Multiplicative Linear Logic

Olivier Laurent

LIP, CNRS - ENS Lyon, France

LL2016, Lyon
school: 7 and 8 November 2016

Classical Formulas

Formulas

$$X \qquad \neg A \qquad A \wedge B \qquad A \vee B$$

De Morgan

$$\neg(\neg A) \equiv A$$
$$\neg(A \wedge B) \equiv \neg A \vee \neg B$$
$$\neg(A \vee B) \equiv \neg A \wedge \neg B$$

Distributivity

$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$
$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$$

From Formulas to Clauses

Negation Elimination

$$\begin{aligned} \neg(\neg A) &\mapsto A \\ \neg(A \wedge B) &\mapsto \neg A \vee \neg B \\ \neg(A \vee B) &\mapsto \neg A \wedge \neg B \end{aligned}$$

Distributivity

$$A \vee (B \wedge C) \mapsto (A \vee B) \wedge (A \vee C)$$

Conjunctive Normal Forms

$$\bigwedge \bigvee X / \neg X$$

i.e. conjunctions of clauses (*disjunctions of literals*)

Example: $(\neg X \vee Z \vee \neg Y) \wedge (\neg X \vee \neg Z) \wedge (\neg X \vee Z \vee \neg Y \vee Z \vee X)$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

- Simplify negations:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

- Simplify negations:

$$\neg X \vee \neg(Z \vee \neg Y) \vee (\neg Y \wedge X)$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

- Simplify negations:

$$\neg X \vee (\neg Z \wedge \neg\neg Y) \vee (\neg Y \wedge X)$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \land (Z \lor \neg Y)) \lor (\neg Y \land X)$$

- Simplify negations:

$$\neg X \lor (\neg Z \land Y) \lor (\neg Y \land X)$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \land (Z \lor \neg Y)) \lor (\neg Y \land X)$$

- Simplify negations:

$$\neg X \lor (\neg Z \land Y) \lor (\neg Y \land X)$$

- Distribute $\lor$ over $\land$:

$$\neg X \color{red}{\lor} (\neg Z \color{blue}{\land} Y) \lor (\neg Y \land X)$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

- Simplify negations:

$$\neg X \vee (\neg Z \wedge Y) \vee (\neg Y \wedge X)$$

- Distribute $\vee$ over $\wedge$:

$$((\neg X \vee \neg Z) \wedge (\neg X \vee Y)) \vee (\neg Y \wedge X)$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

- Simplify negations:

$$\neg X \vee (\neg Z \wedge Y) \vee (\neg Y \wedge X)$$

- Distribute $\vee$ over $\wedge$:

$$(\neg X \vee \neg Z \vee (\neg Y \wedge X)) \wedge (\neg X \vee Y \vee (\neg Y \wedge X))$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

- Simplify negations:

$$\neg X \vee (\neg Z \wedge Y) \vee (\neg Y \wedge X)$$

- Distribute $\vee$ over $\wedge$:

$$(\neg X \vee \neg Z \vee \neg Y) \wedge (\neg X \vee \neg Z \vee X) \wedge (\neg X \vee Y \vee (\neg Y \wedge X))$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

- Simplify negations:

$$\neg X \vee (\neg Z \wedge Y) \vee (\neg Y \wedge X)$$

- Distribute $\vee$ over $\wedge$:

$$(\neg X \vee \neg Z \vee \neg Y) \wedge (\neg X \vee \neg Z \vee X) \wedge (\neg X \vee Y \vee \neg Y) \wedge (\neg X \vee Y \vee X)$$

Proving with Clauses

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

- Simplify negations:

$$\neg X \vee (\neg Z \wedge Y) \vee (\neg Y \wedge X)$$

- Distribute $\vee$ over $\wedge$:

$$(\neg X \vee \neg Z \vee \neg Y) \wedge (\neg X \vee \neg Z \vee X) \wedge (\neg X \vee Y \vee \neg Y) \wedge (\neg X \vee Y \vee X)$$

- Obtained CNF seen as a set of clauses:

$$\neg X \vee \neg Z \vee \neg Y \qquad \neg X \vee \neg Z \vee X \qquad \neg X \vee Y \vee \neg Y \qquad \neg X \vee Y \vee X$$

- Look for pairs of dual literals in all clauses:

$$\neg X \vee \neg Z \vee \neg Y \qquad \neg X \vee \neg Z \vee X \qquad \neg X \vee Y \vee \neg Y \qquad \neg X \vee Y \vee X$$

Clauses in Sequent Calculus

- Start from an arbitrary formula:

$$\neg(X \wedge (Z \vee \neg Y)) \vee (\neg Y \wedge X)$$

- Simplify negations:

$$\neg X \vee (\neg Z \wedge Y) \vee (\neg Y \wedge X)$$

- Build a bottom-up proof in sequent calculus:

$$\dfrac{\dfrac{\dfrac{\dfrac{\color{red}{\vdash \neg X, \neg Z, \neg Y} \qquad \dfrac{}{\vdash \neg X, \neg Z, X}\,\color{green}{ax}}{\vdash \neg X, \neg Z, \neg Y \wedge X}\,\wedge \qquad \dfrac{\dfrac{}{\vdash \neg X, Y, \neg Y}\,\color{green}{ax} \qquad \dfrac{}{\vdash \neg X, Y, X}\,\color{green}{ax}}{\vdash \neg X, Y, \neg Y \wedge X}\,\wedge}{\vdash \neg X, \neg Z \wedge Y, \neg Y \wedge X}\,\wedge}{\vdash \neg X \vee (\neg Z \wedge Y), \neg Y \wedge X}\,\vee}{\vdash \neg X \vee (\neg Z \wedge Y) \vee (\neg Y \wedge X)}\,\vee$$

Remark: Each rule destructs one connective.

Linearity Analysis

Duplication

- in distributivity: $A \vee (B \wedge C) \mapsto (A \vee B) \wedge (A \vee C)$
- in the $\wedge$ rule: $\dfrac{\vdash A, B \qquad \vdash A, C}{\vdash A, B \wedge C} \wedge$

Erasure

- in clause solving: $X \vee Y \vee \neg Z \vee \neg Y$
- in the ax rule: $\dfrac{}{\vdash X, Y, \neg Z, \neg Y}$ ax

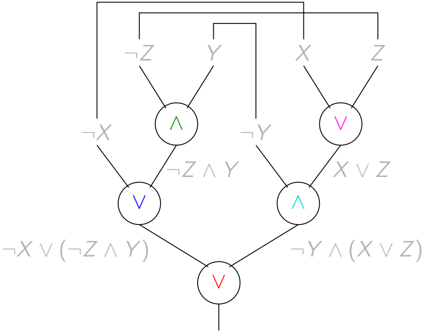
Towards a Linear Proof System

- Destruct connectives without duplication
- Look for dual pairs of literals

$$\dfrac{\dfrac{\neg X \qquad \dfrac{\neg Z \qquad Y}{\neg Z \wedge Y}}{\neg X \vee (\neg Z \wedge Y)} \qquad \dfrac{\neg Y \qquad \dfrac{X \qquad Z}{X \vee Z}}{\neg Y \wedge (X \vee Z)}}{(\neg X \vee (\neg Z \wedge Y)) \vee (\neg Y \wedge (X \vee Z))}$$

Towards a Linear Proof System

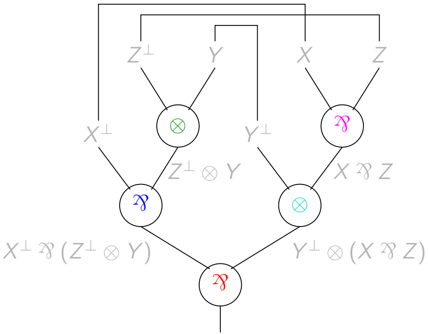
- Formula tree with pairs of leaves



$(\neg X \vee (\neg Z \wedge Y)) \vee (\neg Y \wedge (X \vee Z))$

Towards a Linear Proof System

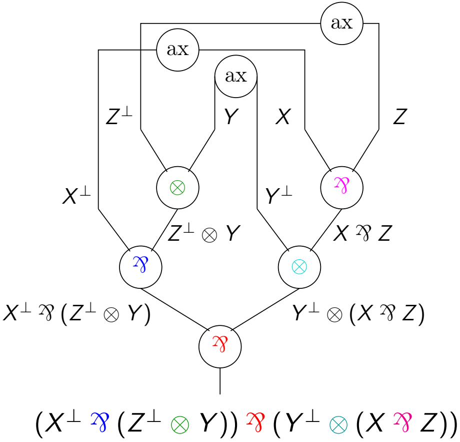
- Linear logic syntax



$$(X^\perp \parr (Z^\perp \otimes Y)) \parr (Y^\perp \otimes (X \parr Z))$$

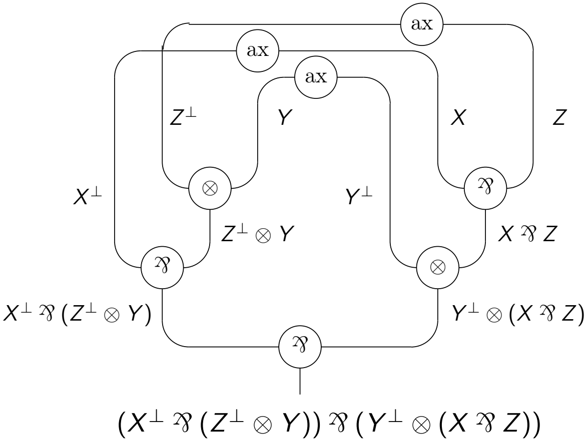
Towards a Linear Proof System

- A directed graph



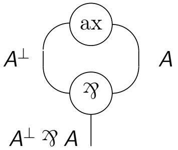
Towards a Linear Proof System

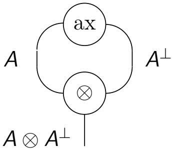
- A proof structure

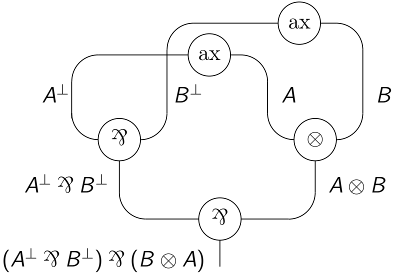


Proof Structures

examples

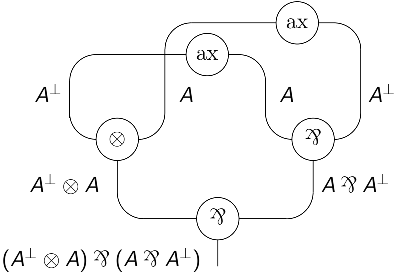






Proof Structures

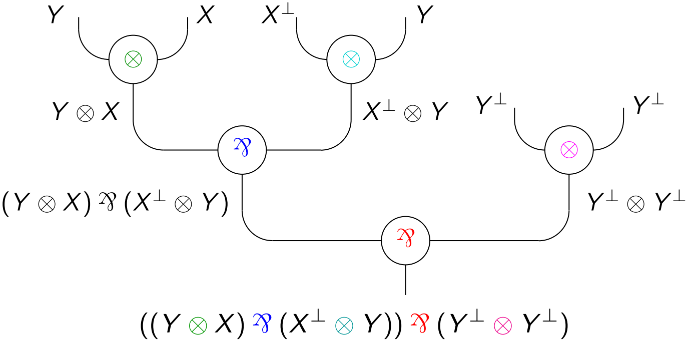
examples



Practice

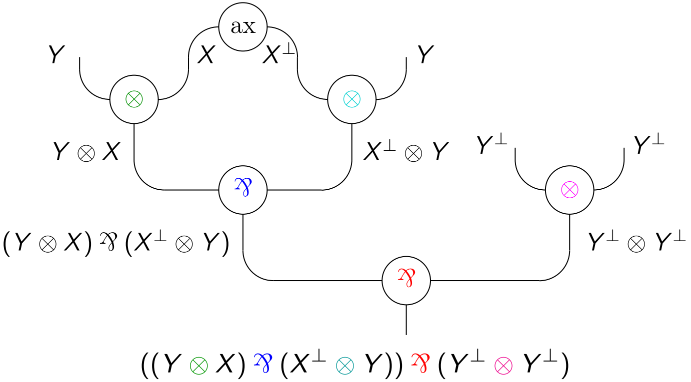
$$((Y \otimes X) \parr (X^{\perp} \otimes Y)) \parr (Y^{\perp} \otimes Y^{\perp})$$

Practice

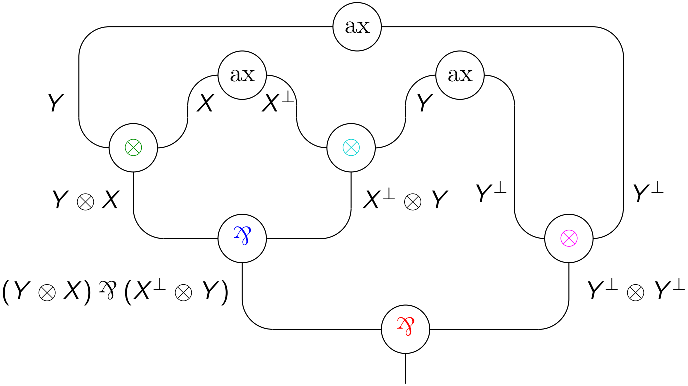


Y
X
$X^\perp$
Y
$\otimes$
$\otimes$
$Y \otimes X$
$X^\perp \otimes Y$
$Y^\perp$
$Y^\perp$
$\parr$
$\otimes$
$(Y \otimes X) \parr (X^\perp \otimes Y)$
$Y^\perp \otimes Y^\perp$
$\parr$
$((Y \otimes X) \parr (X^\perp \otimes Y)) \parr (Y^\perp \otimes Y^\perp)$

Practice


ax
Y
X
$X^\perp$
Y
$\otimes$
$\otimes$
$Y \otimes X$
$X^\perp \otimes Y$
$Y^\perp$
$Y^\perp$
$\parr$
$\otimes$
$(Y \otimes X) \parr (X^\perp \otimes Y)$
$Y^\perp \otimes Y^\perp$
$\parr$
$((Y \otimes X) \parr (X^\perp \otimes Y)) \parr (Y^\perp \otimes Y^\perp)$

Practice



$((Y \otimes X) ⅋ (X^\perp \otimes Y)) ⅋ (Y^\perp \otimes Y^\perp)$

Too Strong Proof System

More than Classical Logic

- $A \otimes A^{\perp}$
  while LK does not prove $\vdash A \wedge \neg A$
- $(X^{\perp} \parr (Z^{\perp} \otimes Y)) \parr (Y^{\perp} \otimes (X \parr Z))$
  while LK does not prove $\vdash (\neg X \vee (\neg Z \wedge Y)) \vee (\neg Y \wedge (X \vee Z))$

Weakness of Proof Structures

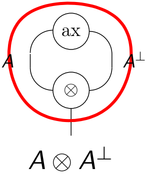
- A proof structure exists *iff* formula with balanced atoms
- No distinction between $\otimes$ and $\parr$ (*i.e.* $\wedge$ vs. $\vee$)

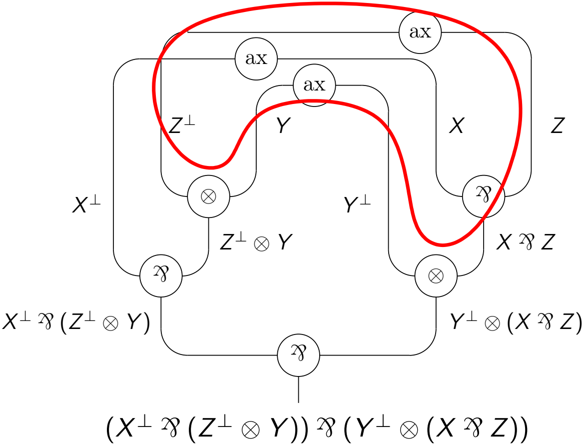
$\Longrightarrow$ Need for an additional condition on graphs.

Correctness Criterion

Cycles

- $\otimes$ is responsible for cyclic dependencies

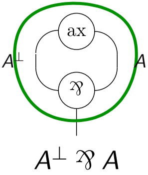




Correctness Criterion

Cycles

- $\otimes$ is responsible for cyclic dependencies
- Some cycles are good



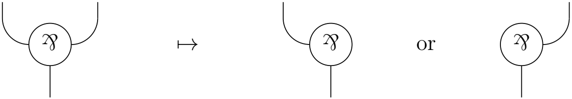
Correctness Criterion

Cycles

- $\otimes$ is responsible for cyclic dependencies
- Some cycles are good

A Criterion

- ⅋ is disjunctive: keep 1 premise only

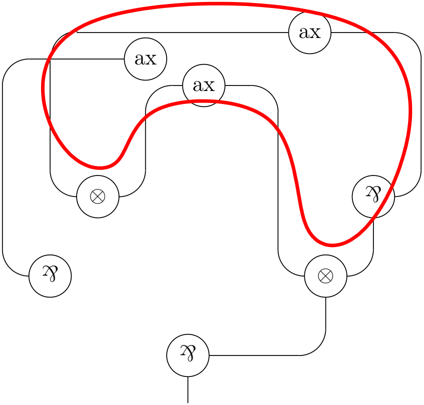


- $\otimes$ is conjunctive: keep both premises
- Every obtained (sub)graph must be acyclic and connected.

Remark: Correct proof structures are called proof nets.

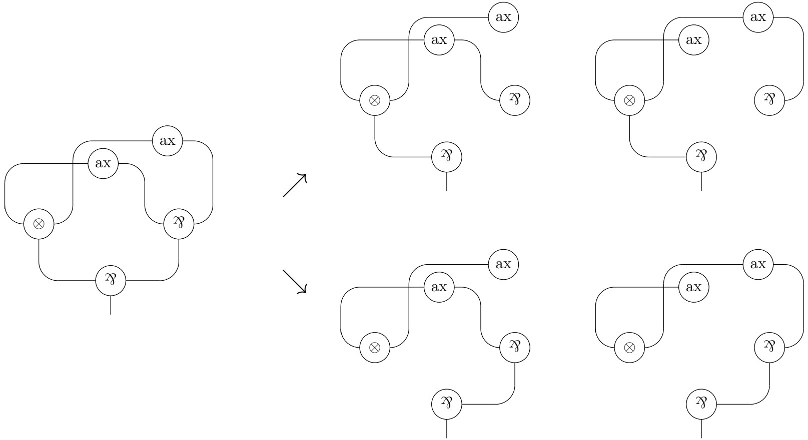
Correctness Criterion

examples



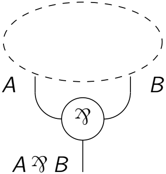
Correctness Criterion

examples



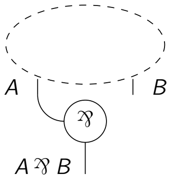
Multiple Conclusions

- Terminal $\parr$ has no impact on correctness:



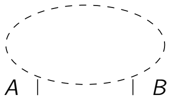
Multiple Conclusions

- Terminal ⅋ has no impact on correctness:



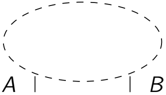
Multiple Conclusions

- Terminal $\parr$ has no impact on correctness:

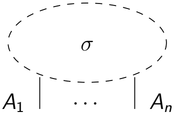


Multiple Conclusions

- Terminal $⅋$ has no impact on correctness:



- Extend proof structures for formulas
  to proof-structures for sequents $\vdash A_1, \ldots, A_n$:



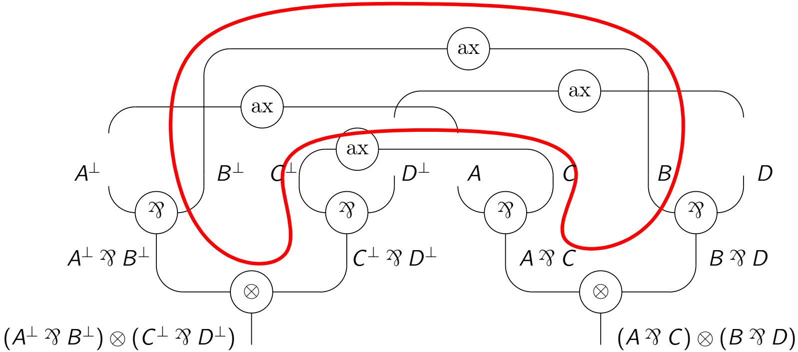
(*n conclusions*)

Linear Logic is not Linearized Classical Logic

$$\vdash (\neg A \vee \neg B) \wedge (\neg C \vee \neg D), (A \vee C) \wedge (B \vee D)$$

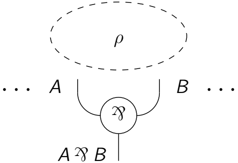
linear and provable in LK

but



From Proof Nets to Sequent Calculus

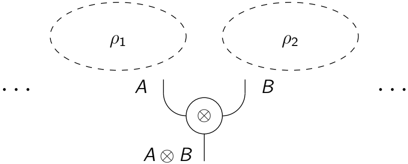
- ⅋ / disjunction / unary rule



$\mapsto$

$$\frac{\vdash \dots, A, B, \dots}{\vdash \dots, A \parr B, \dots}\ \parr$$

- $\otimes$ / conjunction / binary rule



$\mapsto$

$$\frac{\vdash \dots, A \qquad \vdash B, \dots}{\vdash \dots, A \otimes B, \dots}\ \otimes$$

The MLL Sequent Calculus

Formulas

$$X \qquad X^{\perp} \qquad A \otimes B \qquad A \parr B$$

Extended negation

$$(X^{\perp})^{\perp} := X$$
$$(A \otimes B)^{\perp} := A^{\perp} \parr B^{\perp}$$
$$(A \parr B)^{\perp} := A^{\perp} \otimes B^{\perp}$$

Sequents

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

Rules

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

(and permutation in sequents)

The MLL Sequent Calculus

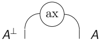
examples

$$\dfrac{\dfrac{}{\vdash A, A^\perp}\,\text{ax}}{\vdash A \parr A^\perp}\,\parr$$

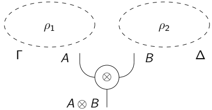
$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp}\,\text{ax} \qquad \dfrac{}{\vdash B, B^\perp}\,\text{ax}}{\vdash A, B, A^\perp \otimes B^\perp}\,\otimes}{\vdash A \parr B, A^\perp \otimes B^\perp}\,\parr \qquad \dfrac{}{\vdash C^\perp, C}\,\text{ax}}{\vdash (A \parr B) \otimes C^\perp, A^\perp \otimes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

The mapping

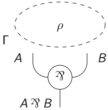
$$\frac{}{\vdash A^{\perp}, A}\ \text{ax} \quad \mapsto$$



$$\frac{\begin{array}{c}\pi_1\\ \vdash \Gamma, A\end{array} \qquad \begin{array}{c}\pi_2\\ \vdash B, \Delta\end{array}}{\vdash \Gamma, A \otimes B, \Delta}\ \otimes \quad \mapsto$$



$$\frac{\begin{array}{c}\pi\\ \vdash \Gamma, A, B\end{array}}{\vdash \Gamma, A \parr B}\ \parr \quad \mapsto$$

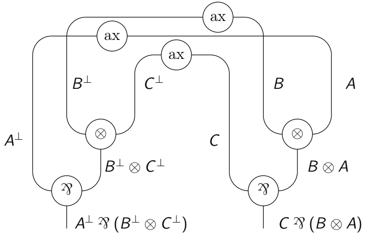


Theorem (Sequentialization)

A proof structure is the image of an MLL *proof* iff *it is a proof net (i.e. correct)*

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

$\searrow$

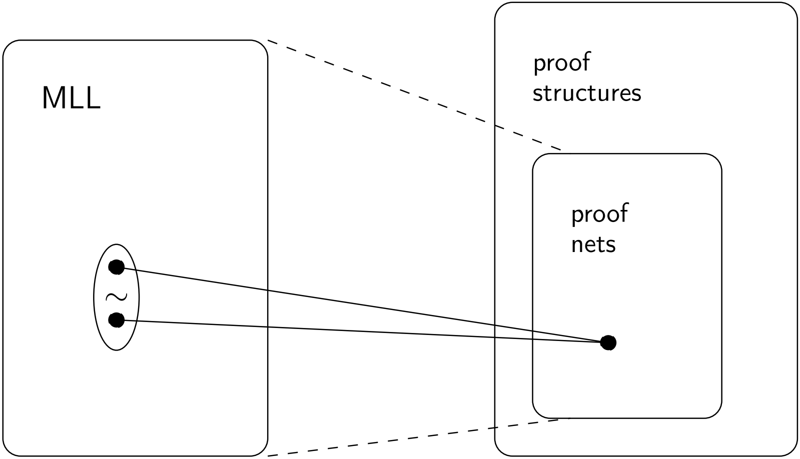


$\nearrow$

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

MLL and Proof Nets: Back and Forth

the big picture



Remark: Forgetting context implies forgetting order of rules.

Linear Implication and Deduction

- A notation: $A \multimap B := A^\perp \parr B$
- We write $A \vdash B$ for $\vdash A^\perp, B$
- The provabilities of the following sequents are equivalent:

$$A \vdash B$$
$$\vdash A^\perp, B$$
$$\vdash A^\perp \parr B$$
$$\vdash A \multimap B$$

- We write $A \dashv\vdash B$ for "$A \vdash B$ provable and $B \vdash A$ provable"

Mutliplicative Linear Logic: Basic Properties

- Associativity:

$$A \parr (B \parr C) \dashv\vdash (A \parr B) \parr C$$
$$A \otimes (B \otimes C) \dashv\vdash (A \otimes B) \otimes C$$

- Commutativity:

$$A \parr B \dashv\vdash B \parr A$$
$$A \otimes B \dashv\vdash B \otimes A$$

- Identity: $\vdash A \multimap A$ is provable (*it is also excluded middle*)
- Consistency: $\vdash$ is not provable
- Non contradiction: $\vdash A \otimes A^{\perp}$ is not provable (*later*)
- Linear distributivity: $A \otimes (B \parr C) \vdash (A \otimes B) \parr C$ is provable

The Cut Rule

introduction

- Is consequence transitive?

  $A \vdash B$ provable and $B \vdash C$ provable implies $A \vdash C$ provable ?

- Are lemmas usable?

  $\vdash A$ provable and $A \vdash B$ provable implies $\vdash B$ provable?

- Is linear implication transitive?

  $A \multimap B$ provable and $B \multimap C$ provable implies $A \multimap C$ provable?

- Is *modus ponens* valid?

  A provable and $A \multimap B$ provable implies B provable?

- A common principle:

$$\frac{A \vdash B \qquad B \vdash C}{A \vdash C}$$

The Cut Rule

introduction

- Is consequence transitive?

$$A \vdash B \text{ provable and } B \vdash C \text{ provable implies } A \vdash C \text{ provable ?}$$

- Are lemmas usable?

$$\vdash A \text{ provable and } A \vdash B \text{ provable implies } \vdash B \text{ provable?}$$

- Is linear implication transitive?

$$A \multimap B \text{ provable and } B \multimap C \text{ provable implies } A \multimap C \text{ provable?}$$

- Is *modus ponens* valid?

$$A \text{ provable and } A \multimap B \text{ provable implies } B \text{ provable?}$$

- A common principle:

$$\frac{\vdash A^\perp, B \qquad \vdash B^\perp, C}{\vdash A^\perp, C}$$

The Cut Rule

introduction

- Is consequence transitive?

$$A \vdash B \text{ provable and } B \vdash C \text{ provable implies } A \vdash C \text{ provable ?}$$

- Are lemmas usable?

$$\vdash A \text{ provable and } A \vdash B \text{ provable implies } \vdash B \text{ provable?}$$

- Is linear implication transitive?

$$A \multimap B \text{ provable and } B \multimap C \text{ provable implies } A \multimap C \text{ provable?}$$

- Is *modus ponens* valid?

$$A \text{ provable and } A \multimap B \text{ provable implies } B \text{ provable?}$$

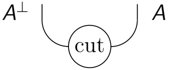
- A common principle:

$$\frac{\vdash \Gamma, B \qquad \vdash B^{\perp}, \Delta}{\vdash \Gamma, \Delta}\ \text{cut}$$

The Cut Rule

the proof net side

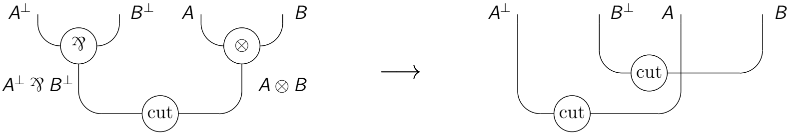
$$\frac{\vdash \Gamma, A^{\perp} \qquad \vdash A, \Delta}{\vdash \Gamma, \Delta}\ \text{cut} \qquad \mapsto$$



- Is the logic modified?
- Can we try to move cuts away?

Axiom cut

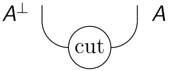
Multiplicative cut



The Cut Rule

the proof net side

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



- Is the logic modified?
- Can we try to move cuts away?

Theorem (Termination)

Linear number of steps: decreasing number of nodes.

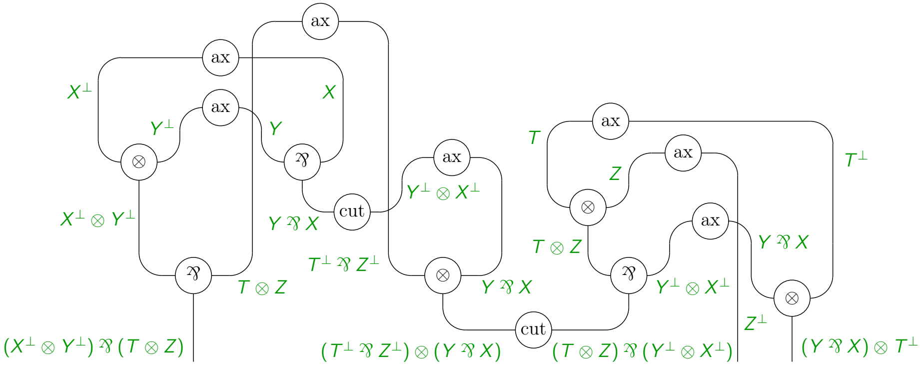
- Is it enough to have cut elimination?

Lemma (Preservation of Correctness)

The two transformations preserve correctness.

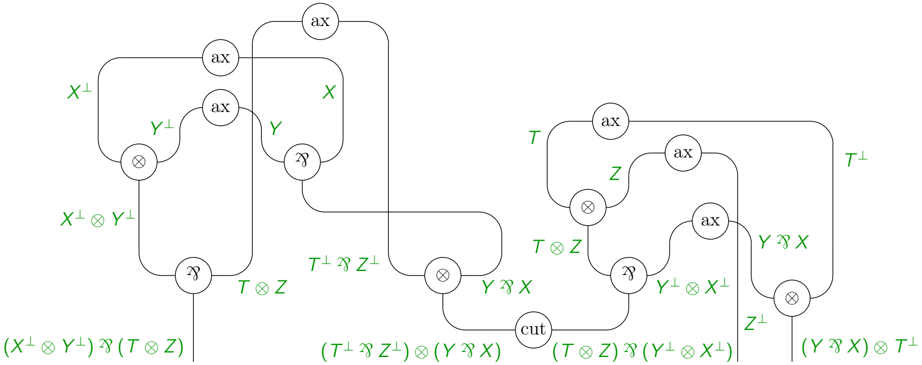
The Cut Rule

example



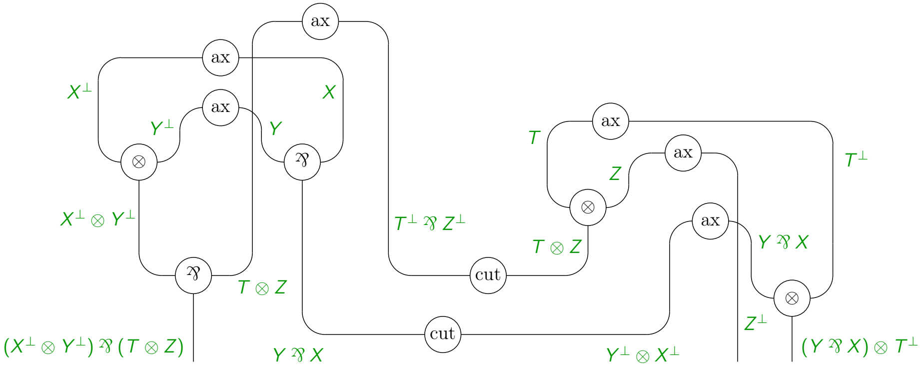
The Cut Rule

example



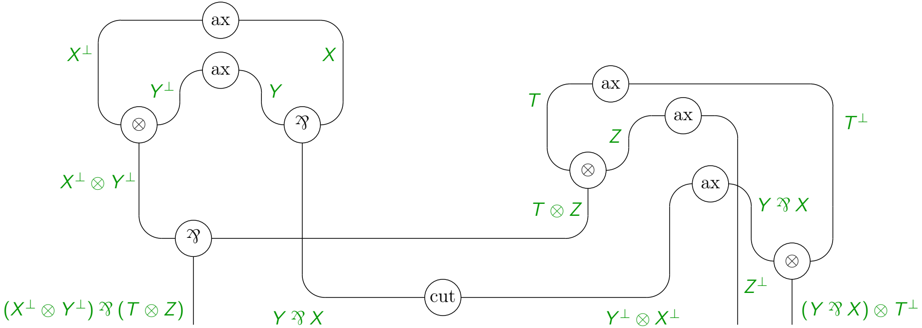
The Cut Rule

example



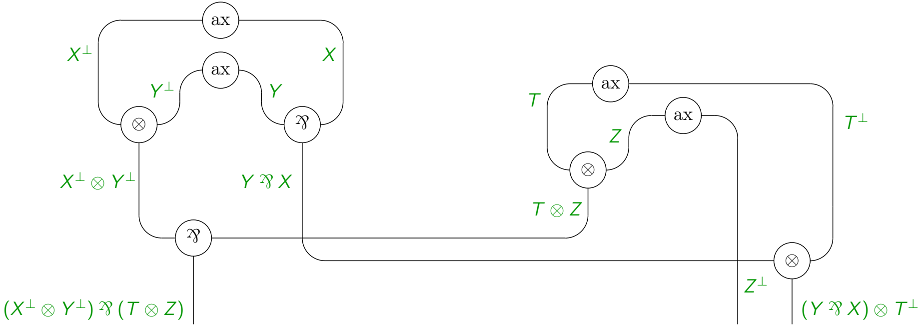
The Cut Rule

example



The Cut Rule

example



The Cut Rule

power and applications

Theorem (Cut Admissibility / Cut Elimination)

Adding $\left(\dfrac{\vdash \Gamma, A^\perp \qquad \vdash A, \Delta}{\vdash \Gamma, \Delta}\ cut \right)$ *to* MLL *does not modify provability.*

- use cut to prove
- remove cut to analyse

Non Contradiction

- Assume $\vdash A \otimes A^\perp$ is provable for some A.
- Using cut, we have:

$$\dfrac{\dfrac{\pi}{\vdash A \otimes A^\perp} \qquad \dfrac{\dfrac{}{\vdash A^\perp, A}\ \text{ax}}{\vdash A^\perp \parr A}\ \parr}{\vdash}\ \text{cut}$$

- Eliminate cut.
- But $\vdash$ is not provable in MLL without cut (*no last rule*).

Reversibility

Theorem (⅋ reversible)

$\vdash \Gamma, A \parr B$ is provable iff $\vdash \Gamma, A, B$ is provable.

$$\dfrac{\overset{\pi}{\vdash \Gamma, A \parr B} \qquad \dfrac{\dfrac{}{\vdash A^\perp, A}\,\text{ax} \qquad \dfrac{}{\vdash B^\perp, B}\,\text{ax}}{\vdash A^\perp \otimes B^\perp, A, B}\,\otimes}{\vdash \Gamma, A, B}\,\text{cut}$$

Theorem (⊗ irreversible)

$\vdash X \otimes Y, X^\perp \parr Y^\perp$ is provable
but neither $\vdash X, X^\perp \parr Y^\perp$ nor $\vdash Y, X^\perp \parr Y^\perp$ is provable.

$$\dfrac{\dfrac{\dfrac{}{\vdash X, X^\perp}\,\text{ax} \qquad \dfrac{}{\vdash Y, Y^\perp}\,\text{ax}}{\vdash X \otimes Y, X^\perp, Y^\perp}\,\otimes}{\vdash X \otimes Y, X^\perp \parr Y^\perp}\,\parr \qquad\qquad \dfrac{\vdash X, X^\perp, Y^\perp}{\vdash X, X^\perp \parr Y^\perp}\,\parr$$

Cut Elimination as Computation

Uniqueness of the Result

If $\sigma \longrightarrow \cdots \longrightarrow \sigma_1$ (σ_1 without cut)
and $\sigma \longrightarrow \cdots \longrightarrow \sigma_2$ (σ_2 without cut)

then $\sigma_1 = \sigma_2$.

Computational Interpretation

$$\begin{array}{ccc} \text{program } P & \text{evaluates to} & \text{result } r \\ \updownarrow & & \updownarrow \\ \rho & \longrightarrow \cdots \longrightarrow & \rho_0 \text{ (cut-free)} \end{array}$$

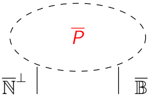
What kind of programs or computational processes can be represented?

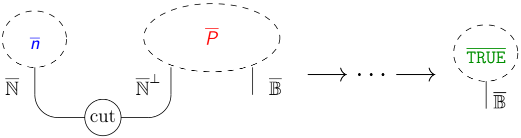
Computing with Proofs Nets

Try to find a representation $\_ \mapsto \overline{(\_)}$ with:

P program from $\mathbb{N}$ to $\mathbb{B}$ such that $P(n)$ evaluates to TRUE

$\updownarrow$ $\updownarrow$





Denotational Semantics

Principles

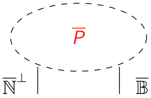
- From models of formulas ...
  - true vs. false
  - or more refined
  - mathematical/algebraic view of formulas
  - existence of proof
- ... to models of proofs ...
  - more than: existence or not
  - proofs seen as mathematical objects
  - algebraic view of proofs
- ... as computational invariants.
  - distinguish proofs, but not up to computation
  - meaning of computation
  - alternative access to results (*next slide*)

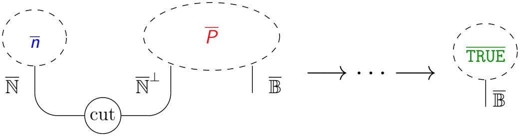
Main Pattern

- for each formula A: an interpretation $[\![A]\!]$
- for each proof π of $\vdash A$: an interpretation $[\![\pi]\!]$ related to $[\![A]\!]$

P program from $\mathbb{N}$ to $\mathbb{B}$ such that $P(n)$ evaluates to TRUE

$\updownarrow$ $\updownarrow$





$\updownarrow$ $\updownarrow$

$[\![\overline{P}]\!]$

$$[\![\overline{P}]\!] \circ [\![\overline{n}]\!] = [\![\overline{\text{TRUE}}]\!]$$

The Relational Model

Set-based Model

- Interpret formula A / sequent $\vdash \Gamma$: a (finite) set $[\![A]\!]$ / $[\![\vdash \Gamma]\!]$
- Interpret a proof π of $\vdash \Gamma$: a sub-set $[\![\pi]\!] \subseteq [\![\vdash \Gamma]\!]$

From Formulas to Sets

- Assume $[\![X]\!]$ given for each X.
- Define $[\![X^\perp]\!] := [\![X]\!]$.
- Define $[\![A \otimes B]\!] := [\![A]\!] \times [\![B]\!]$.
- Define $[\![A \parr B]\!] := [\![A]\!] \times [\![B]\!]$.
- Property: $[\![A^\perp]\!] = [\![A]\!]$.
- Define $[\![\vdash A_1, \ldots, A_n]\!] := [\![A_1]\!] \times \cdots \times [\![A_n]\!] \quad (\simeq [\![A_1 \parr \cdots \parr A_n]\!])$.

Relations

Let π be a proof of $\vdash A \multimap B$,

$$[\![\pi]\!] \subseteq [\![\vdash A \multimap B]\!] = [\![\vdash A^\perp \parr B]\!] = [\![A^\perp]\!] \times [\![B]\!] = [\![A]\!] \times [\![B]\!].$$

Interpretation of Proofs

Decoration of Proofs

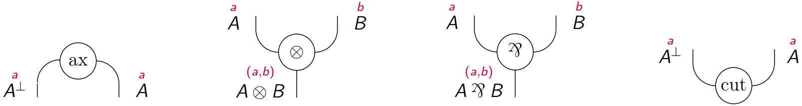
$$\dfrac{a \in [\![A]\!]}{\vdash \overset{a}{A^\perp}, \overset{a}{A}}\ \text{ax} \qquad \dfrac{\vdash \overset{s}{\Gamma}, \overset{a}{A} \quad \vdash \overset{b}{B}, \overset{t}{\Delta}}{\vdash \overset{s}{\Gamma}, \overset{(a,b)}{A \otimes B}, \overset{t}{\Delta}}\ \otimes \qquad \dfrac{\vdash \overset{s}{\Gamma}, \overset{a}{A}, \overset{b}{B}}{\vdash \overset{s}{\Gamma}, \overset{(a,b)}{A \parr B}}\ \parr$$

$$\dfrac{\vdash \overset{s}{\Gamma}, \overset{a}{A^\perp} \quad \vdash \overset{a}{A}, \overset{t}{\Delta}}{\vdash \overset{s}{\Gamma}, \overset{t}{\Delta}}\ \text{cut}$$

Collect the Results

- Property of rules: $\overset{a}{A}$ implies $a \in [\![A]\!]$
- $[\![\pi]\!] := \left\{ s \;\middle|\; \begin{array}{c} \pi \\ \vdots \\ \vdash \overset{s}{\Gamma} \end{array} \right\} \subseteq [\![\vdash \Gamma]\!]$

Decoration of Proof Structures



Collect the Results

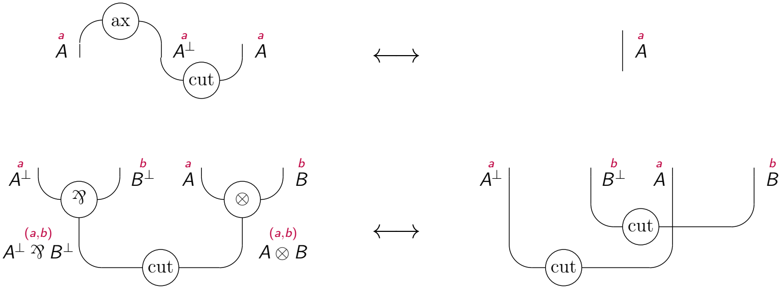
- Property of node decoration: $\overset{a}{A}$ implies $a \in [\![A]\!]$
- $[\![\sigma]\!] := \left\{ s \;\middle|\; \begin{array}{c} \sigma \\ \vdots \\ \overset{s}{\vdash \Gamma} \end{array} \right\} \subseteq [\![\vdash \Gamma]\!]$

Cut Elimination

Theorem (Invariance)

If $\sigma_1 \longrightarrow \sigma_2$ *then* $[\![\sigma_1]\!] = \left\{ s \;\middle|\; \begin{array}{c} \sigma_1 \\ \vdots \\ \vdash \overset{s}{\Gamma} \end{array} \right\} = \left\{ s \;\middle|\; \begin{array}{c} \sigma_2 \\ \vdots \\ \vdash \overset{s}{\Gamma} \end{array} \right\} = [\![\sigma_2]\!]$.

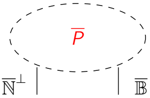
Decoration Transformation



Computing with Relational Semantics

P program from $\mathbb{N}$ to $\mathbb{B}$

$\updownarrow$



$\updownarrow$

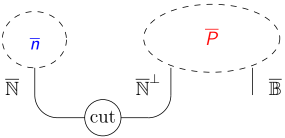
$[\![\overline{P}]\!]$

$=$

$\{(1, b_1), \ldots, (i, b_i), \ldots\}$

evaluates $P(n)$

$\updownarrow$



$\updownarrow$

$[\![\overline{P}]\!] \circ [\![\overline{n}]\!]$

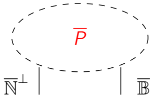
$=$

$\{n\} \quad \{\ldots, (n, b_n), \ldots\}$

Computing with Relational Semantics

P program from $\mathbb{N}$ to $\mathbb{B}$

$\updownarrow$



$\updownarrow$

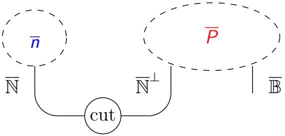
$$[\![\, \overline{P} \,]\!]$$

$$\shortparallel$$

$$\{(1, b_1), \ldots, (i, b_i), \ldots\}$$

evaluates $P(n)$

$\updownarrow$



$\updownarrow$

$$[\![\, \overline{P} \,]\!] \circ [\![\, \overline{n} \,]\!]$$

$$\shortparallel$$

$$\{n\} \quad \{\ldots, (n, b_n), \ldots\}$$

Properties of the Relational Model

Not Complete

- forall Γ, $\emptyset \subseteq [\![\vdash \Gamma]\!]$
- if $[\![X]\!] = \{a, b\}$, $\{(a, b)\} \notin [\![\pi]\!]$ if π proof of $\vdash X^\perp, X$

Injective

Given two proof structures σ_1 and σ_2 with conclusion Γ,
without cuts and with atomic axioms,
if $[\![\sigma_1]\!] = [\![\sigma_2]\!] \subseteq [\![\Gamma]\!]$ then $\sigma_1 = \sigma_2$ (*with* $[\![X]\!]$ *big enough*).

A Coarse Model

- $[\![A]\!] = [\![A^\perp]\!]$ $[\![A \otimes B]\!] = [\![A \parr B]\!]$
- no difference between proof structures and proof nets
- incompleteness
- no information about provability

Summary, etc.

- Two syntaxes
  - Proof nets
    - linear time correctness
    - perfect quotient of proofs
  - Sequent calculus
    - refinement of the classical one
- A denotational model
  - Relational model
    - simple
    - both proof nets and proof structures
    - not very precise
- A computational model
  - Proof structures not just proof nets
  - Linear time cut elimination
  - Unique result
- NP-complete provability