Full linear logic
- The notion of fragment

A bit of semantics

A bit of proof theory

Proof nets

Formulas and sequents

In this talk we focus on the propositional structure:

formulas	$A, B := \alpha$	propositional variable
	$A^{\perp}$	linear negation
	$A \otimes B,\ A ⅋ B,\ 1,\ \perp$	multiplicatives
	$A \& B,\ A \oplus B,\ \top,\ 0$	additives
	$!A,\ ?A$	exponentials
sequents	$\Gamma, \Delta, \Theta := A_1, \dots, A_n \vdash B_1, \dots, B_p$	with $n, p \geqslant 0$

Formulas and sequents

In this talk we focus on the propositional structure:

formulas	$A, B := \alpha$	propositional variable
	$A^\perp$	linear negation
	$A \otimes B,\ A \parr B,\ 1,\ \perp$	multiplicatives
	$A \mathbin{\&} B,\ A \oplus B,\ \top,\ 0$	additives
	$!A,\ ?A$	exponentials
sequents	$\Gamma, \Delta, \Theta := A_1, \dots, A_n \vdash B_1, \dots, B_p$	with $n, p \geqslant 0$

We focus on MLL, the subsystem made only of multiplicative connectives and negation.

Definition

$A \multimap B$ is a notation for $A^\perp \parr B$.

MLL – the deductive structure

The order of formulas is irrelevant:

$$\frac{\Gamma, A, B, \Delta \vdash \Theta}{\Gamma, B, A, \Delta \vdash \Theta}\ \text{exL} \qquad \frac{\Gamma \vdash \Delta, A, B, \Theta}{\Gamma \vdash \Delta, B, A, \Theta}\ \text{exR}$$

Axiom and cut rules:

$$\frac{}{A \vdash A}\ \text{ax} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ \text{cut}$$

Linear negation:

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, A^{\perp} \vdash \Delta}\ \perp\text{L} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash A^{\perp}, \Delta}\ \perp\text{R}$$

MLL – the connectives

Multiplicatives:

$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma' \vdash \Delta', B}{\Gamma, \Gamma' \vdash \Delta, \Delta', A \otimes B} \otimes R \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \otimes B \vdash \Delta} \otimes L$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \parr B \vdash \Delta, \Delta'} \parr L \qquad \frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \parr B} \parr R$$

Additives:

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \oplus B} \oplus R_1 \qquad \frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \oplus B} \oplus R_2 \qquad \frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \oplus B \vdash \Delta} \oplus L$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \,\&\, B \vdash \Delta} \&L_1 \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \,\&\, B \vdash \Delta} \&L_2 \qquad \frac{\Gamma \vdash \Delta, A \qquad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \,\&\, B} \&R$$

MLL – provability

Example

The following sequents are provable in MLL:

- multiplicative excluded middle: $\vdash A \parr A^{\perp}$
- semi-distributivity of tensor over par: $A \otimes (B \parr C) \vdash (A \otimes B) \parr C$

However, $A \vdash A \otimes A$ is *not* provable.

Exercise: Prove that!

Definition

A and B are *linearly equivalent* if $A \vdash B$ and $B \vdash A$ are provable, write this $A \multimapboth B$.

Simplest example: $A \otimes B \multimapboth B \otimes A$.

Symmetries

Let us see if we can simplify the system a bit.

Let us see if we can simplify the system a bit.

Theorem (De Morgan laws)

For all formulas A and B, the following equivalences hold:

$$A \multimap\!\!\circ\, A^{\perp\perp}, \qquad (A \otimes B)^{\perp} \multimap\!\!\circ\, A^{\perp} \parr B^{\perp}, \qquad (A \parr B)^{\perp} \multimap\!\!\circ\, A^{\perp} \otimes B^{\perp}.$$

Exercise: Prove this.

Symmetries

Let us see if we can simplify the system a bit.

Theorem (De Morgan laws)

For all formulas A and B, the following equivalences hold:

$$A \multimap\!\!\!\!\circ\; A^{\perp\perp}, \qquad (A \otimes B)^{\perp} \multimap\!\!\!\!\circ\; A^{\perp} \parr B^{\perp}, \qquad (A \parr B)^{\perp} \multimap\!\!\!\!\circ\; A^{\perp} \otimes B^{\perp}.$$

Exercise: Prove this.

Theorem

A sequent $A_1, \ldots, A_n \vdash B_1, \ldots, B_p$ is provable if and only the sequent $\vdash A_1^{\perp}, \ldots, A_n^{\perp}, B_1, \ldots, B_p$ is provable.

Redefine the language of formulas:

formulas	$A, B := \alpha$	propositional variable
	$\alpha^\perp$	**negated variable**
	$A \otimes B,\ A \parr B,\ 1,\ \perp$	multiplicatives
	$A \,\&\, B,\ A \oplus B,\ \top,\ 0$	additives
	$!A,\ ?A$	exponentials
sequents	$\Gamma, \Delta, \Theta := \vdash A_1, \dots, A_n$	with $n \geqslant 0$

Definition

Negation is the operation on formulas defined as

$$(A \otimes B)^\perp := A^\perp \parr B^\perp \qquad (A \oplus B)^\perp := A^\perp \,\&\, B^\perp \qquad (!A)^\perp := ?(A^\perp)$$

$$(A \parr B)^\perp := A^\perp \otimes B^\perp \qquad (A \,\&\, B)^\perp := A^\perp \oplus B^\perp \qquad (?A)^\perp := !(A^\perp)$$

$$(\alpha^\perp)^\perp := \alpha \qquad 1^\perp := \perp \qquad 0^\perp := \top \qquad \perp^\perp := 1 \qquad \top^\perp := 0$$

By construction, $A^{\perp\perp} = A$.

One-sided sequent calculus

Axiom and cut rules:

$$\frac{}{\vdash A^\perp, A}\ \text{ax} \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\ \text{cut}$$

Multiplicatives:

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ \otimes \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ \parr$$

Additives:

$$\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \,\&\, B}\ \& \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B}\ \oplus_1 \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}\ \oplus_2$$

Units:

$$\frac{}{\vdash 1}\ 1 \qquad \frac{}{\vdash \Gamma, \top}\ \top \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \perp}\ \perp$$

One-sided sequent calculus

Axiom and cut rules:

$$\frac{}{\vdash A^\perp, A}\ \text{ax} \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\ \text{cut}$$

Multiplicatives:

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ \otimes \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ \parr$$

Additives:

$$\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \mathbin{\&} B}\ \& \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B}\ \oplus_1 \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}\ \oplus_2$$

Units:

$$\frac{}{\vdash 1}\ 1 \qquad \frac{}{\vdash \Gamma, \top}\ \top \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \perp}\ \perp$$

One-sided sequent calculus

Axiom and cut rules:

$$\frac{}{\vdash A^\perp, A}\ \text{ax} \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\ \text{cut}$$

Multiplicatives:

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ \otimes \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ \parr$$

Additives:

$$\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \mathbin{\&} B}\ \& \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B}\ \oplus_1 \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}\ \oplus_2$$

Units:

$$\frac{}{\vdash 1}\ 1 \qquad \frac{}{\vdash \Gamma, \top}\ \top \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \bot}\ \bot$$

Additives vs multiplicatives

Example: distributivity of $\otimes$ over $\oplus$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax} \quad \dfrac{}{\vdash B^\perp, B}\,\text{ax}}{\vdash A^\perp, B^\perp, A \otimes B}\,\otimes}{\vdash A^\perp, B^\perp, (A \otimes B) \oplus (A \otimes C)}\,\oplus_1 \quad \dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax} \quad \dfrac{}{\vdash C^\perp, C}\,\text{ax}}{\vdash A^\perp, C^\perp, A \otimes C}\,\otimes}{\vdash A^\perp, B^\perp, (A \otimes B) \oplus (A \otimes C)}\,\oplus_2}{\dfrac{\vdash A^\perp, B^\perp \,\&\, C^\perp, (A \otimes B) \oplus (A \otimes C)}{\vdash A^\perp \parr (B^\perp \,\&\, C^\perp), (A \otimes B) \oplus (A \otimes C)}\,\parr}\,\&$$

Hence $A \otimes (B \oplus C) \multimap (A \otimes B) \oplus (A \otimes C)$,
equivalently $(A^\perp \parr B^\perp) \,\&\, (A^\perp \parr C^\perp) \multimap A^\perp \parr (B^\perp \,\&\, C^\perp)$.

Example: distributivity of $\otimes$ over $\oplus$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax} \qquad \dfrac{\dfrac{}{\vdash B^\perp, B}\,\text{ax}}{\vdash B^\perp, B \oplus C}\,\oplus_1}{\vdash A^\perp, B^\perp, A \otimes (B \oplus C)}\,\otimes}{\vdash A^\perp \parr B^\perp, A \otimes (B \oplus C)}\,\parr \qquad \dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax} \qquad \dfrac{\dfrac{}{\vdash C^\perp, C}\,\text{ax}}{\vdash C^\perp, B \oplus C}\,\oplus_1}{\vdash A^\perp, C^\perp, A \otimes (B \oplus C)}\,\otimes}{\vdash A^\perp \parr C^\perp, A \otimes (B \oplus C)}\,\parr}{\vdash (A^\perp \parr B^\perp) \,\&\, (A^\perp \parr C^\perp), A \otimes (B \oplus C)}\,\&$$

Hence $(A \otimes B) \oplus (A \otimes C) \multimap A \otimes (B \oplus C)$,
equivalently $A^\perp \parr (B^\perp \,\&\, C^\perp) \multimap (A^\perp \parr B^\perp) \,\&\, (A^\perp \parr C^\perp)$.

Exponentials

Contraction and weakening are crucial for logical expressiveness.
Linear logic provides them through *modalities*.

- Allowed structural rules:

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, ?A}\,? \qquad \frac{\vdash \Gamma}{\vdash \Gamma, ?A}\,\mathrm{w} \qquad \frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A}\,\mathrm{c}$$

- Promotion:

$$\frac{\vdash ?A_1, \ldots, ?A_n, B}{\vdash ?A_1, \ldots, ?A_n, !B}\,!$$

Idea:

- $?A$ means "A some number of times"
- $!A$ means "as many A as necessary"

Exponentials – equivalences

- Wrong but not too much:

$$?A = \bigoplus_{n=0}^{\infty} \bigparr_{i=1}^{n} A, \qquad !A = \bigwith_{n=0}^{\infty} \bigotimes_{i=1}^{n} A.$$

- A bit less wrong:

$$?A = \bigparr_{n=0}^{\infty} (A \oplus \bot), \qquad !A = \bigotimes_{n=0}^{\infty} (A \,\&\, 1).$$

- Actually true:

$$!(A \,\&\, B) \multimapboth\, !A \otimes !B$$

$$!A \otimes !A \multimapboth\, !A$$

$$!!A \multimapboth\, !A$$

$$!?!?A \multimapboth\, !?A$$

Fragments

Many *fragments* are interesting:

- (possibly) restrict the set of formulas
- restrict the rules to allowed formulas
- (possibly) further restrict the set of rules

For instance:

- MLL = multiplicative = keep only $\otimes$ and $⅋$
- MELL = multiplicative-exponential = remove additives
- MALL = multiplicative-additive = remove exponentials
- ILL = "intuitionistic" = two-sided, one formula on the right
- focalized = *more on this later*
- polarized = *more on this later*
- LJ, LK = *more on this later*

Plan

The proof-program correspondence

Linear sequent calculus

A bit of semantics
- Cut elimination and consistency
- Provability semantics
- Proof semantics in coherence spaces

A bit of proof theory

Proof nets

The question of consistency

We have a definition of formulas, sequents and deduction rules. But how do we know if the system is consistent?

The question of consistency

We have a definition of formulas, sequents and deduction rules. But how do we know if the system is consistent?

- Provability in LK is preserved through translations.
  This is a good hint but it doesn't say much of LL!

The question of consistency

We have a definition of formulas, sequents and deduction rules. But how do we know if the system is consistent?

- Provability in LK is preserved through translations.
  This is a good hint but it doesn't say much of LL!
- LL has a model in coherent spaces, of course.
  But this does not inform us on the possibilities of the system.

The question of consistency

We have a definition of formulas, sequents and deduction rules. But how do we know if the system is consistent?

- Provability in LK is preserved through translations.
  This is a good hint but it doesn't say much of LL!
- LL has a model in coherent spaces, of course.
  But this does not inform us on the possibilities of the system.
- Use the argument sequent calculus was built for:

  Cut elimination.

Consistency by cut elimination

Theorem (Admissibility of cut)

A sequent is provable if and only if it is provable without the cut rule.

Corollary (Consistency)

The empty sequent $\vdash$ is not provable.

Proof.

All rules except cut have at least one formula in conclusion. □

Hence you cannot prove both A and $A^\perp$.

Cut elimination

- Define reduction rules over proofs that locally eliminate cuts.
- Prove well-foundedness of the reduction relation.
- Prove that irreducible proofs are cut-free.
- Conclude.

Tensor versus par

$$\dfrac{\dfrac{\overset{\pi_1}{\vdash \Gamma, A} \qquad \overset{\pi_2}{\vdash \Delta, B}}{\vdash \Gamma, \Delta, A \otimes B}\otimes \qquad \dfrac{\overset{\pi_3}{\vdash \Theta, A^\perp, B^\perp}}{\vdash \Theta, A^\perp \parr B^\perp}\parr}{\vdash \Gamma, \Delta, \Theta}\text{cut}$$

$$\searrow$$

$$\dfrac{\overset{\pi_1}{\vdash \Gamma, A} \qquad \dfrac{\overset{\pi_2}{\vdash \Delta, B} \qquad \overset{\pi_3}{\vdash \Theta, A^\perp, B^\perp}}{\vdash \Delta, \Theta, A^\perp}\text{cut}}{\vdash \Gamma, \Delta, \Theta}\text{cut}$$

With versus plus

$$\dfrac{\dfrac{\overset{\pi_1}{\vdash \Gamma, A} \qquad \overset{\pi_2}{\vdash \Gamma, B}}{\vdash \Gamma, A \mathbin{\&} B}\,\& \qquad \dfrac{\overset{\pi_3}{\vdash \Delta, A^\perp}}{\vdash \Delta, A^\perp \oplus B^\perp}\,\oplus_1}{\vdash \Gamma, \Delta}\,\text{cut}$$

$$\searrow$$

$$\dfrac{\overset{\pi_1}{\vdash \Gamma, A} \qquad \overset{\pi_3}{\vdash \Delta, A^\perp}}{\vdash \Gamma, \Delta}\,\text{cut}$$

Promotion versus contraction

$$\dfrac{\dfrac{\overset{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\,! \qquad \dfrac{\overset{\pi_2}{\vdash \Delta, ?A^\perp, ?A^\perp}}{\vdash \Delta, ?A^\perp}\,\mathrm{c}}{\vdash ?\Gamma, \Delta}\,\mathrm{cut}$$

$$\searrow$$

$$\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\,! \qquad \dfrac{\dfrac{\overset{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\,! \qquad \overset{\pi_2}{\vdash \Delta, ?A^\perp, ?A^\perp}}{\vdash ?\Gamma, \Delta, ?A^\perp}\,\mathrm{cut}}{\vdash ?\Gamma, ?\Gamma, \Delta}\,\mathrm{cut}}{\vdash ?\Gamma, \Delta}\,\mathrm{c}$$

... plus a few other *cancellation* rules ...

left	right	action
$\otimes$	$⅋$	propagate the cuts to sub-formulas
1	$\bot$	drop the proof of 1
$\oplus_1$	$\&$	keep only the left proof in the & rule
$\oplus_2$	$\&$	keep only the right proof in the & rule
!	?	propagate the cut to the sub-formula
!	w	drop the proof from the promotion
!	c	duplicate the proof from the promotion
ax	anything	drop the axiom

Commutation with tensor

$$\dfrac{\dfrac{\overset{\pi_1}{\vdash \Gamma, A} \quad \overset{\pi_2}{\vdash \Delta, B, C}}{\vdash \Gamma, \Delta, A \otimes B, C}\otimes \quad \overset{\pi_3}{\vdash \Theta, C^\perp}}{\vdash \Gamma, \Delta, \Theta, A \otimes B}\text{cut}$$

$$\searrow$$

$$\dfrac{\overset{\pi_1}{\vdash \Gamma, A} \quad \dfrac{\overset{\pi_2}{\vdash \Delta, B, C} \quad \overset{\pi_3}{\vdash \Theta, C^\perp}}{\vdash \Delta, \Theta, B}\text{cut}}{\vdash \Gamma, \Delta, A \otimes B, C}\otimes$$

Commutation with "with"

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A, C} \quad \dfrac{\pi_2}{\vdash \Gamma, B, C}}{\vdash \Gamma, A \mathbin{\&} B, C}\,\& \qquad \dfrac{\pi_3}{\vdash \Delta, C^\perp}}{\vdash \Gamma, \Delta, A \mathbin{\&} B}\,\text{cut}$$

$$\searrow$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A, C} \quad \dfrac{\pi_3}{\vdash \Delta, C^\perp}}{\vdash \Gamma, \Delta, A}\,\text{cut} \qquad \dfrac{\dfrac{\pi_2}{\vdash \Gamma, B, C} \quad \dfrac{\pi_3}{\vdash \Delta, C^\perp}}{\vdash \Gamma, \Delta, B}\,\text{cut}}{\vdash \Gamma, \Delta, A \mathbin{\&} B}\,\&$$

... plus a lot more *commutation* rules ...

Normalization

With the right set of rules, clearly irreducible proofs are cut-free.
How to prove that reduction always terminates?

Normalization

With the right set of rules, clearly irreducible proofs are cut-free.
How to prove that reduction always terminates?

- Using a clever induction on formulas and proofs.
  Works only in the absence of second-order quantification.

Normalization

With the right set of rules, clearly irreducible proofs are cut-free.
How to prove that reduction always terminates?

- Using a clever induction on formulas and proofs.
  Works only in the absence of second-order quantification.
- Using reducibility candidates, like in system F.
  Lots of technical points to cope with, but it works.

Normalization

With the right set of rules, clearly irreducible proofs are cut-free.
How to prove that reduction always terminates?

- Using a clever induction on formulas and proofs.
  Works only in the absence of second-order quantification.
- Using reducibility candidates, like in system F.
  Lots of technical points to cope with, but it works.
- Indirectly through more tractable systems
  - polarized systems *... more on this in a minute*
  - proof nets *... more on this later*

The question of completeness

How do we know we are not missing some rules?

Theorem (Completeness)

If a formula A is satisfied in every interpretation, then $\vdash A$ is provable in LL.

But what is an interpretation?

The question of completeness

How do we know we are not missing some rules?

Theorem (Completeness)

If a formula A is satisfied in every interpretation, then $\vdash A$ is provable in LL.

But what is an interpretation?

We need a structure that plays in LL the role of Boolean algebras in LK.

Phase spaces

Definition

A *phase space* is a pair $(M, \bot)$ where M is a commutative monoid and $\bot$ is a subset of M.

- points of M are tests/interactions/processes...
- elements of $\bot$ are *successful* tests, valid interactions...
  $\bot$ is the rule of the game

Definition

Two points $x, y \in M$ are *orthogonal* if $xy \in \bot$.
For $A \subseteq M$, let $A^\bot := \left\{ y \in M \;\middle|\; \forall x \in A, xy \in \bot \right\}$.
A *fact* is a set of the form $A^\bot$.

Exercise: Prove that $A \subseteq B$ implies $B^\bot \subseteq A^\bot$
and that $A \subseteq A^{\bot\bot}$ and $A^{\bot\bot\bot} = A^\bot$.

Facts play the role of truth values.

Given $(M, \perp)$, for subsets $A, B \subseteq M$ define

$$A \otimes B := \left\{ pq \,\middle|\, p \in A, q \in B \right\}^{\perp\perp} \qquad A \parr B := (A^\perp \otimes B^\perp)^\perp$$
$$A \oplus B := (A \cup B)^{\perp\perp} \qquad A \,\&\, B := A \cap B \qquad 0 := \varnothing^{\perp\perp} \qquad \top := M$$
$$!A := (A \cap I)^{\perp\perp} \qquad ?A := (A^\perp \cap I)^\perp \qquad 1 := \{1\}^{\perp\perp}$$

where I is the set of idempotents belonging to 1.

- If propositional variables are interpreted as facts, then for any formula A the interpretation $[\![A]\!]_M$ is a fact.
- $A \multimap B = A^\perp \parr B = \left\{ x \in M \,\middle|\, \forall y \in A, xy \in B \right\}$
- If $\perp = \varnothing$ then we get the elementary Boolean algebra $\{\varnothing, \top\}$.

Theorem (Soundness)

If $\vdash A$ is provable, then $1 \in [\![A]\!]_M$ in any phase space M.

Exercise: Check it by induction over proofs.

Theorem (Completeness)

If $1 \in [\![A]\!]_M$ in any phase space M, then $\vdash A$ is provable.

Proof.

Take for M the sequents (up to duplication of ? formulas) and for $\bot$ the provable ones. Check that $[\![A]\!]_M = \left\{\Gamma \,\middle|\, \vdash \Gamma, A \text{ is provable}\right\}$. The neutral element is the empty sequent so $\vdash A$ is provable. □

Coherence spaces: interpreting formulas

Linear logic was extracted from the notion of linearity observed when interpreting the λ-calculus in coherence spaces. It can itself be interpreted in coherence spaces:

Definition

- $\left|A^\perp\right| = |A|$ and $x \coh_{A^\perp} x'$ unless $x \scoh_A x'$.
- $|A \otimes B| = |A \parr B| = |A| \times |B|$ and
  - $(x, y) \coh_{A \otimes B} (x', y')$ if $x \coh_A x'$ and $y \coh_B y'$,
  - $(x, y) \scoh_{A \parr B} (x', y')$ if $x \scoh_A x'$ or $y \scoh_B y'$.
- $|A \oplus B| = |A \,\&\, B| = (\{1\} \times |A|) \cup (\{2\} \times |B|)$ and
  - $(i, x) \coh_{A \oplus B} (j, x')$ if $i = j$ and $x \coh x'$.
  - $(i, x) \coh_{A \& B} (j, x')$ if $i \neq j$ or $x \coh x'$.
- $|!A|$ is the set of finite cliques of A, $x \coh_{!A} x'$ if $x \cup x'$ is a clique in A.

where $x \scoh x'$ means $x \coh x'$ and $x \neq x'$.

Coherence spaces: interpreting proofs

Identity

$$\frac{}{\vdash \alpha : A^\perp, \alpha : A}\ \text{ax} \qquad \frac{\vdash \gamma : \Gamma, \alpha : A \qquad \vdash \alpha : A^\perp, \delta : \Delta}{\vdash \gamma : \Gamma, \delta : \Delta}\ \text{cut}$$

Multiplicatives

$$\frac{\vdash \gamma : \Gamma, \alpha : A \qquad \vdash \beta : B, \delta : \Delta}{\vdash \gamma : \Gamma, (\alpha, \beta) : A \otimes B, \delta : \Delta}\ \otimes \qquad \frac{\vdash \gamma : \Gamma, \alpha : A, \beta : B}{\vdash \gamma : \Gamma, (\alpha, \beta) : A \parr B}\ \parr$$

Coherence spaces: interpreting proofs

Identity

$$\frac{}{\vdash \alpha : A^{\perp}, \alpha : A}\ \text{ax} \qquad \frac{\vdash \gamma : \Gamma, \alpha : A \qquad \vdash \alpha : A^{\perp}, \delta : \Delta}{\vdash \gamma : \Gamma, \delta : \Delta}\ \text{cut}$$

Multiplicatives

$$\frac{\vdash \gamma : \Gamma, \alpha : A \qquad \vdash \beta : B, \delta : \Delta}{\vdash \gamma : \Gamma, (\alpha, \beta) : A \otimes B, \delta : \Delta}\ \otimes \qquad \frac{\vdash \gamma : \Gamma, \alpha : A, \beta : B}{\vdash \gamma : \Gamma, (\alpha, \beta) : A \parr B}\ \parr$$

Exponentials

$$\frac{\vdash \gamma : \Gamma, \alpha : A}{\vdash \gamma : \Gamma, \{\alpha\} : ?A}\ ? \qquad \frac{\vdash \gamma : \Gamma}{\vdash \gamma : \Gamma, \varnothing : ?A}\ \text{w} \qquad \frac{\vdash \gamma : \Gamma, a : ?A, a' ?A}{\vdash \gamma : \Gamma, a \cup a' : ?A}\ \text{c}$$

$$\frac{\left\{\vdash a_{1,i} : ?A_1, \ldots a_{n,i} : ?A_n, b_i : B\right\}_{i \in I}}{\vdash \bigcup_{i \in I} a_{1,i} : ?A_1, \ldots \bigcup_{i \in I} a_n i : ?A_n, \{b_i \mid i \in I\} : !B}\ !$$

Coherence spaces: sanity check

Theorem

The set of tuples in the interpretation of a proof is always a clique.

Proof.

By a simple induction of proofs. □

Theorem

The interpretation of proofs in coherence spaces is invariant by cut elimination.

Proof.

By case analysis on the various cases of cut elimination. □

Plan

The proof-program correspondence

Linear sequent calculus

A bit of semantics

A bit of proof theory
- Intuitionistic and classical logics as fragments
- Cut elimination and proof equivalence
- Reversibility and focalization

Proof nets

LJ expressed in linear logic

Linear logic arises from the decomposition

$$A \Rightarrow B \qquad = \qquad !A \multimap B \qquad = \qquad ?A^\perp \parr B$$

Deduction rules can be translated accordingly:

$$\frac{\Gamma, A \vdash_{LJ} B}{\Gamma \vdash_{LJ} A \Rightarrow B} \quad \rightsquigarrow \quad \frac{\vdash \Gamma^*, ?(A^*)^\perp, B^*}{\vdash \Gamma^*, ?(A^*)^\perp \parr B^*}\ \parr$$

$$\frac{\Gamma \vdash_{LJ} A \Rightarrow B \qquad \Delta \vdash_{LJ} A}{\Gamma, \Delta \vdash_{LJ} B} \quad \rightsquigarrow \quad \frac{\vdash \Gamma^*, ?(A^*)^\perp \parr B^* \qquad \dfrac{\dfrac{\vdash \Delta^*, A^*}{\vdash \Delta^*, !A^*}\ ! \qquad \dfrac{}{\vdash (B^*)^\perp, B^*}\ \text{ax}}{\vdash \Delta^*, !A \otimes (B^*)^\perp, B^*}\ \otimes}{\vdash \Gamma^*, \Delta^*, B^*}\ \text{cut}$$

The other connectives have adequate translations.

LK expressed in linear logic

Classical sequents have the shape

$$A_1, \ldots, A_n \vdash B_1, \ldots, B_p$$

with contraction and weakening allowed on both sides.
This suggests translating $A \Rightarrow B$ into something like $!A \multimap ?B$.
This does not work, but $!A \multimap ?!B$ and $!?A \multimap ?B$ do work.

Theorem

A sequent is provable in classical sequent calculus if and only if its translation in linear logic, by any of the above translations, is provable.

- LK proofs are translated into LL proofs,
- mapping linear connectives to classical ones is the reverse translation.

Exercise: Prove that in more detail.

LK as two fragments?

There are two families of translations:

- "left-handed": $!?A \multimap ?B$
  the associated reduction for λ-calculus is call by name
- "right-handed": $!A \multimap ?!B$
  the associated reduction for λ-calculus is call by value

More precise study of control operators is possible along these lines.

Cut-elimination as computation

Let us look again at cut elimination.

It is a computational process for turning arbitrary proofs into cut-free *canonical* proofs:

- cut-free proofs are like *values*,
- a proof of $A \multimap B$ maps *values* of A to *values* of B,
- equivalence modulo cut-elimination implies semantic equality.

Incidentally, it decomposes the reduction of the λ-calculus.

It turns arbitrary proofs into *explicit*, *direct* proofs:

- subformula property,
- mechanical proof search is possible.

In the absence of second-order quantification.

Consider possible cut-free proofs of $A \oplus (B \otimes C) \multimap A \oplus (B \otimes C)$.

$$\dfrac{}{\vdash A^\perp \mathbin{\&} (B^\perp \parr C^\perp), A \oplus (B \otimes C)}\ \text{ax}$$

Consider possible cut-free proofs of $A \oplus (B \otimes C) \multimap A \oplus (B \otimes C)$.

$$\dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax}}{\vdash A^\perp, A \oplus (B \otimes C)}\,\oplus_1 \qquad \dfrac{\dfrac{}{\vdash B^\perp \parr C^\perp, B \otimes C}\,\text{ax}}{\vdash B^\perp \parr C^\perp, A \oplus (B \otimes C)}\,\oplus_2}{\vdash A^\perp \mathbin{\&} (B^\perp \parr C^\perp), A \oplus (B \otimes C)}\,\&$$

Type isomorphisms

Technical aside: η-equivalence

Consider possible cut-free proofs of $A \oplus (B \otimes C) \multimap A \oplus (B \otimes C)$.

$$
\dfrac{
  \dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax}}{\vdash A^\perp, A \oplus (B \otimes C)}\,\oplus_1
  \qquad
  \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash B^\perp, B}\,\text{ax} \quad \dfrac{}{\vdash C^\perp, C}\,\text{ax}}{\vdash B^\perp, C^\perp, B \otimes C}\,\otimes}{\vdash B^\perp \parr C^\perp, B \otimes C}\,\parr}{\vdash B^\perp \parr C^\perp, A \oplus (B \otimes C)}\,\oplus_2
}{\vdash A^\perp \mathbin{\&} (B^\perp \parr C^\perp), A \oplus (B \otimes C)}\,\&
$$

Type isomorphisms

Technical aside: η-equivalence

Consider possible cut-free proofs of $A \oplus (B \otimes C) \multimap A \oplus (B \otimes C)$.

$$
\dfrac{
  \dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax}}{\vdash A^\perp, A \oplus (B \otimes C)}\,\oplus_1
  \qquad
  \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash B^\perp, B}\,\text{ax} \quad \dfrac{}{\vdash C^\perp, C}\,\text{ax}}{\vdash B^\perp, C^\perp, B \otimes C}\,\otimes}{\vdash B^\perp \parr C^\perp, B \otimes C}\,\parr}{\vdash B^\perp \parr C^\perp, A \oplus (B \otimes C)}\,\oplus_2
}{\vdash A^\perp \,\&\, (B^\perp \parr C^\perp), A \oplus (B \otimes C)}\,\&
$$

We will consider these proofs as equivalent.
This is the LL version of η-equivalence in the λ-calculus: $t \simeq_\eta \lambda x.(t)x$.

Type isomorphisms

Definition

Two formulas A and B are *isomorphic* if

- there are proofs $\pi \vdash A^\perp, B$ and $\rho \vdash B^\perp, A$
- π cut with ρ on A is equivalent to the axiom on B
- π cut with ρ on B is equivalent to the axiom on A

This implies isomorphism in any model.

These equivalences are isomorphisms:

$$A \otimes B \simeq B \otimes A \qquad A \otimes (B \oplus C) \simeq (A \otimes B) \oplus (A \otimes C) \qquad !(A \,\&\, B) \simeq\, !A \otimes !B$$

Exercise: Prove it!

These are not:

$$A \oplus A \multimap\!\circ\; A \qquad !A \otimes !A \multimap\!\circ\; !A \qquad !!A \multimap\!\circ\; !A \qquad !?!?A \multimap\!\circ\; !?A$$

Exercise: Explain why!

Standard isomorphisms

- Remark that $A \simeq B$ iff $A^\perp \simeq B^\perp$.
- Associativity and commutativity

$$(A \oplus B) \oplus C \simeq A \oplus (B \oplus C) \qquad (A \otimes B) \otimes C \simeq A \otimes (B \otimes C)$$
$$A \oplus B \simeq B \oplus A \qquad A \oplus B \simeq B \oplus A$$
$$A \oplus 0 \simeq A \qquad A \otimes 1 \simeq A$$

- Distributivity

$$A \otimes (B \oplus C) \simeq (A \otimes B) \oplus (A \otimes C) \qquad A \otimes 0 \simeq 0$$

- Exponentiation

$$!(A \,\&\, B) \simeq\, !A \otimes !B \qquad !\top \simeq 1$$

Reversibility

The rules for $\parr$ and & are reversible, i.e.

- $\vdash \Gamma, A \parr B$ is provable iff $\vdash \Gamma, A, B$ is provable,
- $\vdash \Gamma, A \& B$ is provable iff $\vdash \Gamma, A$ and $\vdash \Gamma, B$ are provable,

i.e. one can always assume that the introduction rule for a $\parr$ or for a & comes last.

Moreover:

- this can be proved directly using only permutations of rules
- moving these rules down does not change the behaviour of the proofs w.r.t. cut-elimination

$\parr$, &, $\bot$, $\top$ are called *negative*.

Focalization

Definition

A formula is *positive* if its main connective is $\otimes$, $\oplus$, 1, 0 or $!$.
It is *negative* if its main connective is $\parr$, $\&$, $\bot$, $\top$ or $?$.

Let $\Gamma = P_1, \ldots, P_n$ be a provable sequent consisting of positive formulas only. Then there is a formula P_i and proof of $\vdash \Gamma$ of the form

$$\dfrac{\begin{matrix}\pi_1 \\ \vdash \Gamma_1, N_1\end{matrix} \qquad \ldots \qquad \begin{matrix}\pi_k \\ \vdash \Gamma_k, N_k\end{matrix}}{\vdash \Gamma_1, \ldots, \Gamma_k, P_i}\ R$$

where the N_j are the maximal negative subformulas of P_i and the last set of rules R builds P_i from the N_j.

Synthetic connectives

Let $\Phi(X_1, \ldots, X_n)$ be a formula made of positive connectives from the variables $X_1, \ldots, X_n$. Call Φ^* the dual of Φ.

- Up to associativity/commutativity/neutrality, for some set $\mathscr{I} \subseteq \mathscr{P}(\{1, \ldots, n\})$ one has

$$\Phi(X_1, \ldots, X_n) \simeq \bigoplus_{I \in \mathscr{I}} \bigotimes_{i \in I} X_i \qquad \Phi^*(X_1, \ldots, X_n) \simeq \&_{I \in \mathscr{I}} \mathop{⅋}_{i \in I} X_i$$

- There is one family of rules

$$\frac{\left(\vdash \Gamma_i, A_i\right)_{i \in I}}{\vdash (\Gamma_i)_{i \in I}, \Phi(A_1, \ldots, A_n)}\ \Phi_I \qquad \frac{\left(\vdash \Gamma, (A_i)_{i \in I}\right)_{I \in \mathscr{I}}}{\vdash \Gamma, \Phi^*(A_1, \ldots, A_n)}\ \Phi^*$$

- Any provable sequent using Φ and Φ^* can be proved with these rules without decomposing Φ and Φ^*.

Push this further and you get ludics...

Polarized linear logic

Since connectives of the same polarity behave well, let us restrict to a system where polarities are never mixed:

$$P, Q := \alpha,\ \ P \otimes Q,\ \ P \oplus Q,\ \ 1,\ \ 0,\ \ !N$$
$$M, N := \alpha^\perp,\ \ M \parr N,\ \ M \mathbin{\&} N,\ \ \bot,\ \ \top,\ \ ?P$$

- If P is a positive formula where variables only appear under modalities, then $P \multimap !P$ is provable.
- Hence the following rules are derivable:

$$\frac{\vdash \Gamma}{\vdash \Gamma, N}\ \mathsf{W} \qquad \frac{\vdash \Gamma, N, N}{\vdash \Gamma, N}\ \mathsf{C} \qquad \frac{\vdash N_1, \dots, N_n, N}{\vdash N_1, \dots, N_n, !N}\ !$$

- Any provable polarized sequent has at most one positive formula (assuming the $\top$ rule respects this as a constraint).

Push this further and you get LLP...

Plan

The proof-program correspondence

Linear sequent calculus

A bit of semantics

A bit of proof theory

Proof nets

- Intuitionistic LL and natural deduction
- Proof structures
- Correctness criteria

Proof nets

Why would we need another formalism for proofs?

- Cut elimination in LL requires a lot of commutation rules
  as in other sequent calculi,
- Proofs that differ only by commutation are equivalent w.r.t. cut elimination.

On the other hand:

- Normalization in the λ-calculus only has one rule
  unless we use explicit substitutions,
- There are *separation results.*

We would like a natural deduction for LL.

Intuitionistic LL

The λ-calculus is simpler because it is asymmetric.
What if we made LL asymmetric too?

The λ-calculus is simpler because it is asymmetric.
What if we made LL asymmetric too?

Definition (Formulas of MILL)

$$
\begin{aligned}
A, B := {} & \alpha && \text{propositional variable} \\
& A \multimap B && \text{linear implication} \\
& A \otimes B && \text{multiplicative conjunction}
\end{aligned}
$$

Intuitionistic LL

The λ-calculus is simpler because it is asymmetric.
What if we made LL asymmetric too?

Definition (Formulas of MILL)

$A, B := \alpha$	propositional variable
$A \multimap B$	linear implication
$A \otimes B$	multiplicative conjunction

Definition (Proof terms for MILL)

$t, u := x$	variable — axiom
$\lambda x.t$	linear abstraction — introduction of $\multimap$
$(t)u$	linear application — elimination of $\multimap$
(t, u)	pair — introduction of $\otimes$
$t(x,y{:=}u)$	matching — elimination of $\otimes$

Identity

$$\frac{}{x : A \vdash x : A}\ \text{ax}$$

Implication

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \multimap B}\ {\multimap}\text{R} \qquad \frac{\Gamma \vdash t : A \multimap B \quad \Delta \vdash u : A}{\Gamma, \Delta \vdash (t)u : B}\ {\multimap}\text{E}$$

Tensor

$$\frac{\Gamma \vdash t : A \quad \Delta \vdash u : B}{\Gamma, \Delta \vdash (t, u) : A \otimes B}\ \otimes\text{R} \qquad \frac{\Gamma, x : A, y : B \vdash t : C \quad \Delta \vdash u : A \otimes B}{\Gamma, \Delta \vdash t(x,y{:=}u) : C}\ \otimes\text{E}$$

No contraction or weakening, of course.

MILL – reduction

Definition

Cut elimination for MILL is generated by the following rules:

$$(\lambda x.t)u \rightsquigarrow t[u/x] \qquad t(x,y{:=}(u,v)) \rightsquigarrow t[u/x][v/y]$$

MILL – reduction

Definition

Cut elimination for MILL is generated by the following rules:

$$(\lambda x.t)u \rightsquigarrow t[u/x] \qquad t(x{,}y{:=}(u,v)) \rightsquigarrow t[u/x][v/y]$$

Theorem

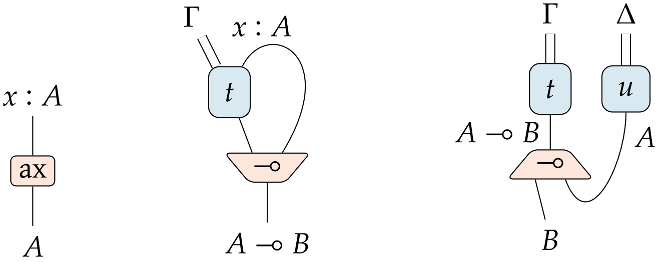
Cut elimination in MILL computes a unique normal form for every proof.

Subject reduction: straightforward.

Strong normalization: each step decreases the number of typing rules.

Confluence: MILL is *strongly* confluent.

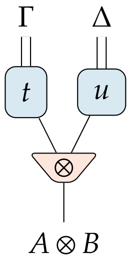
Linearity makes things simpler than in the λ-calculus.



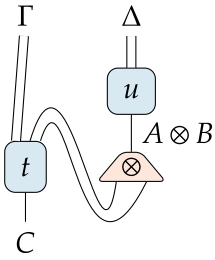
x $\lambda x.t$ $(t)u$

MILL – a graphical notation

Tensor



(t, u)



$t(x,y{:=}u)$

The substitution lemma

Lemma

$$\frac{\Gamma, x : A \vdash t : B \qquad \Delta \vdash u : A}{\Gamma, \Delta \vdash t[u/x] : B} \quad \textit{if } \Gamma \textit{ and } \Delta \textit{ have disjoint domains.}$$

The substitution lemma

Lemma

$$\frac{\Gamma, x : A \vdash t : B \qquad \Delta \vdash u : A}{\Gamma, \Delta \vdash t[u/x] : B} \qquad \text{if } \Gamma \text{ and } \Delta \text{ have disjoint domains.}$$

The cut rule is admissible.

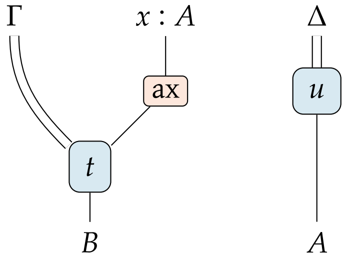
The substitution lemma

Lemma

$$\frac{\Gamma, x : A \vdash t : B \qquad \Delta \vdash u : A}{\Gamma, \Delta \vdash t[u/x] : B}$$

if Γ *and* Δ *have disjoint domains.*

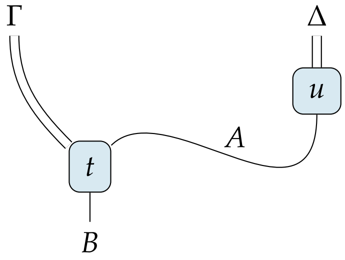
The cut rule is admissible.
Graphically:



Lemma

$$\frac{\Gamma, x : A \vdash t : B \qquad \Delta \vdash u : A}{\Gamma, \Delta \vdash t[u/x] : B}$$ *if* Γ *and* Δ *have disjoint domains.*

The cut rule is admissible.
Graphically:

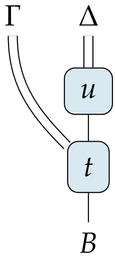


The substitution lemma

Lemma

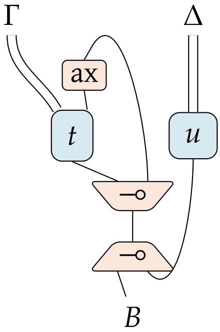
$$\frac{\Gamma, x : A \vdash t : B \qquad \Delta \vdash u : A}{\Gamma, \Delta \vdash t[u/x] : B}$$ *if* Γ *and* Δ *have disjoint domains.*

The cut rule is admissible.
Graphically:



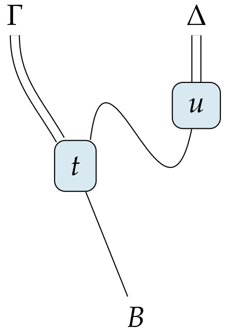
MILL – graphical cut elimination

Linear implication



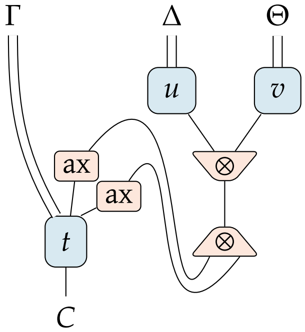
MILL – graphical cut elimination

Linear implication



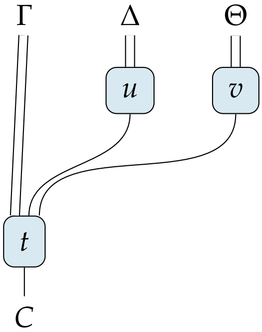
MILL – graphical cut elimination

Tensor



MILL – graphical cut elimination

Tensor



Proof structures

We extend the graphical formalism to MLL sequent calculus.

1. Allow several formulas on the right hand side of sequents.
   $\Rightarrow$ arbitrary number of outputs

Proof structures

We extend the graphical formalism to MLL sequent calculus.

1. Allow several formulas on the right hand side of sequents.
   $\Rightarrow$ arbitrary number of outputs
2. Reintroduce negation
   $\Rightarrow$ transform a hypothesis into a conclusion and vice versa

Proof structures

We extend the graphical formalism to MLL sequent calculus.

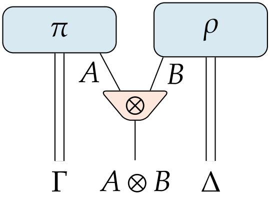
1. Allow several formulas on the right hand side of sequents.
   $\Rightarrow$ arbitrary number of outputs
2. Reintroduce negation
   $\Rightarrow$ transform a hypothesis into a conclusion and vice versa
3. Hard-wire De Morgan duality
   $\Rightarrow$ negation is again an operation on formulas and sequents

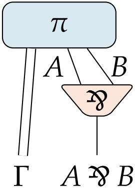
Proof structures

We extend the graphical formalism to MLL sequent calculus.

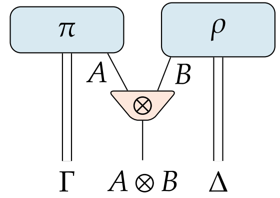
1. Allow several formulas on the right hand side of sequents.
   $\Rightarrow$ arbitrary number of outputs
2. Reintroduce negation
   $\Rightarrow$ transform a hypothesis into a conclusion and vice versa
3. Hard-wire De Morgan duality
   $\Rightarrow$ negation is again an operation on formulas and sequents
4. Forget about inputs.

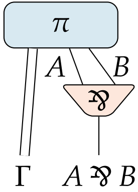
Proof structures – MLL proofs

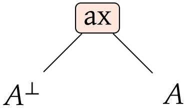


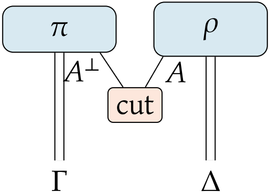


Proof structures – MLL proofs







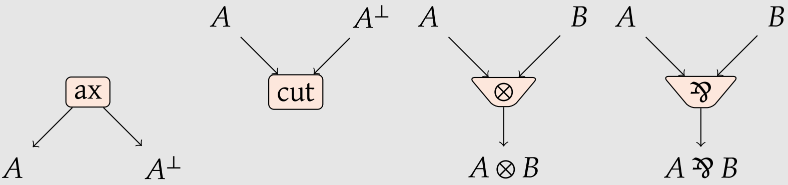


Proof structures – a definition

Definition

An MLL proof structure is a directed multigraph

- with edges labelled by MLL formulas and nodes labelled by rule names or the symbol "c",
- with a total order on incoming and outgoing edges on each node,
- where nodes have one of these shapes:

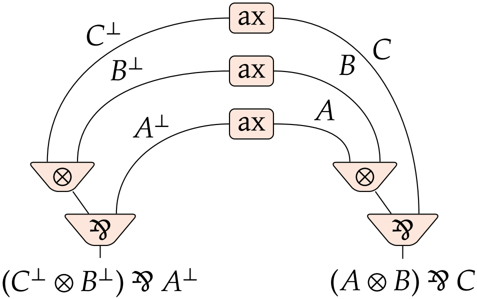


The nodes labeled "c" are called the *conclusions* of the structure.

Proof structures – an example

Rule commutations are ignored

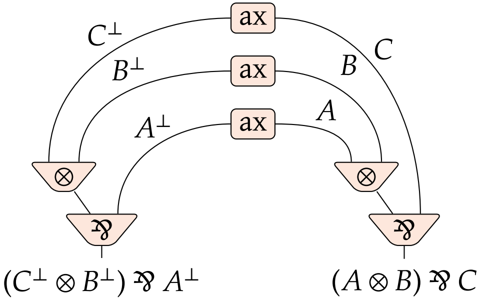
$$
\dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax} \qquad \dfrac{\dfrac{}{\vdash C^\perp, C}\,\text{ax} \qquad \dfrac{}{\vdash B^\perp, B}\,\text{ax}}{\vdash C^\perp \otimes B^\perp, B, C}\,\otimes}{\dfrac{\vdash C^\perp \otimes B^\perp, A^\perp, A \otimes B, C}{\dfrac{\vdash C^\perp \otimes B^\perp, A^\perp, (A \otimes B) \parr C}{\vdash (C^\perp \otimes B^\perp) \parr A^\perp, (A \otimes B) \parr C}\,\parr}\,\parr}\,\otimes
$$



Proof structures – an example

Rule commutations are ignored

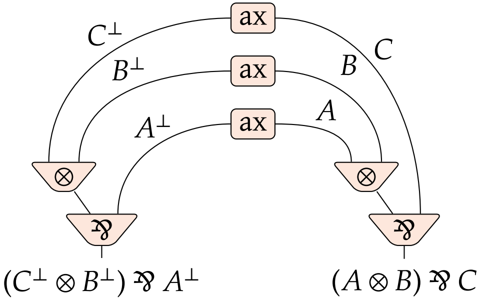
$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax} \qquad \dfrac{\dfrac{}{\vdash C^\perp, C}\,\text{ax} \quad \dfrac{}{\vdash B^\perp, B}\,\text{ax}}{\vdash C^\perp \otimes B^\perp, B, C}\,\otimes}{\vdash C^\perp \otimes B^\perp, A^\perp, A \otimes B, C}\,\otimes}{\vdash (C^\perp \otimes B^\perp) \parr A^\perp, A \otimes B, C}\,\parr}{\vdash (C^\perp \otimes B^\perp) \parr A^\perp, (A \otimes B) \parr C}\,\parr$$



Proof structures – an example

Rule commutations are ignored

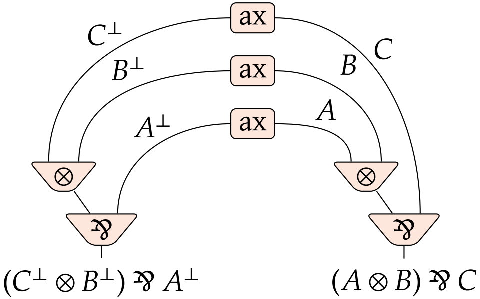
$$
\dfrac{\dfrac{\dfrac{}{\vdash C^{\perp}, C}\,\text{ax} \qquad \dfrac{\dfrac{}{\vdash A^{\perp}, A}\,\text{ax} \qquad \dfrac{}{\vdash B^{\perp}, B}\,\text{ax}}{\vdash B^{\perp}, A^{\perp}, A \otimes B}\,\otimes}{\dfrac{\vdash C^{\perp} \otimes B^{\perp}, A^{\perp}, A \otimes B, C}{\vdash C^{\perp} \otimes B^{\perp}, A^{\perp}, (A \otimes B) \parr C}\,\parr}\,\otimes}{\vdash (C^{\perp} \otimes B^{\perp}) \parr A^{\perp}, (A \otimes B) \parr C}\,\parr
$$



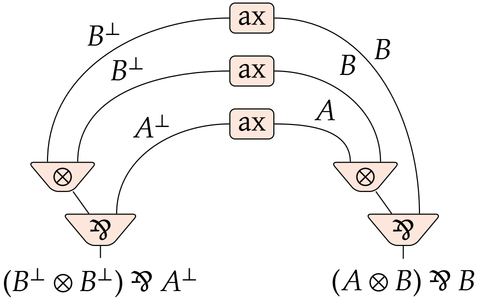
Proof structures – an example

Rule commutations are ignored

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash C^{\perp}, C}\,\text{ax} \qquad \dfrac{\dfrac{}{\vdash A^{\perp}, A}\,\text{ax} \quad \dfrac{}{\vdash B^{\perp}, B}\,\text{ax}}{\vdash B^{\perp}, A^{\perp}, A \otimes B}\,\otimes}{\vdash C^{\perp} \otimes B^{\perp}, A^{\perp}, A \otimes B, C}\,\otimes}{\vdash (C^{\perp} \otimes B^{\perp}) ⅋ A^{\perp}, A \otimes B, C}\,⅋}{\vdash (C^{\perp} \otimes B^{\perp}) ⅋ A^{\perp}, (A \otimes B) ⅋ C}\,⅋
$$



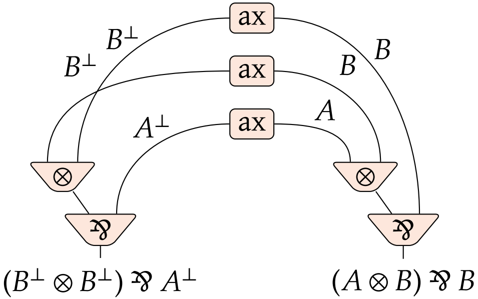
$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax} \quad \dfrac{\dfrac{}{\vdash B^\perp, B}\,\text{ax} \quad \dfrac{}{\vdash B^\perp, B}\,\text{ax}}{\vdash B^\perp \otimes B^\perp, B, B}\,\otimes}{\vdash B^\perp \otimes B^\perp, A^\perp, A \otimes B, B}\,\otimes}{\vdash B^\perp \otimes B^\perp, A^\perp, (A \otimes B) \parr B}\,\parr}{\vdash (B^\perp \otimes B^\perp) \parr A^\perp, (A \otimes B) \parr B}\,\parr$$



Proof structures – an example

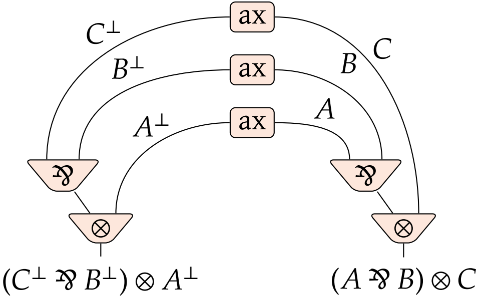
Not all proofs are identified

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax} \qquad \dfrac{\dfrac{}{\vdash B^\perp, B}\,\text{ax} \qquad \dfrac{}{\vdash B^\perp, B}\,\text{ax}}{\vdash B^\perp \otimes B^\perp, B, B}\,\otimes,\text{ex}}{\vdash B^\perp \otimes B^\perp, A^\perp, A \otimes B, B}\,\otimes}{\vdash B^\perp \otimes B^\perp, A^\perp, (A \otimes B) \parr B}\,\parr}{\vdash (B^\perp \otimes B^\perp) \parr A^\perp, (A \otimes B) \parr B}\,\parr$$



Correctness

Not all proof structures are translations of sequential proofs:



Indeed, the conclusion is not provable.

Proof nets

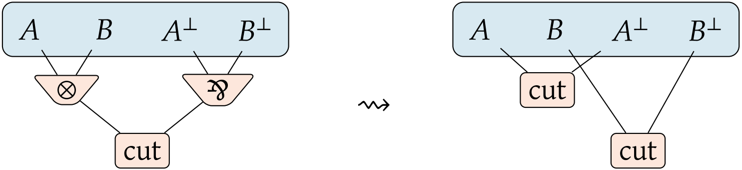
Definition

A proof net is a proof structure that is the translation of some sequential proof.

Exercise: Enumerate all the cut-free proof structures with conclusions $(A^{\perp} \otimes A^{\perp}) \parr A^{\perp}, (A \otimes A) \parr A$ and identify which ones are proof nets.

Cut elimination in proof structures

Tensor versus par:



Plus the same rules with the left and right premisses of the cut exchanged.

Cut elimination in proof structures

Axiom:

This assumes that the right premiss of the cut node is not the left conclusion of the axiom node.

Cut elimination in proof structures

Theorem (Strong normalization)

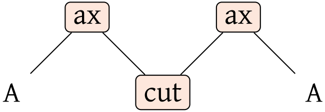
In any MLL proof structure, all maximal sequences of cut elimination steps are finite.

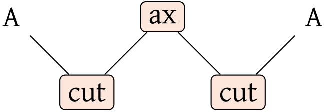
Each step decreases the number of nodes.

Theorem (Strong confluence)

They all have the same length and they all reach the same irreducible proof structure (up to graph isomorphism).

The only critical pairs are in these situations:





Correctness

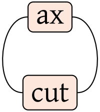
Theorem (Subject reduction)

Irreducible proof structures are cut free.

Correctness

Problem

Not all irreducible proof structures are cut free.



Related problem

How do we know that reducing a proof net gives a proof net?

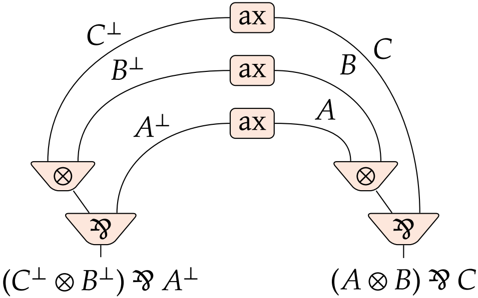
Correctness criteria

A correctness criterion is characterization of correct proofs among proof structures.

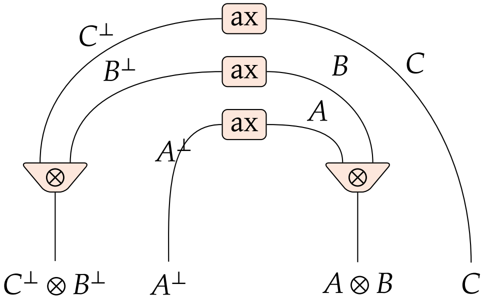
- It should be reasonably easy to prove that correctness is preserved by cut elimination.
- The complexity of actually computing whether a structure satisfies the criterion is directly related to the complexity of the decision problem for the considered logic.

Reversibility revisited

The ⅋ nodes in conclusion are irrelevant for correctness:

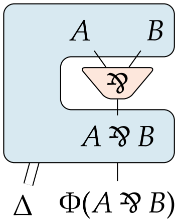


The ⅋ nodes in conclusion are irrelevant for correctness:



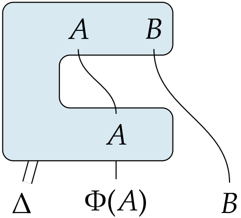
Switchings

The reversibility property can be applied even inside proofs:



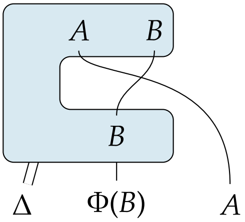
Switchings

The reversibility property can be applied even inside proofs:



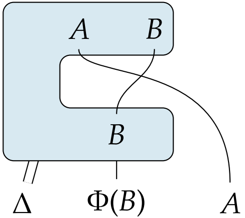
Switchings

The reversibility property can be applied even inside proofs:



Switchings

The reversibility property can be applied even inside proofs:



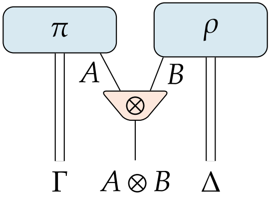
Lemma

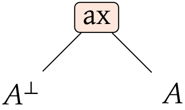
If π is a correct cut-free proof structure, then all its $\invamp$-switchings are correct.

Switchings

How can we recognize if a proof structure with only axioms and tensors is correct?

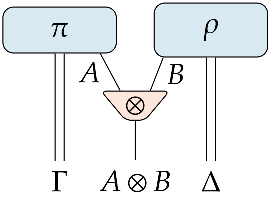
How can we recognize if a proof structure with only axioms and tensors is correct?

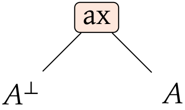




Switchings

How can we recognize if a proof structure with only axioms and tensors is correct?





Fact

The structures built using these rules are the acyclic and connected ones.

The DR criterion

Theorem (Danos-Regnier)

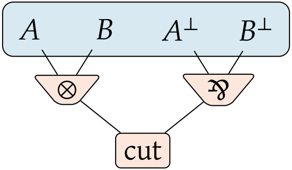
An MLL proof structure is sequentializable if and only if all its switchings are acyclic and connected.

- The “only if” part is essentially contained in the previous arguments.
- For the “if” part, the key point is to prove that the condition implies the existence of a splitting $\otimes$ node.

More on this tomorrow...

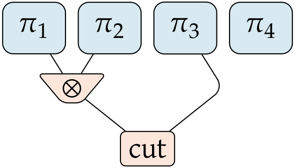
Cut elimination preserves correctness

Take a tensor/par cut.



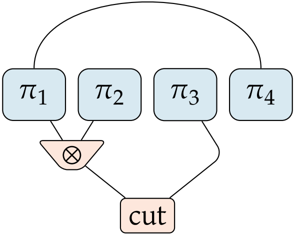
Cut elimination preserves correctness

Switch it.



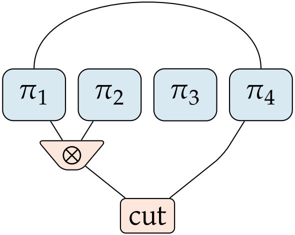
Cut elimination preserves correctness

It is connected.



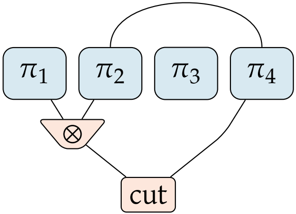
Cut elimination preserves correctness

It is connected and acyclic.



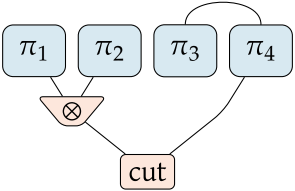
Cut elimination preserves correctness

It is connected and acyclic.



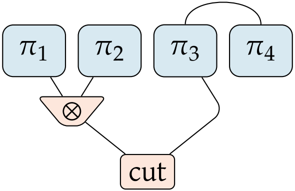
Cut elimination preserves correctness

It is connected and acyclic.



Cut elimination preserves correctness

It is connected and acyclic.



Cut elimination preserves correctness

Reduce the cut.