Introduction to Proof Theory

Lecture notes for ESSLLI'10

August 9–20, 2010, University of Copenhagen, Denmark

Lutz Straßburger

INRIA Saclay – Île-de-France
École Polytechnique, Laboratoire d'Informatique (LIX)
Rue de Saclay — 91128 Palaiseau Cedex — France
http://www.lix.polytechnique.fr/~lutz/

July 9, 2010

Contents

0 What is this?

These are the notes for a 5-lecture-course given at ESSLLI'10, held from August 9 to 20, 2010, at The University of Copenhagen (KUA), Denmark. The URL of the school is

`http://esslli2010cph.info/`

The course is intended to be introductory. That means no prior knowledge of proof theory is required. However, the student should be familiar with the basics of propositional logic.

The course will give a basic introduction to proof theory, focussing on those aspects of the field that are most relevant to ESSLLI. In particular, the student will learn what is a deductive system and why cut elimination is important. The course will also discuss the presentation of proofs via proof nets, which are graph-like objects that allow to quotient away the syntactic bureaucracy of deductive systems. Finally, we will also see how category theory can be used to describe proofs as algebraic objects.

The main emphasis will be put on the observation that the various ways of presenting proofs are just different aspects of the same theory. We will use the notion of deep inference to substanciate this observation and to visualize the close relationship between deductive systems, categories, and proof nets: A morphism in a category is the same as a derivation in a deductive system, and a proof net is the same as the flowgraph of a derivation or the coherence graph in the category.

1 What is a formal system?

Already in ancient Greece people tried to formalize the notion of a logical argument. For example, the rule of *modus ponens*, in modern notation written as

$$\mathsf{mp}\,\frac{A \qquad A \to B}{B} \tag{1}$$

goes back at least to Aristoteles. The figure in (1) says that if you know that A is true and you also know that A implies B, then you can conclude B.

In the early 20th century David Hilbert had the idea to formalize mathematics. He wanted to prove its consistency in order to avoid paradoxes (like *Russel's paradox*). Although this plan failed, due to Gödel's Incompleteness Theorem, Hilbert's work had huge impact on the development of modern proof theory. He introduced the first *formal deductive system* consisting of *axioms* and *inference rules*.

1.1 Hilbert systems

Figure 1 shows a so-called *Hilbert system* (also called *Frege systems* or *Hilbert-Frege-systems* or *Hilbert-Ackermann-systems*) for classical propositional logic. The system in Figure 1, that we call here H, contains ten axioms and one rule: modus ponens.

More precisely, we should speak of ten *axiom schemes* and one *rule scheme*. Each axiom scheme represents infinitely many axioms. For example

$$(a \wedge c) \to \langle [a \vee (b \wedge \neg c)] \to (a \wedge c)\rangle$$

is an instance of the axiom scheme

$$A \to \langle B \to A\rangle$$

1.1.1 Notation Throughout this lecture notes, we use lower case latin letters a, b, c, $\ldots$, for propositional variables, and capital latin letters A, B, C, $\ldots$, for formula variables. As usual, the symbol $\wedge$ stands for conjunction (*and*), $\vee$ stands for disjunction (*or*), and $\to$ stands for implication. Furthermore, to ease the reading of long formulas, we use different types of brackets for the different connectives. We use $(\ldots)$ for $\wedge$, $[\ldots]$ for $\vee$, and $\langle\ldots\rangle$ for $\to$. This is pure redundancy and has no deep meaning.

A *proof* in a Hilbert system is a sequence of formulas $A_0, A_1, A_2, \ldots, A_n$, where for each $0 \leq i \leq n$, the formula A_i is either an axiom, or it follows from A_j and A_k via modus ponens, where $j, k < i$. The formula A_n is called the *conclusion* of the proof.

The main results on Hilbert systems are *soundness* and *completeness*:

1.1.2 Theorem (Soundness) *If there is a proof in* H *with conclusion* A*, then* A *is a tautology.*

1.1.3 Theorem (Completeness) *If the formula* A *is a tautology, then there is a proof in* H *with conclusion* A*.*

$$
\begin{array}{ll}
A \to \langle B \to A \rangle & (A \wedge B) \to A \\
\langle A \to \langle B \to C \rangle \rangle \to \langle A \to B \rangle \to A \to C & (A \wedge B) \to B \\
A \to [A \vee B] & A \to \langle B \to (A \wedge B) \rangle \\
B \to [A \vee B] & \mathsf{f} \to A \\
\langle A \to C \rangle \to \langle B \to C \rangle \to \langle [A \vee B] \to C \rangle & \neg\neg A \to A
\end{array}
$$

$$
\mathsf{mp}\ \dfrac{A \quad A \to B}{B}
$$

Figure 1: The Hilbert system H

1.2 Natural deduction

Proving stuff in a Hilbert system can be quite tedious. For this reason, Gerhard Gentzen introduced the notion of *natural deduction*. Figure 2 shows his system NK.

Let us now see why Gentzen called this system "natural deduction". For this, let us more closely inspect some of the rules:

$\wedge$I: This rule is called $\wedge$-introduction, because it introduces an $\wedge$ in the conclusion. It says: if there is a proof of A and a proof of B, then we can form a proof of $A \wedge B$ which has as assumptions the union of the assumptions of the proofs of A and B.

$\to$I: This rule is called $\to$-introduction, because introduces an $\to$. It says that if we can prove B under the assumption A, then we can prove $A \to B$ without that assumption. The notation $\cancel{A}$ simply says that A had been removed from the list of assumptions.

$\to$E: This rule is called $\to$-elimination, because it eliminates an $\to$. It is exactly the same as modus ponens.

1.2.1 Exercise Find similar explanations for the other rules.

1.2.2 Example Let us now see an example proof:

$$
\to\mathrm{I}\ \dfrac{\vee\mathrm{E}\ \dfrac{\cancel{A \vee (B \wedge C)} \qquad \wedge\mathrm{I}\ \dfrac{\vee\mathrm{I_R}\ \dfrac{\cancel{A}}{A \vee B} \quad \vee\mathrm{I_R}\ \dfrac{\cancel{A}}{A \vee C}}{[A \vee B] \wedge [A \vee C]} \qquad \wedge\mathrm{I}\ \dfrac{\vee\mathrm{I_R}\ \dfrac{\wedge\mathrm{E_R}\ \dfrac{\cancel{B \wedge C}}{B}}{A \vee B} \quad \vee\mathrm{I_R}\ \dfrac{\wedge\mathrm{E_L}\ \dfrac{\cancel{B \wedge C}}{C}}{A \vee C}}{[A \vee B] \wedge [A \vee C]}}{[A \vee B] \wedge [A \vee C]}}{[A \vee (B \wedge C)] \to ([A \vee B] \wedge [A \vee C])} \tag{2}
$$

Informally, we can read this proof as follows: We want to prove

$$
[A \vee (B \wedge C)] \to ([A \vee B] \wedge [A \vee C])
$$

We assume $A \vee (B \wedge C)$. There are two cases: We have A or we have $B \wedge C$. In the first case we can conclude $A \vee B$ as well as $A \vee C$, and therefore also $[A \vee B] \wedge [A \vee C]$. In the second case we can conclude B and C, and therefore also $A \vee B$ as well as $A \vee C$, from which

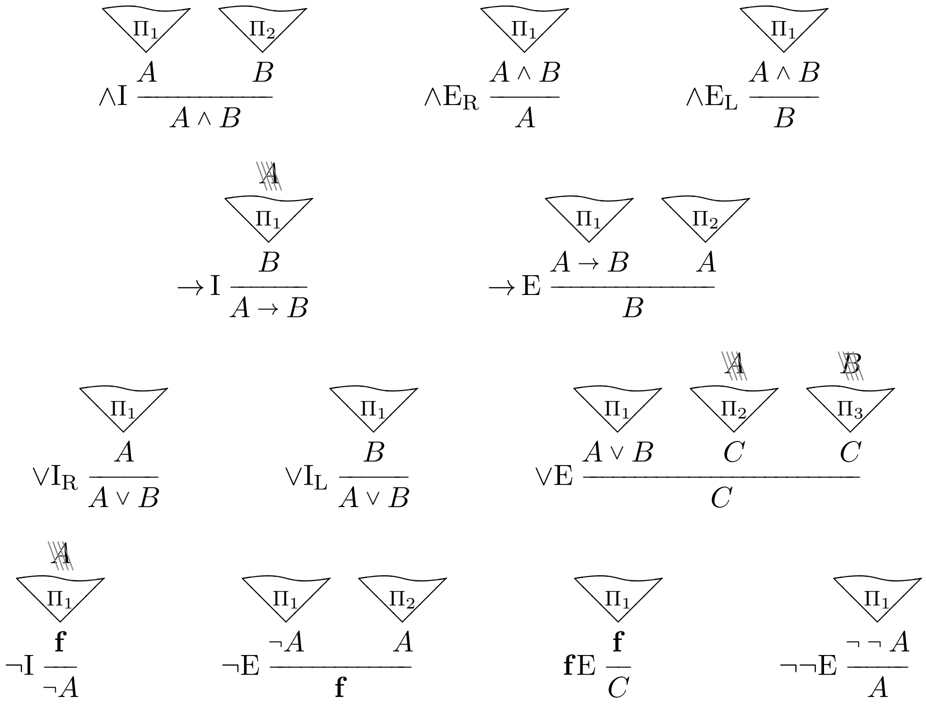


Figure 2: The natural deduction system NK

we get $[A \vee B] \wedge [A \vee C]$. We have therefore shown $[A \vee B] \wedge [A \vee C]$ from the assumption $A \vee (B \wedge C)$, and we can conclude $[A \vee (B \wedge C)] \to ([A \vee B] \wedge [A \vee C])$.

As for Hilbert systems, we have soundness and completeness for NK.

1.2.3 Theorem (Soundness) *If there is a proof in* NK *with conclusion A, then A is a tautology.*

1.2.4 Theorem (Completeness) *If the formula A is a tautology, then there is a proof in* NK *with conclusion A.*

1.2.5 Exercise Use the system NK (shown in Figure 2) for proving the axioms of the system H (shown in Figure 1).

1.3 Sequent calculus

In order to reason about derivations in natural deduction, Gentzen also introduced the *sequent calculus.* Figure 3 shows his system LK. While Hilbert systems have many axioms and few rules, sequent systems have few axioms and many rules. Gentzen's original system (Figure 3) is a variant of what is nowadays called a *two-sided system*, where a *sequent*

$$A_1, \ldots, A_n \vdash B_1, \ldots, B_m \tag{3}$$

$$\mathsf{id}\ \frac{}{A \vdash A}$$

$$\mathsf{weakL}\ \frac{\Gamma \vdash \Theta}{A, \Gamma \vdash \Theta} \qquad \mathsf{weakR}\ \frac{\Gamma \vdash \Theta}{\Gamma \vdash \Theta, A}$$

$$\mathsf{contL}\ \frac{A, A, \Gamma \vdash \Theta}{A, \Gamma \vdash \Theta} \qquad \mathsf{contR}\ \frac{\Gamma \vdash \Theta, A, A}{\Gamma \vdash \Theta, A}$$

$$\mathsf{exchL}\ \frac{\Delta, B, A, \Gamma \vdash \Theta}{\Delta, A, B, \Gamma \vdash \Theta} \qquad \mathsf{exchR}\ \frac{\Gamma \vdash \Theta, B, A, \Lambda}{\Gamma \vdash \Theta, A, B, \Lambda}$$

$$\wedge\mathrm{L}_1\ \frac{A, \Gamma \vdash \Theta}{A \wedge B, \Gamma \vdash \Theta} \qquad \wedge\mathrm{L}_2\ \frac{B, \Gamma \vdash \Theta}{A \wedge B, \Gamma \vdash \Theta} \qquad \wedge\mathrm{R}\ \frac{\Gamma \vdash \Theta, A \qquad \Gamma \vdash \Theta, B}{\Gamma \vdash \Theta, A \wedge B}$$

$$\vee\mathrm{L}\ \frac{A, \Gamma \vdash \Theta \qquad B, \Gamma \vdash \Theta}{A \vee B, \Gamma \vdash \Theta} \qquad \vee\mathrm{R}_1\ \frac{\Gamma \vdash \Theta, A}{\Gamma \vdash \Theta, A \vee B} \qquad \vee\mathrm{R}_2\ \frac{\Gamma \vdash \Theta, B}{\Gamma \vdash \Theta, A \vee B}$$

$$\to\mathrm{L}\ \frac{\Gamma \vdash \Theta, A \qquad B, \Delta \vdash \Lambda}{A \to B, \Gamma, \Delta \vdash \Theta, \Lambda} \qquad \to\mathrm{R}\ \frac{A, \Gamma \vdash \Theta, B}{\Gamma \vdash \Theta, A \to B}$$

$$\neg\mathrm{L}\ \frac{\Gamma \vdash \Theta, A}{\neg A, \Gamma \vdash \Theta} \qquad \neg\mathrm{R}\ \frac{A, \Gamma \vdash \Theta}{\Gamma \vdash \Theta, \neg A}$$

$$\mathsf{cut}\ \frac{\Gamma \vdash \Theta, A \qquad A, \Delta \vdash \Lambda}{\Gamma, \Delta \vdash \Theta, \Lambda}$$

Figure 3: Gentzen's sequent calculus LK

consists of two lists of formulas, and should be read as: The conjunction of the A_i entails the disjunction of the B_j. As formula:

$$(A_1 \wedge \cdots \wedge A_n) \to [B_1 \vee \cdots \vee B_m]$$

Lists of formulas are usually denoted by capital greek letters, like Γ, Δ, Λ, ...

As for Hilbert systems an natural deduction, we have soundness and completeness for LK.

1.3.1 Theorem (Soundness) *If there is a proof in* LK *with conclusion* $\vdash A$*, then* A *is a tautology.*

1.3.2 Theorem (Completeness) *If the formula* A *is a tautology, then there is a proof in* LK *with conclusion* $\vdash A$*.*

1.3.3 Example To give an example how the rules work, we prove here the same formula as in Example 1.2.2:

$$\to\mathrm{R}\,\dfrac{\vee\mathrm{L}\,\dfrac{\wedge\mathrm{R}\,\dfrac{\vee\mathrm{R}_1\,\dfrac{\mathsf{id}\,\dfrac{}{A\vdash A}}{A\vdash A\vee B}\qquad \vee\mathrm{R}_1\,\dfrac{\mathsf{id}\,\dfrac{}{A\vdash A}}{A\vdash A\vee C}}{A\vdash [A\vee B]\wedge[A\vee C]}\qquad \wedge\mathrm{R}\,\dfrac{\vee\mathrm{R}_2\,\dfrac{\wedge\mathrm{L}_1\,\dfrac{\mathsf{id}\,\dfrac{}{B\vdash B}}{B\wedge C\vdash B}}{B\wedge C\vdash A\vee B}\qquad \vee\mathrm{R}_2\,\dfrac{\wedge\mathrm{L}_2\,\dfrac{\mathsf{id}\,\dfrac{}{C\vdash C}}{B\wedge C\vdash C}}{B\wedge C\vdash A\vee C}}{B\wedge C\vdash [A\vee B]\wedge[A\vee C]}}{A\vee(B\wedge C)\vdash [A\vee B]\wedge[A\vee C]}}{\vdash [A\vee(B\wedge C)]\to([A\vee B]\wedge[A\vee C])} \tag{4}$$

1.3.4 Exercise Prove the axioms of the system H with the sequent calculus LK.

Observe that in natural deduction there are *introduction rules* and *elimination rules*, whereas in the sequent calculus there are only introduction rules: *introduction on the left* and *introduction on the right*. The rules for contraction (contL and contR), weakening (weakL and weakR), and exchange (exchL and exchR) are called *structural rules* because they modify only the "structure" of the sequent. The rules for $\wedge$, $\vee$, $\to$, and $\neg$ are called *logical rules*. A special role is played by the id rule and by the cut rule, which, in a certain sense can considered duals of each other.

The rule id is the axiom. It says that A implies A. An interesting observation is that in the sequent calculus the identity axiom can be reduced to an atomic version

$$\mathsf{atomic\ id}\,\dfrac{}{a\vdash a} \tag{5}$$

1.3.5 Proposition *The rule* id *is derivable in the system* $\{\mathsf{atomic\ id}\}\cup\mathsf{LK}\setminus\{\mathsf{id}\}$.

Proof: Suppose we have an instance of id:

$$\mathsf{id}\,\dfrac{}{A\vdash A}$$

We proceed by induction on the size of A to construct a derivation that uses only the atomic version of id.

- If $A = B\wedge C$, then we can replace

$$\mathsf{id}\,\dfrac{}{B\wedge C\vdash B\wedge C} \qquad \text{by} \qquad \wedge\mathrm{R}\,\dfrac{\wedge\mathrm{L}_1\,\dfrac{\mathsf{id}\,\dfrac{}{B\vdash B}}{B\wedge C\vdash B}\qquad \wedge\mathrm{L}_2\,\dfrac{\mathsf{id}\,\dfrac{}{C\vdash C}}{B\wedge C\vdash C}}{B\wedge C\vdash B\wedge C} \tag{6}$$

  and proceed by induction hypothese.

The other cases are similar (see Execise 1.3.6). □

$$\mathsf{id}\,\frac{}{\vdash \bar{A}, A}$$

$$\mathsf{weak}\,\frac{\vdash \Gamma}{\vdash \Gamma, A} \qquad \mathsf{cont}\,\frac{\vdash \Gamma, A, A}{\vdash \Gamma, A} \qquad \mathsf{exch}\,\frac{\vdash \Delta, B, A, \Gamma}{\vdash \Delta, A, B, \Gamma}$$

$$\wedge\,\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B} \qquad \vee_1\,\frac{\vdash \Gamma, A}{\vdash \Gamma, A \vee B} \qquad \vee_2\,\frac{\vdash \Gamma, B}{\vdash \Gamma, A \vee B}$$

$$\mathsf{cut}\,\frac{\vdash \Gamma, A \quad \vdash \bar{A}, \Delta}{\vdash \Gamma, \Delta}$$

Figure 4: One-sided version of LK

1.3.6 Exercise Complete the proof of Proposition 1.3.5 (i.e., show the cases that are omitted).

The cut rule expesses the transitivity of the logical consequence relation: if from B we can conclude A, and from A we can conclude C, then from B we can conclude C directly. One can say that the cut rule allows to use "lemmas" in a proof. The main and most surprising result for the sequent calculus LK is that if there is a proof in LK, then the same conclusion can be proved in LK *without* using the cut rule. This is nowadays called *cut elimination.*

1.3.7 Theorem *If a sequent* $\Gamma \vdash \Theta$ *is provable in* LK*, then it is also provable in* $\mathsf{LK} \setminus \{\mathsf{cut}\}$.

We do not show the proof here, but in the next section we will see a complete proof of a cut elimination result for a simpler system.

Some consequences of cut elimination are (in propositional logic and in first order predicate logic) the *subformula property* and the *consistency* of the system.

The subformula property says that every formula that occurs somewhere in the proof is a subformula of the conclusion. It is easy to see that only the cut rule violates this property in LK.

Consistency says that there is no formula A such that we can prove both A and $\neg A$. This can be proved as follows: By way of contradiction assume we have such a formula. By using the cut rule, we can derive the empty sequent $\vdash$. By cut elimination there is a cut-free proof of the empty sequent $\vdash$. But by the subformula property this is impossible.

If the logic has DeMorgan duality (like classical logic), we only need to consider formulas in negation normal form, i.e., negation is pushed to the atoms via the DeMorgan laws:

$$\neg(A \wedge B) = \neg A \vee \neg B \qquad \neg[A \vee B] = \neg A \wedge \neg B \qquad \neg\neg A = A \tag{7}$$

and implication is eliminated by using

$$A \to B = \neg A \vee B \tag{8}$$

$$\text{weak}\ \frac{\vdash \Gamma}{\vdash \Gamma, A} \qquad \text{cont}\ \frac{\vdash \Gamma, A, A}{\vdash \Gamma, A} \qquad \text{exch}\ \frac{\vdash \Delta, B, A, \Gamma}{\vdash \Delta, A, B, \Gamma}$$

$$\text{id}\ \frac{}{\vdash a, \bar{a}} \qquad \wedge\ \frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, A \wedge B, \Delta} \qquad \vee\ \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \vee B} \qquad \text{cut}\ \frac{\vdash \Gamma, A \quad \vdash \bar{A}, \Delta}{\vdash \Gamma, \Delta}$$

Figure 5: Another one-sided sequent calculus for classical logic

Then we need to consider only *one-sided sequents*:

$$\vdash B_1, \ldots, B_m \tag{9}$$

In such a system, negation is often denoted by $\overline{(\cdot)}$, i.e., we write $\bar{A}$ instead of $\neg A$.

The translation of a two-sided sequent (3) into a one-sided sequent is simply $\vdash \bar{A}_1, \ldots, \bar{A}_n, B_1, \ldots, B_m$

The practical advantage is that we can halve the number of rules. Figure 4 shows the one-sided version of LK.

There are many different sequent systems for classical logic; a second one is shown in Figure 5. One-sided systems are also called *Gentzen-Schütte* systems.

1.3.8 Exercise Translate the axioms of the Hilbert system H into negation normal form, and prove them using the rules in Figure 4.

1.4 Deep inference

The design feature of the sequent calculus is, that during a proof, a formula is always decomposed at its main connective. We will see in the next lecture that this is crucial for the cut elimination proof. However, it also restricts the freedom in designing inference rules.

The *calculus of structures* breaks with the tradition of the main connective and allows rewriting of formulas deep inside any context. This principle is also called *deep inference*. Figure 6 shows system SKSg. In that system, Formulas have to be considered modulo an equational theory generated by the equations shown in Figure 7. Such an equivalence class of formulas is also called *structure* (hence the name "calculus of structures").

However, one can avoid this equational theory by incorporating the equations into the rules, as it is done in the system shown in Figure 8. That system has another property: all rules are *local*.

We have seen in Proposition 1.3.5 that in the sequent calculus, the identity axiom can be reduced to an atomic form. The same can be done for the corresponding rule in SKSg. By duality, we can do the same for the cut rule, which is not possible in the sequent calculus. Furthermore, if we add the rules

$$\text{nm}{\downarrow}\ \frac{S\{\mathbf{f}\}}{S\{\mathbf{f} \wedge \mathbf{f}\}} \qquad \text{m}\ \frac{S\{(A \wedge B) \vee (C \wedge D)\}}{S\{[A \vee C] \wedge [B \vee D]\}} \qquad \text{nm}{\uparrow}\ \frac{S\{\mathbf{t} \vee \mathbf{t}\}}{S\{\mathbf{t}\}} \tag{10}$$

we can do the same with contraction and weakening, which is also impossible in the sequent calculus.

$$\mathsf{i}\!\downarrow \frac{S\{\mathbf{t}\}}{S\{A \vee \bar{A}\}} \qquad\qquad \mathsf{i}\!\uparrow \frac{S\{A \wedge \bar{A}\}}{S\{\mathbf{f}\}}$$

$$\mathsf{s}\,\frac{S\{[A \vee B] \wedge C\}}{S\{A \vee (B \wedge C)\}}$$

$$\mathsf{w}\!\downarrow \frac{S\{\mathbf{f}\}}{S\{A\}} \qquad\qquad \mathsf{w}\!\uparrow \frac{S\{A\}}{S\{\mathbf{t}\}}$$

$$\mathsf{c}\!\downarrow \frac{S\{A \vee A\}}{S\{A\}} \qquad\qquad \mathsf{c}\!\uparrow \frac{S\{A\}}{S\{A \wedge A\}}$$

Figure 6: The deep inference system SKSg for classical logic

$$\begin{array}{lll} A \wedge (B \wedge C) = (A \wedge B) \wedge C & A \wedge B = B \wedge A & A \wedge \mathbf{t} = A \\ A \vee [B \vee C] = [A \vee B] \vee C & A \vee B = B \vee A & A \vee \mathbf{f} = A \end{array}$$

Figure 7: Equational theory for SKSg

1.4.1 Proposition *The rules* $\mathsf{i}\!\downarrow$, $\mathsf{i}\!\uparrow$, $\mathsf{c}\!\downarrow$, $\mathsf{c}\!\uparrow$, $\mathsf{w}\!\downarrow$, *and* $\mathsf{w}\!\uparrow$ *are derivable in* SKS.

Proof: As in the proof of Proposition 1.3.5, we proceed by induction on the size of the principal formula of the rule.

- If $A = B \wedge C$, then we can do the following replacements:

$$\mathsf{i}\!\downarrow \frac{S\{\mathbf{t}\}}{S\{(B \wedge C) \vee \bar{C} \vee \bar{B}\}} \quad \rightarrow \quad \mathsf{s}\,\frac{\mathsf{i}\!\downarrow \dfrac{\mathsf{i}\!\downarrow \dfrac{S\{\mathbf{t}\}}{S\{B \vee \bar{B}\}}}{S\{(B \wedge [C \vee \bar{C}]) \vee \bar{B}\}}}{S\{(B \wedge C) \vee \bar{C} \vee \bar{B}\}} \tag{11}$$

$$\mathsf{w}\!\downarrow \frac{S\{\mathbf{f}\}}{S\{B \wedge C\}} \quad \rightarrow \quad \mathsf{w}\!\downarrow \frac{\mathsf{w}\!\downarrow \dfrac{\mathsf{nm}\!\downarrow \dfrac{S\{\mathbf{f}\}}{S\{\mathbf{f} \wedge \mathbf{f}\}}}{S\{\mathbf{f} \wedge C\}}}{S\{B \wedge C\}} \tag{12}$$

$$\mathsf{c}\!\downarrow \frac{S\{(B \wedge C) \vee (B \wedge C)\}}{S\{B \wedge C\}} \quad \rightarrow \quad \mathsf{c}\!\downarrow \frac{\mathsf{c}\!\downarrow \dfrac{\mathsf{m}\, \dfrac{S\{(B \wedge C) \vee (B \wedge C)\}}{S\{[B \vee B] \wedge [C \vee C]\}}}{S\{[B \vee B] \wedge C\}}}{S\{B \wedge C\}} \tag{13}$$

  In each case we can proceed by induction hypothesis. For the rules $\mathsf{i}\!\uparrow$, $\mathsf{c}\!\uparrow$, and $\mathsf{w}\!\uparrow$ the situation is similar.

- We leave the cases $A = B \vee C$, $A = \mathbf{t}$, $A = \mathbf{f}$, and $A = a$ as an exercise. □

$$\mathsf{ai}\!\downarrow \frac{S\{\mathbf{t}\}}{S\{a \vee \bar{a}\}} \qquad \mathsf{ai}\!\uparrow \frac{S\{a \wedge \bar{a}\}}{S\{\mathbf{f}\}}$$

$$\mathsf{s}\ \frac{S\{A \wedge [B \vee C]\}}{S\{(A \wedge B) \vee C\}}$$

$$\mathsf{aw}\!\downarrow \frac{S\{\mathbf{f}\}}{S\{a\}} \qquad \mathsf{ac}\!\downarrow \frac{S\{a \vee a\}}{S\{a\}} \qquad \mathsf{ac}\!\uparrow \frac{S\{a\}}{S\{a \wedge a\}} \qquad \mathsf{aw}\!\uparrow \frac{S\{a\}}{S\{\mathbf{t}\}}$$

$$\mathsf{nm}\!\downarrow \frac{S\{\mathbf{f}\}}{S\{\mathbf{f} \wedge \mathbf{f}\}} \qquad \mathsf{m}\ \frac{S\{(A \wedge B) \vee (C \wedge D)\}}{S\{[A \vee C] \wedge [B \vee D]\}} \qquad \mathsf{nm}\!\uparrow \frac{S\{\mathbf{t} \vee \mathbf{t}\}}{S\{\mathbf{t}\}}$$

$$\alpha\!\downarrow \frac{S\{A \vee [B \vee C]\}}{S\{[A \vee B] \vee C\}} \qquad \sigma\!\downarrow \frac{S\{A \vee B\}}{S\{B \vee A\}} \qquad \sigma\!\uparrow \frac{S\{A \wedge B\}}{S\{B \wedge A\}} \qquad \alpha\!\uparrow \frac{S\{A \wedge (B \wedge C)\}}{S\{(A \wedge B) \wedge C\}}$$

$$\mathbf{f}\!\downarrow \frac{S\{A\}}{S\{A \vee \mathbf{f}\}} \qquad \mathbf{t}\!\downarrow \frac{S\{A\}}{S\{A \wedge \mathbf{t}\}} \qquad \mathbf{t}\!\uparrow \frac{S\{\mathbf{f} \vee A\}}{S\{A\}} \qquad \mathbf{f}\!\uparrow \frac{S\{\mathbf{t} \wedge A\}}{S\{A\}}$$

Figure 8: System SKS

1.4.2 Exercise Complete the proof of Proposition 1.4.1.

1.4.3 Proposition *The rules* nm↓, nm↑, *and* m *are derivable in* SKSg.

Proof: The rules nm↓ and nm↑ are instances of w↓ and w↑, respectively. The rule m can be derived using w↓ and c↓ (see Exercise 1.4.4). □

1.4.4 Exercise Show how medial can be derived using w↓ and c↓. Can we also derive medial using w↑ and c↑?

1.4.5 Exercise Conclude that if there is a derivation from A to B in SKSg then there is one in SKS, and vice versa.

We use the following notation

$$\begin{array}{c} A \\ \mathscr{S}\big\Vert\Pi \\ B \end{array} \qquad \text{and} \qquad \begin{array}{c} \mathscr{S}\big\Vert\Pi' \\ B \end{array}$$

for denoting a derivation Π in system $\mathscr{S}$ from premise A to conclusion B, and a proof Π' of conclusion B in system $\mathscr{S}$, respectively, where a proof is a derivation with premise $\mathbf{t}$.

1.4.6 Theorem (Soundness and Completeness) *The formula $A \rightarrow B$ is a tautology if and only if there is a derivation*

$$\begin{array}{c} A \\ \mathsf{SKS}\big\Vert\Pi \\ B \end{array}$$

1.4.7 Exercise Prove the axioms of the Hilbert system H into using SKS.

The two systems in the calculus of structures that we presented so far have an interesting property. All inference rules come in pairs:

$$\rho\,\frac{S\{A\}}{S\{B\}} \qquad \text{and} \qquad \bar{\rho}\,\frac{S\{\bar{B}\}}{S\{\bar{A}\}} \tag{14}$$

where $\bar{\rho}$ is the *dual* of ρ, and is obtained from ρ by negating and exchanging premise and conclusion. For example, $\mathsf{c}{\downarrow}$ is the dual of $\mathsf{c}{\uparrow}$, and $\mathsf{i}{\uparrow}$ is the dual of $\mathsf{i}{\downarrow}$. The rules s and m are *self-dual.*

If the rules $\mathsf{i}{\downarrow}$, $\mathsf{i}{\uparrow}$, and s a derivable in a system $\mathscr{S}$, then $\mathscr{S}$ can derive for each rule also its dual:

1.4.8 Proposition *Let ρ and $\bar{\rho}$ be a pair of dual rules. Then $\bar{\rho}$ is derivable in the system* $\{\rho, \mathsf{i}{\downarrow}, \mathsf{i}{\uparrow}, \mathsf{s}\}$.

Proof: The rule $\bar{\rho}$ can be derived in the following way:

$$\bar{\rho}\,\frac{S\{\bar{B}\}}{S\{\bar{A}\}} \quad \rightsquigarrow \quad \mathsf{i}{\uparrow}\,\frac{\mathsf{s}\,\frac{\rho\,\frac{\mathsf{i}{\downarrow}\,\frac{S\{\bar{B}\}}{S\{\bar{B} \wedge [a \vee \bar{A}]\}}}{S\{\bar{B} \wedge [B \vee \bar{A}]\}}}{S\{(\bar{B} \wedge B) \vee \bar{A}\}}}{S\{\bar{A}\}} \tag{15}$$

□

In a well-defined system in the calculus of structures, *cut elimination* means not only the admissibility of the cut-rule $\mathsf{i}{\uparrow}$, but the admissibility of the whole *up fragment*, i.e., all rules with an $\uparrow$ in the name.

1.5 Notes

As the name says, Hilbert systems have been introduced by David Hilbert [Hil22, HA28]. Gödel's Incompleteness Theorem has been published in [Göd31]. Natural Deduction and the sequent calculus have been introduced by Gerhard Gentzen in [Gen34, Gen35], where he also presented cut elimination. There is a similar result for natural deduction, called *normalization*, which has first been described by Dag Prawitz [Pra65]. A standard textbook on proof theory, treating these issues in more detail is [TS00]. The calculus of structures is due to Alessio Guglielmi [Gug07, GS01]. The system SKS has first been presented by Kai Brünnler and Alwen Tiu [BT01, Brü03].

2 What is cut-elimination?

In the previous section we have already mentioned cut elimination. In this section we will give a complete proof. In fact, there will be two proofs, one using the sequent calculus, and one using the calculus of structures. Since a complete (syntactic) cut elimination proof is usually very tedious, we restrict ourselves to a rather rudimentary logic: multiplicative linear logic (MLL).

2.1 Sequent Calculus for MLL

Consider again the system shown in Figure 5 for classical logic. In this section we remove the rules for weakening and contraction. The result is called *unit-free multiplicative linear logic*. Since this is a different logic, there is also a different notation. Conjunction is written as $\otimes$, disjunction as $\parr$, and negation as $(-)^\perp$. What we get is the following system

$$\mathsf{id}\,\frac{}{\vdash a, a^\perp} \qquad \otimes\,\frac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \qquad \parr\,\frac{\vdash A, B, \Gamma}{\vdash A \parr B, \Gamma} \tag{16}$$

To simplify the presentation, we consider sequents as multisets (and not as lists), i.e., order does not matter (which means that we do not need the exchange rule). The system in (16) is called MLL^-, where the $-$ indicates the fact that the system is unit-free. For adding the units $\perp$ and $\mathbf{1}$ of linear logic, which correspond to *false* and *true* in classical logic, we need to add the rules

$$\mathbf{1}\,\frac{}{\vdash \mathbf{1}} \qquad \text{and} \qquad \perp\,\frac{\vdash \Gamma}{\vdash \perp, \Gamma} \tag{17}$$

The system consisting of the rules in (16) and (17) is denoted by MLL. The logic is called *multiplicative linear logic*.

Note that in MLL-formulas negation is only allowed at the atomic level, but we can define it inductively for all formulas via the deMorgan laws:

$$a^{\perp\perp} = a \qquad \mathbf{1}^\perp = \perp \qquad \perp^\perp = \mathbf{1} \qquad (A \otimes B)^\perp = A^\perp \parr B^\perp \qquad [A \parr B]^\perp = A^\perp \otimes B^\perp \tag{18}$$

This allows us to write the cut rule as

$$\mathsf{cut}\,\frac{\vdash A, \Gamma \quad \vdash A^\perp, \Delta}{\vdash \Gamma, \Delta}$$

As for classical logic, we have that the id-rule can be reduced to atoms, but the cut-rule cannot.

2.1.1 Proposition *The the general rule*

$$\mathsf{id}\,\frac{}{\vdash A, A^\perp}$$

is derivable in MLL.

Proof: We proceed by structural induction on A. If A is an atom, then we are done. If A is a unit, then we replace

$$\mathsf{id}\ \frac{}{\vdash \bot, \mathbf{1}} \qquad \text{by} \qquad \bot\ \frac{\mathbf{1}\ \dfrac{}{\vdash \mathbf{1}}}{\vdash \bot, \mathbf{1}}$$

If A is a compound formula, say $A = B \otimes C$, then we replace

$$\mathsf{id}\ \frac{}{\vdash B \otimes C, B^{\perp} \parr C^{\perp}} \qquad \text{by} \qquad \parr\ \frac{\otimes\ \dfrac{\mathsf{id}\ \dfrac{}{\vdash B, B^{\perp}} \quad \mathsf{id}\ \dfrac{}{\vdash C, C^{\perp}}}{\vdash B \otimes C, B^{\perp}, C^{\perp}}}{\vdash B \otimes C, B^{\perp} \parr C^{\perp}}$$

and apply the induction hypothesis. If $A = B \parr C$ we proceed similarly. □

As before, we have the cut-elimination theorem.

2.1.2 Theorem *If a sequent $\vdash \Gamma$ is provable in* $\mathsf{MLL} + \mathsf{cut}$*, then it is provable in* MLL *without cut.*

The proof of this theorem is for linear logic much simpler than for classical logic. For this reason we can show it here in full. We define the *size* of a proof Π, denoted by $\mathsf{size}(\Pi)$ to be the number of rule applications in Π. Now we begin by showing the following lemma:

2.1.3 Lemma *A proof of the shape*

$$\mathsf{cut}\ \frac{\overset{\Pi_1}{\vdash A, \Gamma} \qquad \overset{\Pi_2}{\vdash A^{\perp}, \Delta}}{\vdash \Gamma, \Delta} \tag{19}$$

where Π_1 and Π_2 are both cut-free, can be transformed into a cut-free proof

$$\overset{\Pi_3}{\vdash \Gamma, \Delta} \tag{20}$$

such that $\mathsf{size}(\Pi_3) < \mathsf{size}(\Pi_1) + \mathsf{size}(\Pi_2) + 1$.

Proof: We do this by induction on the size of the proof in (19), i.e., $\mathsf{size}(\Pi_1) + \mathsf{size}(\Pi_2) + 1$. We now proceed by a case analysis on the bottommost rules appearing in Π_1 and Π_2. If these rules do not interfere with the cut, we can permute them down, as in the following cases:

$$\mathsf{cut}\ \frac{\bot\ \dfrac{\overset{\Pi_1'}{\vdash A, \Gamma'}}{\vdash A, \bot, \Gamma'} \qquad \overset{\Pi_2}{\vdash A^{\perp}, \Delta}}{\vdash \bot, \Gamma', \Delta} \quad \to \quad \bot\ \frac{\mathsf{cut}\ \dfrac{\overset{\Pi_1'}{\vdash A, \Gamma'} \qquad \overset{\Pi_2}{\vdash A^{\perp}, \Delta}}{\vdash \Gamma', \Delta}}{\vdash \bot, \Gamma', \Delta} \tag{21}$$

$$\mathsf{cut}\,\dfrac{\parr\,\dfrac{\begin{matrix}\Pi'_1\\ \vdash A, C, D, \Gamma'\end{matrix}}{\vdash A, C \parr D, \Gamma'} \qquad \begin{matrix}\Pi_2\\ \vdash A^\perp, \Delta\end{matrix}}{\vdash C \parr D, \Gamma', \Delta} \quad \rightarrow \quad \parr\,\dfrac{\mathsf{cut}\,\dfrac{\begin{matrix}\Pi'_1\\ \vdash A, C, D, \Gamma'\end{matrix} \qquad \begin{matrix}\Pi_2\\ \vdash A^\perp, \Delta\end{matrix}}{\vdash C, D, \Gamma', \Delta}}{\vdash C \parr D, \Gamma', \Delta} \tag{22}$$

$$\mathsf{cut}\,\dfrac{\otimes\,\dfrac{\begin{matrix}\Pi'_1\\ \vdash C, \Gamma'\end{matrix} \qquad \begin{matrix}\Pi''_1\\ \vdash A, D, \Gamma''\end{matrix}}{\vdash A, C \otimes D, \Gamma', \Gamma''} \qquad \begin{matrix}\Pi_2\\ \vdash A^\perp, \Delta\end{matrix}}{\vdash C \otimes D, \Gamma', \Gamma'', \Delta} \quad \rightarrow \quad \otimes\,\dfrac{\begin{matrix}\Pi'_1\\ \vdash C, \Gamma'\end{matrix} \qquad \mathsf{cut}\,\dfrac{\begin{matrix}\Pi''_1\\ \vdash A, D, \Gamma''\end{matrix} \qquad \begin{matrix}\Pi_2\\ \vdash A^\perp, \Delta\end{matrix}}{\vdash D, \Gamma'', \Delta}}{\vdash C \otimes D, \Gamma', \Gamma'', \Delta} \tag{23}$$

And similarly for Π_2. In all these cases we can apply the induction hypothesis because the sum of the sizes of the proofs above the cut has been decreased. Note also that in all three cases the total size of the proof is not changed. In the literature on cut-elimination, cases like (21), (22), and (23) are called *commutative cases*. Let us now look at the cases where the rules above the cut apply to the formulas introduced by the cut. In the literature on cut-elimination, such cases are called *key cases*. For MLL, there are three key cases:

$$\mathsf{cut}\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash a, a^\perp} \qquad \begin{matrix}\Pi\\ \vdash a^\perp, \Delta\end{matrix}}{\vdash a^\perp, \Delta} \quad \rightarrow \quad \begin{matrix}\Pi\\ \vdash a^\perp, \Delta\end{matrix} \tag{24}$$

$$\mathsf{cut}\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash \mathbf{1}} \qquad \bot\,\dfrac{\begin{matrix}\Pi\\ \vdash \Delta\end{matrix}}{\vdash \bot, \Delta}}{\vdash \Delta} \quad \rightarrow \quad \begin{matrix}\Pi\\ \vdash \Delta\end{matrix} \tag{25}$$

$$\mathsf{cut}\,\dfrac{\otimes\,\dfrac{\begin{matrix}\Pi'_1\\ \vdash A, \Gamma'\end{matrix} \qquad \begin{matrix}\Pi''_1\\ \vdash B, \Gamma''\end{matrix}}{\vdash A \otimes B, \Gamma', \Gamma''} \qquad \parr\,\dfrac{\begin{matrix}\Pi'_2\\ \vdash A^\perp, B^\perp, \Delta\end{matrix}}{\vdash A^\perp \parr B^\perp, \Delta}}{\vdash \Gamma', \Gamma'', \Delta} \quad \rightarrow \quad \mathsf{cut}\,\dfrac{\begin{matrix}\Pi'_1\\ \vdash A, \Gamma'\end{matrix} \qquad \mathsf{cut}\,\dfrac{\begin{matrix}\Pi''_1\\ \vdash B, \Gamma_2\end{matrix} \qquad \begin{matrix}\Pi'_2\\ \vdash A^\perp, B^\perp, \Delta\end{matrix}}{\vdash A^\perp, \Gamma'', \Delta}}{\vdash \Gamma', \Gamma'', \Delta} \tag{26}$$

Note that in all three cases the total size of the proof is strictly decreased. In the first two cases the cut disappears. In case (26), the cut is replaced by two cuts, which means we need a slightly more sophisticated argument: First, note that we can apply the induction hypothesis to the proof

$$\mathsf{cut}\,\dfrac{\begin{matrix}\Pi''_1\\ \vdash B, \Gamma_2\end{matrix} \qquad \begin{matrix}\Pi'_2\\ \vdash A^\perp, B^\perp, \Delta\end{matrix}}{\vdash A^\perp, \Gamma'', \Delta}$$

because $\mathsf{size}(\Pi_1'') + \mathsf{size}(\Pi_2') + 1 < \mathsf{size}(\Pi_1') + \mathsf{size}(\Pi_1'') + \mathsf{size}(\Pi_2') + 3$. This gives us a proof

$$\begin{array}{c} \Pi_2'' \\ \vdots \\ \vdash A^\perp, \Gamma'', \Delta \end{array}$$

with

$$\mathsf{size}(\Pi_2'') < \mathsf{size}(\Pi_1'') + \mathsf{size}(\Pi_2') + 1 \quad .$$

Hence, we also have

$$\mathsf{size}(\Pi_1') + \mathsf{size}(\Pi_2'') + 1 < \mathsf{size}(\Pi_1') + \mathsf{size}(\Pi_1'') + \mathsf{size}(\Pi_2') + 3 \quad .$$

This means we can apply the induction hypothesis again to

$$\mathsf{cut}\,\frac{\begin{array}{c}\Pi_1' \\ \vdots \\ \vdash A, \Gamma'\end{array} \qquad \begin{array}{c}\Pi_2'' \\ \vdots \\ \vdash A^\perp, \Gamma'', \Delta\end{array}}{\vdash \Gamma', \Gamma'', \Delta}$$

which gives us a cut-free proof

$$\begin{array}{c} \Pi_3 \\ \vdots \\ \vdash \Gamma, \Delta \end{array} \tag{27}$$

such that

$$\begin{array}{rcl} \mathsf{size}(\Pi_3) & < & \mathsf{size}(\Pi_1') + \mathsf{size}(\Pi_2'') + 1 \\ & < & \mathsf{size}(\Pi_1') + \mathsf{size}(\Pi_1'') + \mathsf{size}(\Pi_2') + 3 \\ & = & \mathsf{size}(\Pi_1) + \mathsf{size}(\Pi_2) + 1 \end{array}$$

This completes the proof of the lemma.

Proof (of Theorem 2.1.2): The statement of the theorem now follows from Lemma 2.1.3 by an induction on the number of cuts in the proof of $\vdash \Gamma$. □

2.1.4 Remark The system MLL is an exceptionally simple case for cut elimination. In most other logics, the size of the proof *does not* decrease during cut elimination. Usually there is an exponential or even hyper-exponential blow-up of the proof when cut elimination is applied. In particular, in classical logic we have due to the presence of contraction the following case:

$$\mathsf{cut}\,\frac{\mathsf{cont}\,\dfrac{\begin{array}{c}\Pi_1 \\ \vdots \\ \vdash \Gamma, A, A\end{array}}{\vdash \Gamma, A} \qquad \begin{array}{c}\Pi_2 \\ \vdots \\ \vdash \bar{A}, \Delta\end{array}}{\vdash \Gamma, \Delta} \quad \to \quad \mathsf{cont}\,\dfrac{\begin{array}{c}\mathsf{cont}\,\dfrac{\mathsf{cut}\,\dfrac{\mathsf{cut}\,\dfrac{\begin{array}{c}\Pi_1 \\ \vdots \\ \vdash \Gamma, A, A\end{array} \qquad \begin{array}{c}\Pi_2 \\ \vdots \\ \vdash \bar{A}, \Delta\end{array}}{\vdash \Gamma, \Delta, A} \qquad \begin{array}{c}\Pi_2 \\ \vdots \\ \vdash \bar{A}, \Delta\end{array}}{\vdash \Gamma, \Delta, \Delta}}{} \\ \vdots \end{array}}{\vdash \Gamma, \Delta}$$

This means one has to find more sophisticated induction measures.

2.2 Calculus of structures for MLL

In the calculus of structures, multiplicative linear logic is given by the following system:

$$\mathsf{ai}{\downarrow}\,\frac{S\{\mathbf{1}\}}{S\{a \parr a^{\perp}\}} \qquad \mathsf{s}\,\frac{S\{[A \parr B] \otimes C\}}{S\{A \parr (B \otimes C)\}} \tag{28}$$

which we will call MLS. As mentioned in Section 1.4, we consider formulas equivalent modulo an equational theory. For the MLS, this is generated by the equations

$$\begin{array}{lll} A \otimes (B \otimes C) = (A \otimes B) \otimes C & A \otimes B = B \otimes A & A \otimes \mathbf{1} = A \\ A \parr [B \parr C] = [A \parr B] \parr C & A \parr B = B \parr A & A \parr \bot = A \end{array} \tag{29}$$

A *proof* in this system is a derivation with premise $\mathbf{1}$. A formula A is *provable* if there is a proof Π with conclusion A. We denote this by

$$\begin{array}{c} \mathbf{1} \\ \mathsf{MLS}\,\Big\Vert\,\Pi \\ A \end{array} \qquad \text{or simply by} \qquad \begin{array}{c} \mathsf{MLS}\,\Big\Vert\,\Pi \\ A \end{array}$$

The cut rule is

$$\mathsf{ai}{\uparrow}\,\frac{S\{a \otimes a^{\perp}\}}{S\{\bot\}} \tag{30}$$

In the the calculus of structures, the cut can be reduced to atomic form, which is not possible in the sequent calculus. The general form of the rules $\mathsf{ai}{\downarrow}$ and $\mathsf{ai}{\uparrow}$ are

$$\mathsf{i}{\downarrow}\,\frac{S\{\mathbf{1}\}}{S\{A \parr A^{\perp}\}} \qquad \text{and} \qquad \mathsf{i}{\uparrow}\,\frac{S\{A \otimes A^{\perp}\}}{S\{\bot\}} \tag{31}$$

2.2.1 Proposition *The rule* $\mathsf{i}{\downarrow}$ *is derivable in* $\{\mathsf{ai}{\downarrow}, \mathsf{s}\}$*, and the rule* $\mathsf{i}{\uparrow}$ *is derivable in* $\{\mathsf{ai}{\uparrow}, \mathsf{s}\}$*.*

Proof: The proof is very similar to the proof of Proposition 2.1.1. For $\mathsf{i}{\downarrow}$, the inductive cases are

$$\mathsf{i}{\downarrow}\,\frac{S\{\mathbf{1}\}}{S\{\bot \parr \mathbf{1}\}} \qquad \to \qquad =\,\frac{S\{\mathbf{1}\}}{S\{\bot \parr \mathbf{1}\}}$$

and

$$\mathsf{i}{\downarrow}\,\frac{S\{\mathbf{1}\}}{S\{(B \otimes C) \parr B^{\perp} \parr C^{\perp}\}} \qquad \to \qquad \mathsf{s}\,\frac{\mathsf{i}{\downarrow}\,\dfrac{=\,\dfrac{\mathsf{i}{\downarrow}\,\dfrac{S\{\mathbf{1}\}}{S\{C \parr C^{\perp}\}}}{S\{(\mathbf{1} \otimes C) \parr C^{\perp}\}}}{S\{([B \parr B^{\perp}] \otimes C) \parr C^{\perp}\}}}{S\{(B \otimes C) \parr B^{\perp} \parr C^{\perp}\}}$$

The cases for $\mathsf{i}{\uparrow}$ are dual. □

The system $\mathsf{MLS} + \mathsf{ai}{\uparrow}$ will be called SMLS. For this system, we have the cut elimination theorem:

2.2.2 Theorem *If a formula A is provable in* SMLS*, then it is provable in* MLS*.*

We can prove this theorem either by using the sequent calculus cut elimination, or by giving a direct proof in the calculus of structures. We show here both proofs. Before that, let us see some interesting consequences.

2.2.3 Corollary *The rule* $\mathsf{i}\!\uparrow$ *is admissible in* MLS*.*

Proof: Suppose we have a proof

$$\begin{array}{c} \mathsf{MLS}\cup\{\mathsf{i}\!\uparrow\}\,\Big\Vert\,\Pi \\ A \end{array}$$

By Proposition 2.2.1, this can be transformed into a proof

$$\begin{array}{c} \mathsf{SMLS}\,\Big\Vert\,\Pi' \\ A \end{array}$$

To this we apply Theorem 2.2.2. □

2.2.4 Corollary *For all formulas A and B, we have*

$$\begin{array}{c} A \\ \mathsf{SMLS}\,\Big\Vert\,\Pi_1 \\ B \end{array} \qquad \textit{if and only if} \qquad \begin{array}{c} \mathsf{MLS}\,\Big\Vert\,\Pi_2 \\ A^\perp \mathbin{⅋} B \end{array}$$

Proof: From

$$\begin{array}{c} A \\ \mathsf{SMLS}\,\Big\Vert\,\Pi_1 \\ B \end{array}$$

we can obtain

$$\begin{array}{c} \mathsf{i}\!\downarrow \dfrac{\mathbf{1}}{A^\perp \mathbin{⅋} A} \\ \mathsf{SMLS}\,\Big\Vert\,\Pi_1 \\ A^\perp \mathbin{⅋} B \end{array}$$

Via Proposition 2.2.1, we obtain

$$\begin{array}{c} \mathsf{SMLS}\,\Big\Vert \\ A^\perp \mathbin{⅋} B \end{array}$$

By Theorem 2.2.2 we get

$$\begin{array}{c} \mathsf{MLS}\,\Big\Vert\,\Pi_2 \\ A^\perp \mathbin{⅋} B \end{array}$$

Conversely, from

$$\begin{array}{c} \mathsf{MLS}\,\Big\Vert\,\Pi_2 \\ A^\perp \mathbin{⅋} B \end{array}$$

we can construct

$$
\begin{array}{c}
= \dfrac{A}{A \otimes \mathbf{1}} \\
\mathsf{MLS} \Big\| \Pi_2 \\
\mathsf{s}\,\dfrac{A \otimes [A^{\perp} \parr B]}{\mathsf{i}\!\uparrow \dfrac{(A \otimes A^{\perp}) \parr B}{= \dfrac{\perp \parr B}{B}}}
\end{array}
$$

From which we get

$$
\begin{array}{c}
A \\
\mathsf{SMLS} \Big\| \Pi_1 \\
B
\end{array}
$$

by applying Proposition 2.2.1. □

Now, let us establish the relation between the systems MLL and MLS.

2.2.5 Proposition *If there is a proof*

$$
\begin{array}{c}
\Pi \\
\vdash A_1, \ldots, A_n
\end{array}
$$

in MLL*, then there is a proof*

$$
\begin{array}{c}
\mathsf{MLS} \Big\| \Pi' \\
A_1 \parr \cdots \parr A_n
\end{array}
\quad .
$$

Proof: We proceed by induction on the size of the proof Π, and make a case analysis on the bottommost rule instance in Π:

$$
\mathsf{id}\,\dfrac{}{\vdash a, a^{\perp}} \quad \rightarrow \quad \mathsf{ai}\!\downarrow \dfrac{\mathbf{1}}{a \parr a^{\perp}}
$$

$$
\mathbf{1}\,\dfrac{}{\vdash \mathbf{1}} \quad \rightarrow \quad = \dfrac{\mathbf{1}}{\mathbf{1}}
$$

$$
\perp \dfrac{\begin{array}{c}\Pi_1 \\ \vdash A_2, \ldots, A_n\end{array}}{\vdash \perp, A_2, \ldots, A_n} \quad \rightarrow \quad \begin{array}{c}\mathsf{MLS} \Big\| \Pi'_1 \\ = \dfrac{A_2 \parr \cdots \parr A_n}{\perp \parr A_2 \parr \cdots \parr A_n}\end{array}
$$

$$
\parr \dfrac{\begin{array}{c}\Pi_1 \\ \vdash A'_1, A''_1, A_2, \ldots, A_n\end{array}}{\vdash A'_1 \parr A''_1, A_2, \ldots, A_n} \quad \rightarrow \quad \begin{array}{c}\mathsf{MLS} \Big\| \Pi'_1 \\ A'_1 \parr A''_1 \parr A_2 \parr \cdots \parr A_n\end{array}
$$

$$
\otimes\frac{\begin{array}{c}\Pi_1\\ \vdash A_1', A_2, \dots, A_k\end{array} \quad \begin{array}{c}\Pi_2\\ \vdash A_1'', A_{k+1}, \dots, A_n\end{array}}{\vdash A_1' \otimes A_1'', A_2, \dots, A_k, A_{k+1}, \dots, A_n}
\quad \rightarrow \quad
\begin{array}{c}
\mathsf{MLS}\Vert\Pi_2' \\
= \dfrac{A_1'' \mathbin{⅋} A_{k+1} \mathbin{⅋} \cdots \mathbin{⅋} A_n}{(\mathbf{1} \otimes A_1'') \mathbin{⅋} A_{k+1} \mathbin{⅋} \cdots \mathbin{⅋} A_n} \\
\mathsf{MLS}\Vert\Pi_1' \\
\mathsf{s}\dfrac{([A_1' \mathbin{⅋} A_2 \mathbin{⅋} \cdots \mathbin{⅋} A_k] \otimes A_1'') \mathbin{⅋} A_{k+1} \mathbin{⅋} \cdots \mathbin{⅋} A_n}{(A_1' \otimes A_1'') \mathbin{⅋} A_2 \mathbin{⅋} \cdots \mathbin{⅋} A_k \mathbin{⅋} A_{k+1} \mathbin{⅋} \cdots \mathbin{⅋} A_n}
\end{array}
$$

In all cases the derivations Π_1' and Π_2' are obtained via the induction hypothesis from Π_1 and Π_2. □

2.2.6 Proposition *If there is a proof*

$$
\begin{array}{c}\Pi\\ \vdash A_1, \dots, A_n\end{array}
$$

in $\mathsf{MLL} + \mathsf{cut}$*, then there is a proof*

$$
\begin{array}{c}\mathsf{SMLS}\Vert\Pi'\\ A_1 \mathbin{⅋} \cdots \mathbin{⅋} A_n\end{array} \quad .
$$

Proof: The proof is the same as the previous one. We only need to add the case for the cut:

$$
\otimes\frac{\begin{array}{c}\Pi_1\\ \vdash B, A_1, \dots, A_k\end{array} \quad \begin{array}{c}\Pi_2\\ \vdash B^\perp, A_{k+1}, \dots, A_n\end{array}}{\vdash A_1, \dots, A_k, A_{k+1}, \dots, A_n}
\quad \rightarrow \quad
\begin{array}{c}
\mathsf{MLS}\Vert\Pi_2' \\
= \dfrac{B^\perp \mathbin{⅋} A_{k+1} \mathbin{⅋} \cdots \mathbin{⅋} A_n}{(\mathbf{1} \otimes B^\perp) \mathbin{⅋} A_{k+1} \mathbin{⅋} \cdots \mathbin{⅋} A_n} \\
\mathsf{MLS}\Vert\Pi_1' \\
\mathsf{s}\dfrac{([B \mathbin{⅋} A_1 \mathbin{⅋} \cdots \mathbin{⅋} A_k] \otimes B^\perp) \mathbin{⅋} A_{k+1} \mathbin{⅋} \cdots \mathbin{⅋} A_n}{\mathsf{i}{\uparrow}\dfrac{(B \otimes B^\perp) \mathbin{⅋} A_1 \mathbin{⅋} \cdots \mathbin{⅋} A_k \mathbin{⅋} A_{k+1} \mathbin{⅋} \cdots \mathbin{⅋} A_n}{A_1 \mathbin{⅋} \cdots \mathbin{⅋} A_k \mathbin{⅋} A_{k+1} \mathbin{⅋} \cdots \mathbin{⅋} A_n}}
\end{array}
$$

Finally, we need to apply Proposition 2.2.1. □

2.2.7 Proposition *If there is a proof*

$$
\begin{array}{c}\mathsf{SMLS}\Vert\Pi\\ Q\end{array} \quad ,
$$

then there is a proof

$$
\begin{array}{c}\Pi'\\ \vdash Q\end{array}
$$

in $\mathsf{MLL} + \mathsf{cut}$.

Proof: Again, we proceed by induction on the size of Π, and consider the bottommost rule instance in Π:

$$\rho \frac{\begin{array}{c} \Vert \Pi_1 \\ Q_1 \end{array}}{Q}$$

By induction hypothesis, there is a proof

$$\begin{array}{c} \bigtriangledown \Pi'_1 \\ \vdash Q_1 \end{array}$$

in $\mathsf{MLL} + \mathsf{cut}$. Now we show that there is also a proof

$$\begin{array}{c} \bigtriangledown \Pi'_2 \\ \vdash Q_1^{\perp}, Q \end{array}$$

in $\mathsf{MLL} + \mathsf{cut}$, from which we can then construct Π':

$$\mathsf{cut} \frac{\begin{array}{c} \bigtriangledown \Pi'_1 \\ \vdash Q_1 \end{array} \qquad \begin{array}{c} \bigtriangledown \Pi'_2 \\ \vdash Q_1^{\perp}, Q \end{array}}{\vdash Q}$$

For constructing Π'_2, we first show for every rule

$$\rho \frac{S\{A\}}{S\{B\}}$$

there is a proof

$$\begin{array}{c} \bigtriangledown \\ \vdash A^{\perp}, B \end{array}$$

For $\mathsf{ai}\!\downarrow$ and $\mathsf{ai}\!\uparrow$, we have

$$\perp \frac{\parr \frac{\mathsf{id} \frac{}{\vdash a, a^{\perp}}}{\vdash a \parr a^{\perp}}}{\vdash \perp, a \parr a^{\perp}}$$

For s, we have

$$\parr \frac{\parr \frac{\otimes \frac{\mathsf{id} \frac{}{\vdash A^{\perp}, A} \qquad \otimes \frac{\mathsf{id} \frac{}{\vdash B^{\perp}, B} \qquad \mathsf{id} \frac{}{\vdash C^{\perp}, C}}{\vdash B^{\perp}, C^{\perp}, A, B \otimes C}}{\vdash A^{\perp} \otimes B^{\perp}, C^{\perp}, A, B \otimes C}}{\vdash A^{\perp} \otimes B^{\perp}, C^{\perp}, A \parr (B \otimes C)}}{\vdash (A^{\perp} \otimes B^{\perp}) \parr C^{\perp}, A \parr (B \otimes C)}$$

Similarly, we have to show for the equations in (29) that whenever $A = B$, then there is a proof

$$\begin{array}{c}\bigtriangledown\\ \vdash A^{\perp}, B\end{array}$$

We leave this as an exercise. Finally, it remains to show that for every positive context $S\{\ \}$, we have

$$\text{If}\quad \begin{array}{c}\bigtriangledown\\ \vdash A^{\perp}, B\end{array}\quad \text{then}\quad \begin{array}{c}\bigtriangledown\\ \vdash S\{A\}^{\perp}, S\{B\}\end{array}$$

For this, we proceed by induction on the structure of $S\{\ \}$. The inductive case is

$$\mathord{\bindnasrepma}\,\dfrac{\otimes\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash C^{\perp}, C} \qquad \begin{array}{c}\Pi''\\ \vdash S'\{A\}^{\perp}, S'\{B\}\end{array}}{\vdash C^{\perp} \otimes S'\{A\}^{\perp}, C, S\{B\}}}{\vdash C^{\perp} \otimes S'\{A\}^{\perp}, C \mathbin{\bindnasrepma} S\{B\}}$$

where Π'' exists by induction hypothesis. □

Now we are ready for the first proof of Theorem 2.2.2:

Proof (First proof of Theorem 2.2.2): A given proof in SMLS is first transformed into a proof in MLL + cut (by Proposition 2.2.7). To this proof we apply cut-elimination in the sequent calculus (Theorem 2.1.2). The result is translated into a proof in MLS (via Proposition 2.2.5). □

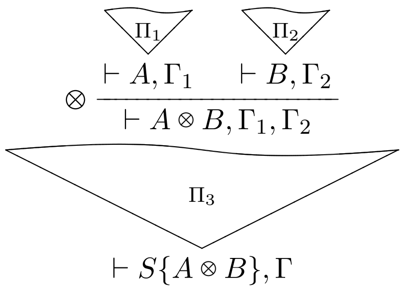
2.3 Splitting

The key argument for proving cut elimination in the sequent calculus (Theorem 2.1.2) relies on the following property: when the principal formulas in a cut are active in both branches, they determine which rules are applied immediately above the cut. This is a consequence of the fact that formulas have a root connective, and logical rules only hinge on that, and nowhere else in the formula.

This property does not necessarily hold in the calculus of structures. Further, since rules can be applied anywhere deep inside structures, everything can happen above a cut. This complicates the task of proving cut elimination. On the other hand, simplification is made possible by the reduction of cut to its atomic form, which happens simply and independently of cut elimination. The remaining difficulty is understanding what happens, while going up in a proof, *around* the atoms produced by an atomic cut. The two atoms of an atomic cut can be produced inside any structure, and they do not belong to distinct branches, as in the sequent calculus. In fact, complex interactions with their context are possible. The solution that we show here is called *splitting*.

It can be best understood by looking again at the sequent calculus. If we have an MLL-proof of the sequent $\vdash S\{A \otimes B\}, \Gamma$, where $S\{A \otimes B\}$ is a formula that contains the subformula

$A \otimes B$, we know for sure that somewhere in the proof there is one and only one instance of the $\otimes$ rule, which splits A and B along with their context. This is indicated below:



corresponds to

$$\begin{array}{c} \Vert \Pi_1 \\ A \parr \Gamma_1 \\ \Vert \Pi_2 \\ \mathsf{s}\dfrac{[A \parr \Gamma_1] \otimes [B \parr \Gamma_2]}{\mathsf{s}\dfrac{([A \parr \Gamma_1] \otimes B) \parr \Gamma_2}{(A \otimes B) \parr \Gamma_1 \parr \Gamma_2}} \\ \Vert \Pi_3 \\ S\{A \otimes B\} \parr \Gamma \end{array} \qquad (32)$$

We can consider, as shown at the left, the proof for the given sequent as composed of three pieces, Π_1, Π_2 and Π_3. In the calculus of structures, many different proofs correspond to the sequent calculus one: they differ for the possible sequencing of rules, and because rules in the calculus of structures have smaller granularity and larger applicability. But, among all these proofs, there must also be one that fits the scheme at the right in (32). This precisely illustrates the idea behind the splitting technique.

The derivation Π_3 above implements a *context reduction* and a proper splitting. We can state, in general, these principles separately as follows:

1. Context reduction: The idea of context reduction is to reduce a problem that concerns an arbitrary (deep) context $S\{\ \}$ to a problem that concerns only a shallow context $\{\ \} \parr U$. In the case of cut elimination, for example, we will then be able to apply splitting. In the example above, $S\{\ \} \parr \Gamma$ is reduced to $\{\ \} \parr \Gamma'$, for some Γ'.

2. Splitting: In the example above Γ' is reduced to $\Gamma_1 \parr \Gamma_2$. More generally, if $(A \otimes B) \parr K$ is provable, then K can be reduced to $K_A \parr K_B$, such that $A \parr K_A$ and $B \parr K_B$ are provable.

Context reduction is proved by splitting, which is at the core of the matter.

2.3.1 Lemma (Splitting) *Let A, B, K be formulas. If there is a derivation*

$$\begin{array}{c} \mathsf{MLS}\Vert \Pi \\ (A \otimes B) \parr K \end{array}$$

then there are formulas K_A and K_B such that

$$\begin{array}{c} K_A \parr K_B \\ \mathsf{MLS}\Vert \Pi_K \\ K \end{array} \qquad \textit{and} \qquad \begin{array}{c} \mathsf{MLS}\Vert \Pi_A \\ A \parr K_A \end{array} \qquad \textit{and} \qquad \begin{array}{c} \mathsf{MLS}\Vert \Pi_B \\ B \parr K_B \end{array}$$

where $\mathsf{size}(\Pi_A) + \mathsf{size}(\Pi_B) < \mathsf{size}(\Pi)$.

Proof: We proceed by induction on the size of Π. We consider the bottommost rule instance ρ in the proof Π. There are three diffent types of cases:

(a) Assume ρ is applied inside A. Then Π is

$$\rho \frac{\overset{\mathsf{MLS}\Vert\Pi'}{(A' \otimes B) \parr K}}{(A \otimes B) \parr K}$$

and we can apply the induction hypothesis to Π' because it has shorter length than Π. Hence, we get

$$\begin{array}{c} K_{A'} \parr K_B \\ \mathsf{MLS}\Vert\Pi_K \\ K \end{array} \quad \text{and} \quad \rho \frac{\overset{\mathsf{MLS}\Vert\Pi_{A'}}{A' \parr K_{A'}}}{A \parr K_{A'}} \quad \text{and} \quad \begin{array}{c} \mathsf{MLS}\Vert\Pi_B \\ B \parr K_B \end{array}$$

We have

$$\begin{array}{rcl} \mathsf{size}(\Pi_A) + \mathsf{size}(\Pi_B) & = & \mathsf{size}(\Pi_{A'}) + 1 + \mathsf{size}(\Pi_B) \\ & < & \mathsf{size}(\Pi') + 1 \\ & = & \mathsf{size}(\Pi) \end{array}$$

If ρ applies inside B or inside K, the situation is similar.

(b) The second type of case appears when the subformula $A \otimes B$ remains untouched by ρ. This means ρ is s. The most general form of this case is

$$\mathsf{s} \frac{\overset{\mathsf{MLS}\Vert\Pi'}{([(A \otimes B) \parr K_1 \parr K_3] \otimes K_2) \parr K_4}}{(A \otimes B) \parr (K_1 \otimes K_2) \parr K_3 \parr K_4}$$

Since the length of Π' is smaller than the length of Π, we can apply the induction hypothesis to Π'. This gives us

$$\begin{array}{c} Q_1 \parr Q_2 \\ \mathsf{MLS}\Vert\Pi_1 \\ K_4 \end{array} \quad \text{and} \quad \begin{array}{c} \mathsf{MLS}\Vert\Pi_2 \\ (A \otimes B) \parr K_1 \parr K_3 \parr Q_1 \end{array} \quad \text{and} \quad \begin{array}{c} \mathsf{MLS}\Vert\Pi_3 \\ K_2 \parr Q_2 \end{array}$$

where $\mathsf{size}(\Pi_2) + \mathsf{size}(\Pi_3) < \mathsf{size}(\Pi')$. In particular, we have $\mathsf{size}(\Pi_2) < \mathsf{size}(\Pi')$. Hence we can apply the induction hypothesis to Π_2. From this we get

$$\begin{array}{c} K_A \parr K_B \\ \mathsf{MLS}\Vert\Pi_4 \\ K_1 \parr K_3 \parr Q_1 \end{array} \quad \text{and} \quad \begin{array}{c} \mathsf{MLS}\Vert\Pi_A \\ A \parr K_A \end{array} \quad \text{and} \quad \begin{array}{c} \mathsf{MLS}\Vert\Pi_B \\ B \parr K_B \end{array}$$

where $\mathsf{size}(\Pi_A) + \mathsf{size}(\Pi_B) < \mathsf{size}(\Pi_2) < \mathsf{size}(\Pi)$ and we can build Π_K as follows:

$$
\begin{array}{c}
K_A \parr K_B \\
\mathsf{MLS}\Big\Vert\Pi_4 \\
= \dfrac{K_1 \parr K_3 \parr Q_1}{(K_1 \otimes \mathbf{1}) \parr K_3 \parr Q_1} \\
\mathsf{MLS}\Big\Vert\Pi_3 \\
\mathsf{s}\,\dfrac{(K_1 \otimes [K_2 \parr Q_2]) \parr K_3 \parr Q_1}{(K_1 \otimes K_2) \parr K_3 \parr Q_1 \parr Q_2} \\
\mathsf{MLS}\Big\Vert\Pi_1 \\
(K_1 \otimes K_2) \parr K_3 \parr K_4
\end{array}
$$

"Morally", this case is similar to the commutative cases in the sequent calculus.

(c) Finally, we have consider the situations where the subformula $A \otimes B$ is destroyed by ρ. Again this means ρ is s. The most general form of this case is

$$
\begin{array}{c}
\mathsf{MLS}\Big\Vert\Pi' \\
\mathsf{s}\,\dfrac{([(A_1 \otimes B_1) \parr K_1] \otimes A_2 \otimes B_2) \parr K_2}{(A_1 \otimes A_2 \otimes B_1 \otimes B_2) \parr K_1 \parr K_2}
\end{array}
$$

For the same reasons as before, we can apply the induction hypothesis to Π':

$$
\begin{array}{c}
Q_1 \parr Q_2 \\
\mathsf{MLS}\Big\Vert\Pi_1 \\
K_2
\end{array}
\quad \text{and} \quad
\begin{array}{c}
\mathsf{MLS}\Big\Vert\Pi_2 \\
(A_1 \otimes B_1) \parr K_1 \parr Q_1
\end{array}
\quad \text{and} \quad
\begin{array}{c}
\mathsf{MLS}\Big\Vert\Pi_3 \\
(A_2 \otimes B_2) \parr Q_2
\end{array}
$$

where $\mathsf{size}(\Pi_2) + \mathsf{size}(\Pi_3) < \mathsf{size}(\Pi')$. In particular, we have $\mathsf{size}(\Pi_2) < \mathsf{size}(\Pi)$ and $\mathsf{size}(\Pi_3) < \mathsf{size}(\Pi)$, which allows us to apply the induction hypothesis to Π_2 and Π_3. We get:

$$
\begin{array}{c}
K_{A_1} \parr K_{B_1} \\
\mathsf{MLS}\Big\Vert\Pi_4 \\
K_1 \parr Q_1
\end{array}
\quad \text{and} \quad
\begin{array}{c}
\mathsf{MLS}\Big\Vert\Pi_5 \\
A_1 \parr K_{A_1}
\end{array}
\quad \text{and} \quad
\begin{array}{c}
\mathsf{MLS}\Big\Vert\Pi_6 \\
B_1 \parr K_{B_1}
\end{array}
$$

where $\mathsf{size}(\Pi_5) + \mathsf{size}(\Pi_6) < \mathsf{size}(\Pi_2)$ and

$$
\begin{array}{c}
K_{A_2} \parr K_{B_2} \\
\mathsf{MLS}\Big\Vert\Pi_7 \\
Q_2
\end{array}
\quad \text{and} \quad
\begin{array}{c}
\mathsf{MLS}\Big\Vert\Pi_8 \\
A_2 \parr K_{A_2}
\end{array}
\quad \text{and} \quad
\begin{array}{c}
\mathsf{MLS}\Big\Vert\Pi_9 \\
B_2 \parr K_{B_2}
\end{array}
$$

where $\mathsf{size}(\Pi_8) + \mathsf{size}(\Pi_9) < \mathsf{size}(\Pi_3)$. We let $K_A = K_{A_1} \parr K_{A_2}$ and $K_B = K_{B_1} \parr K_{B_2}$, and we can put all the bits and pieces together as follows:

$$= \frac{K_{A_1} \parr K_{A_2} \parr K_{B_1} \parr K_{B_2}}{\dfrac{K_{A_1} \parr K_{B_1} \parr K_{A_2} \parr K_{B_2}}{\dfrac{\mathsf{MLS}\,\|\,\Pi_4}{\dfrac{K_1 \parr Q_1 \parr K_{A_2} \parr K_{B_2}}{\dfrac{\mathsf{MLS}\,\|\,\Pi_7}{\dfrac{K_1 \parr Q_1 \parr Q_2}{\dfrac{\mathsf{MLS}\,\|\,\Pi_1}{K_1 \parr K_2}}}}}}} \qquad \text{and} \qquad \begin{array}{c} \mathsf{MLS}\,\|\,\Pi_5 \\ = \dfrac{A_1 \parr K_{A_1}}{(A_1 \otimes \mathbf{1}) \parr K_{A_1}} \\ \mathsf{MLS}\,\|\,\Pi_8 \\ \mathsf{s}\,\dfrac{(A_1 \otimes [A_2 \parr K_{A_2}]) \parr K_{A_1}}{(A_1 \otimes A_2) \parr K_{A_1} \parr K_{A_2}} \end{array}$$

and similarly we get a proof of $(B_1 \otimes B_2) \parr K_{B_1} \parr K_{B_2}$. This gives us

$$\mathsf{size}(\Pi_A) = \mathsf{size}(\Pi_5) + \mathsf{size}(\Pi_8) + 1 \qquad \text{and} \qquad \mathsf{size}(\Pi_B) = \mathsf{size}(\Pi_6) + \mathsf{size}(\Pi_9) + 1 \quad .$$

Note that we also have

$$\mathsf{size}(\Pi_5) + \mathsf{size}(\Pi_6) + 1 \leq \mathsf{size}(\Pi_2) \qquad \text{and} \qquad \mathsf{size}(\Pi_8) + \mathsf{size}(\Pi_9) + 1 \leq \mathsf{size}(\Pi_3) \quad .$$

Hence, we have

$$\begin{array}{rcl} \mathsf{size}(\Pi_A) + \mathsf{size}(\Pi_B) & = & \mathsf{size}(\Pi_5) + \mathsf{size}(\Pi_8) + \mathsf{size}(\Pi_6) + \mathsf{size}(\Pi_9) + 2 \\ & \leq & \mathsf{size}(\Pi_2) + \mathsf{size}(\Pi_3) \\ & < & \mathsf{size}(\Pi) \end{array}$$

as desired. □

2.3.2 Lemma (Atomic "splitting") *Let a be an atom and let K be a formula. If $a \parr K$ is provable in* MLS*, then there is a derivation*

$$\begin{array}{c} a^{\perp} \\ \mathsf{MLS}\,\| \\ K \end{array}$$

Proof: Exercise. □

2.3.3 Lemma (Context Reduction) *Let A be a formula, and let $S\{\ \}$ be a context. If $S\{A\}$ is provable in* MLS*, then there is a formula K_A, such that*

$$\begin{array}{c} \{\ \} \parr K_A \\ \mathsf{MLS}\,\|\,\Pi_S \\ S\{\ \} \end{array} \qquad \textit{and} \qquad \begin{array}{c} \mathsf{MLS}\,\|\,\Pi_A \\ A \parr K_A \end{array}$$

Proof: We proceed by induction on the size of $S\{\ \}$. There is only one case to consider, namely, $S\{\ \}$ is of the shape $(S'\{\ \} \otimes B) \parr C$ where $B \neq \mathbf{1}$ (but we allow $C = \bot$). Then we apply splitting (Lemma 2.3.1) to the proof of $(S'\{A\} \otimes B) \parr C$, which gives us

$$\begin{array}{c} C_S \parr C_B \\ \mathsf{MLS}\Big\| \Pi_1 \\ C \end{array} \qquad \text{and} \qquad \begin{array}{c} \mathsf{MLS}\Big\| \Pi_2 \\ S'\{A\} \parr C_S \end{array} \qquad \text{and} \qquad \begin{array}{c} \mathsf{MLS}\Big\| \Pi_3 \\ B \parr C_B \end{array}$$

Because $B \neq \mathbf{1}$, we can now apply the induction hypothesis to Π_2. This gives us

$$\begin{array}{c} \{\ \} \parr K_A \\ \mathsf{MLS}\Big\| \Pi_4 \\ S'\{\ \} \parr C_S \end{array} \qquad \text{and} \qquad \begin{array}{c} \mathsf{MLS}\Big\| \Pi_A \\ A \parr K_A \end{array}$$

From this we can get Π_S as follows:

$$\begin{array}{c} \{\ \} \parr K_A \\ \mathsf{MLS}\Big\| \Pi_4 \\ S'\{\ \} \parr C_S \\ \mathsf{MLS}\Big\| \Pi_3 \\ \mathsf{s}\,\dfrac{(S'\{\ \} \otimes [B \parr C_B]) \parr C_S}{(S'\{\ \} \otimes B) \parr C_S \parr C_B} \\ \mathsf{MLS}\Big\| \Pi_1 \\ (S'\{\ \} \otimes B) \parr C \end{array}$$

□

Now we can put the pieces together.

Proof (Second proof of Theorem 2.2.2): Let a proof Π of a formula A in SMLS be given. We proceed by induction on the number of instances of $\mathsf{ai}\!\uparrow$ in Π. If this number is zero, then Π is in MLS, and we are done. So, let us assume there is at least one $\mathsf{ai}\!\uparrow$ in Π. Let us consider the topmost instance of $\mathsf{ai}\!\uparrow$ in Π, i.e., for us Π looks as follows:

$$\begin{array}{c} \mathsf{MLS}\Big\| \Pi_1 \\ \mathsf{ai}\!\uparrow\dfrac{S\{a \otimes a^\bot\}}{S\{\bot\}} \\ \mathsf{SMLS}\Big\| \Pi_2 \\ A \end{array}$$

To Π_1, we can apply context reduction (Lemma 2.3.3). This gives us a K such that

$$\begin{array}{c} \{\ \} \parr K \\ \mathsf{MLS}\Big\| \Pi_3 \\ S\{\ \} \end{array} \qquad \text{and} \qquad \begin{array}{c} \mathsf{MLS}\Big\| \Pi_4 \\ (a \otimes a^\bot) \parr K \end{array}$$

From Π_3 we get

$$\begin{array}{c} K \\ \mathsf{MLS}\Big\Vert\Pi_3' \\ S\{\bot\} \end{array}$$

and to Π_4 we can apply splitting (Lemma 2.3.1), which gives us

$$\begin{array}{c} K_1 \parr K_2 \\ \mathsf{MLS}\Big\Vert\Pi_5 \\ K \end{array} \qquad \text{and} \qquad \begin{array}{c} \mathsf{MLS}\Big\Vert\Pi_6 \\ a \parr K_1 \end{array} \qquad \text{and} \qquad \begin{array}{c} \mathsf{MLS}\Big\Vert\Pi_7 \\ a^\bot \parr K_2 \end{array}$$

To Π_6 and Π_7, we can apply atomic splitting (Lemma 2.3.2), which gives us

$$\begin{array}{c} a^\bot \\ \mathsf{MLS}\Big\Vert\Pi_8 \\ K_1 \end{array} \qquad \text{and} \qquad \begin{array}{c} a \\ \mathsf{MLS}\Big\Vert\Pi_9 \\ K_2 \end{array}$$

Now we simply put all the bits and pieces together to get a proof Π' of A in which one instance of $\mathsf{ai}\!\uparrow$ is removed:

$$\begin{array}{c} \mathsf{ai}\!\downarrow \dfrac{\mathbf{1}}{a^\bot \parr a} \\ \mathsf{MLS}\Big\Vert\Pi_8,\Pi_9 \\ K_1 \parr K_2 \\ \mathsf{MLS}\Big\Vert\Pi_5 \\ K \\ \mathsf{MLS}\Big\Vert\Pi_3' \\ S\{\bot\} \\ \mathsf{SMLS}\Big\Vert\Pi_2 \\ A \end{array}$$

Hence, we can apply the induction hypothesis. □

2.4 Exponentials

Now we reintroduce contraction and weakening in a restricted form, by using *modalities*. These are unary connectives. In linear logic, they are denoted by ? and !, i.e., if A is a formula, then so are $?A$ and $!A$. They are dual to each other, i.e., for defining negation for all formulas, the equations in (18) have to be extended by

$$(!A)^\bot = ?A^\bot \qquad (?A)^\bot = !A^\bot \tag{33}$$

The sequent calculus rules for these modalities are:

$$?\mathsf{w}\,\frac{\vdash \Gamma}{\vdash ?A, \Gamma} \qquad ?\mathsf{c}\,\frac{\vdash ?A, ?A, \Gamma}{\vdash ?A, \Gamma} \qquad ?\mathsf{d}\,\frac{\vdash A, \Gamma}{\vdash ?A, \Gamma} \qquad !\mathsf{p}\,\frac{\vdash A, ?B_1, \ldots, ?B_n}{\vdash !A, ?B_1, \ldots, ?B_n} \tag{34}$$

where in the $!\mathsf{p}$-rule we have that $n \geq 0$. The system consisting of set of rules in (16), (17) and (34) is called MELL (without the rules in (17) it is denoted by MELL^-). The logic is called *multiplicative exponential linear logic*. For MELL, we have the cut elimination result:

2.4.1 Theorem *If a sequent* $\vdash \Gamma$ *is provable in* $\mathsf{MELL}+\mathsf{cut}$, *then it is provable in* MELL *without cut.*

The proof is much more involved than for MLL, and we do not show it here. The main problem is finding the right induction measure, since one cut reduction case is as follows:

$$\mathsf{cut}\,\dfrac{?\mathsf{c}\,\dfrac{\begin{array}{c}\Pi_1\\ \vdash \Gamma, ?A, ?A\end{array}}{\vdash \Gamma, ?A} \qquad !\mathsf{p}\,\dfrac{\begin{array}{c}\Pi_2\\ \vdash A, ?B_1, \ldots, ?B_n\end{array}}{\vdash !A, ?B_1, \ldots, ?B_n}}{\vdash \Gamma, ?B_1, \ldots, ?B_n}$$

is reduced to

$$?\mathsf{c}\,\dfrac{\begin{array}{c}?\mathsf{c}\,\dfrac{\mathsf{cut}\,\dfrac{\mathsf{cut}\,\dfrac{\begin{array}{c}\Pi_1\\ \vdash \Gamma, ?A, ?A\end{array} \qquad !\mathsf{p}\,\dfrac{\begin{array}{c}\Pi_2\\ \vdash A, ?B_1, \ldots, ?B_n\end{array}}{\vdash !A, ?B_1, \ldots, ?B_n}}{\vdash \Gamma, ?A, ?B_1, \ldots, ?B_n} \qquad !\mathsf{p}\,\dfrac{\begin{array}{c}\Pi_2\\ \vdash A, ?B_1, \ldots, ?B_n\end{array}}{\vdash !A, ?B_1, \ldots, ?B_n}}{\vdash \Gamma, ?B_1, \ldots, ?B_n, ?B_1, \ldots, ?B_n}}{\vdots}\end{array}}{\vdash \Gamma, ?B_1, \ldots, ?B_n}$$

where the proof Π_2 has been duplicated.

For the equivalent system in the calculus of structures, we add the following rules to MLS:

$$\mathsf{e}{\downarrow}\,\frac{S\{\mathbf{1}\}}{S\{!\mathbf{1}\}} \qquad \mathsf{p}{\downarrow}\,\frac{S\{![A \parr B]\}}{S\{[!A \parr ?B]\}} \qquad \mathsf{w}{\downarrow}\,\frac{S\{\bot\}}{S\{?A\}} \qquad \mathsf{b}{\downarrow}\,\frac{S\{[?A \parr A]\}}{S\{?A\}} \qquad \mathsf{g}{\downarrow}\,\frac{S\{??A\}}{S\{?A\}} \tag{35}$$

We use the same equational theory as before, and we write ELS to denote the system MLS extended by the rules in (35). To get the symmetric version SELS of that system, we need to add the duals of these rules as well:

$$\mathsf{e}{\uparrow}\,\frac{S\{?\bot\}}{S\{\bot\}} \qquad \mathsf{p}{\uparrow}\,\frac{S\{(?A \otimes !B)\}}{S\{?(A \otimes B)\}} \qquad \mathsf{w}{\uparrow}\,\frac{S\{!A\}}{S\{\mathbf{1}\}} \qquad \mathsf{b}{\uparrow}\,\frac{S\{!A\}}{S\{(!A \otimes A)\}} \qquad \mathsf{g}{\uparrow}\,\frac{S\{!A\}}{S\{!!A\}} \tag{36}$$

As before, the general versions of $\mathsf{i}{\downarrow}$ and $\mathsf{i}{\uparrow}$ can be reduced to their atomic version:

2.4.2 Proposition *The rule* $\mathsf{i}{\downarrow}$ *is derivable in* $\{\mathsf{ai}{\downarrow}, \mathsf{s}, \mathsf{e}{\downarrow}, \mathsf{p}{\downarrow}\}$, *and the rule* $\mathsf{i}{\uparrow}$ *is derivable in* $\{\mathsf{ai}{\uparrow}, \mathsf{s}, \mathsf{e}{\uparrow}, \mathsf{p}{\uparrow}\}$.

The proof is similar to the one for Proposition 2.2.1 where ! and ? where not in the language. The cut elimination theorem also holds:

2.4.3 Theorem *If a formula A is provable in* SELS*, then it is provable in* ELS*.*

As before, we can prove this theorem either by using the sequent calculus cut elimination, or by giving a direct proof in the calculus of structures. We will not go into further details here, but note that we have the same corollaries as for MLS, and they can be proved in exactly the same way:

2.4.4 Corollary *The rule* $\mathsf{i}{\uparrow}$ *is admissible in* ELS*.*

2.4.5 Corollary *For all formulas A and B, we have*

$$\begin{array}{c} A \\ \mathsf{SELS}\,\Big\|\,\Pi_1 \\ B \end{array} \qquad \textit{if and only if} \qquad \begin{array}{c} \mathsf{ELS}\,\Big\|\,\Pi_2 \\ A^{\perp} \parr B \end{array}$$

The relation between the systems MELL in the sequent calculus and ELS in the calculus of structures is as expected.

2.4.6 Proposition *If there is a proof*

$$\begin{array}{c} \nabla\,\Pi \\ \vdash A_1, \ldots, A_n \end{array}$$

in MELL*, then there is a proof*

$$\begin{array}{c} \mathsf{ELS}\,\Big\|\,\Pi' \\ A_1 \parr \cdots \parr A_n \end{array} .$$

2.4.7 Proposition *If there is a proof*

$$\begin{array}{c} \nabla\,\Pi \\ \vdash A_1, \ldots, A_n \end{array}$$

in MELL + cut*, then there is a proof*

$$\begin{array}{c} \mathsf{SELS}\,\Big\|\,\Pi' \\ A_1 \parr \cdots \parr A_n \end{array} .$$

2.4.8 Proposition *If there is a proof*

$$\begin{array}{c} \mathsf{SELS}\,\Big\|\,\Pi \\ Q \end{array} ,$$

then there is a proof

$$\begin{array}{c} \nabla\,\Pi' \\ \vdash Q \end{array}$$

in MELL + cut*.*

All three propositions are proved in the same way as for MLL and MLS.

Finally, we have for SELS a property, that has no counterpart in the sequent calculus:

2.4.9 Theorem *Every derivation*

$$\begin{array}{c} P \\ {\scriptstyle \mathsf{SELS}}\Vert \\ Q \end{array}$$

can be decomposed into

$$
\begin{array}{c} P \\ {\scriptstyle \mathsf{e}\downarrow}\Vert \\ P_1 \\ {\scriptstyle \mathsf{g}\uparrow}\Vert \\ P_2 \\ {\scriptstyle \mathsf{b}\uparrow}\Vert \\ P_3 \\ {\scriptstyle \mathsf{ai}\downarrow}\Vert \\ P_4 \\ {\scriptstyle \mathsf{w}\downarrow}\Vert \\ P_5 \\ {\scriptstyle \mathsf{s},\mathsf{p}\downarrow,\mathsf{p}\uparrow}\Vert \\ Q_5 \\ {\scriptstyle \mathsf{w}\uparrow}\Vert \\ Q_4 \\ {\scriptstyle \mathsf{ai}\uparrow}\Vert \\ Q_3 \\ {\scriptstyle \mathsf{b}\downarrow}\Vert \\ Q_2 \\ {\scriptstyle \mathsf{g}\downarrow}\Vert \\ Q_1 \\ {\scriptstyle \mathsf{e}\uparrow}\Vert \\ Q \end{array}
\qquad
\begin{array}{c} P \\ {\scriptstyle \mathsf{g}\uparrow}\Vert \\ U_1 \\ {\scriptstyle \mathsf{b}\uparrow}\Vert \\ U_2 \\ {\scriptstyle \mathsf{e}\downarrow}\Vert \\ U_3 \\ {\scriptstyle \mathsf{w}\downarrow}\Vert \\ U_4 \\ {\scriptstyle \mathsf{ai}\downarrow}\Vert \\ U_5 \\ {\scriptstyle \mathsf{s},\mathsf{p}\downarrow,\mathsf{p}\uparrow}\Vert \\ V_5 \\ {\scriptstyle \mathsf{ai}\uparrow}\Vert \\ V_4 \\ {\scriptstyle \mathsf{w}\uparrow}\Vert \\ V_3 \\ {\scriptstyle \mathsf{e}\uparrow}\Vert \\ V_2 \\ {\scriptstyle \mathsf{b}\downarrow}\Vert \\ V_1 \\ {\scriptstyle \mathsf{g}\downarrow}\Vert \\ Q \end{array}
\qquad
\begin{array}{c} P \\ {\scriptstyle \mathsf{e}\downarrow}\Vert \\ W_1 \\ {\scriptstyle \mathsf{g}\uparrow}\Vert \\ W_2 \\ {\scriptstyle \mathsf{b}\uparrow}\Vert \\ W_3 \\ {\scriptstyle \mathsf{w}\uparrow}\Vert \\ W_4 \\ {\scriptstyle \mathsf{ai}\downarrow}\Vert \\ W_5 \\ {\scriptstyle \mathsf{s},\mathsf{p}\downarrow,\mathsf{p}\uparrow}\Vert \\ Z_5 \\ {\scriptstyle \mathsf{ai}\uparrow}\Vert \\ Z_4 \\ {\scriptstyle \mathsf{w}\downarrow}\Vert \\ Z_3 \\ {\scriptstyle \mathsf{b}\downarrow}\Vert \\ Z_2 \\ {\scriptstyle \mathsf{g}\downarrow}\Vert \\ Z_1 \\ {\scriptstyle \mathsf{e}\uparrow}\Vert \\ Q \end{array}
\qquad
\begin{array}{c} P \\ {\scriptstyle \mathsf{g}\uparrow}\Vert \\ T_1 \\ {\scriptstyle \mathsf{b}\uparrow}\Vert \\ T_2 \\ {\scriptstyle \mathsf{w}\uparrow}\Vert \\ T_3 \\ {\scriptstyle \mathsf{e}\downarrow}\Vert \\ T_4 \\ {\scriptstyle \mathsf{ai}\downarrow}\Vert \\ T_5 \\ {\scriptstyle \mathsf{s},\mathsf{p}\downarrow,\mathsf{p}\uparrow}\Vert \\ R_5 \\ {\scriptstyle \mathsf{ai}\uparrow}\Vert \\ R_4 \\ {\scriptstyle \mathsf{e}\uparrow}\Vert \\ R_3 \\ {\scriptstyle \mathsf{w}\downarrow}\Vert \\ R_2 \\ {\scriptstyle \mathsf{b}\downarrow}\Vert \\ R_1 \\ {\scriptstyle \mathsf{g}\downarrow}\Vert \\ Q \end{array}
$$

The four statements are called first, second, third, and fourth decomposition (from left to right).

Apart from a decomposition into eleven subsystems, the first and the second decomposition can also be read as a decomposition into three subsystems that could be called *creation*, *merging* and *destruction*. In the creation subsystem, each rule increases the size of the structure; in the merging system, each rule does some rearranging of substructures, without changing the size of the structures; and in the destruction system, each rule decreases the size of the structure. Here, the size of the structure incorporates not only the number of atoms in it, but also the modality-depth for each atom. In a decomposed derivation, the merging part is in the middle of the derivation, and (depending on your preferred reading of a derivation) the creation and destruction are at the top and at the bottom, as shown in the left of Figure 9. In system SELS the merging part contains the rules s, p↓ and p↑. In

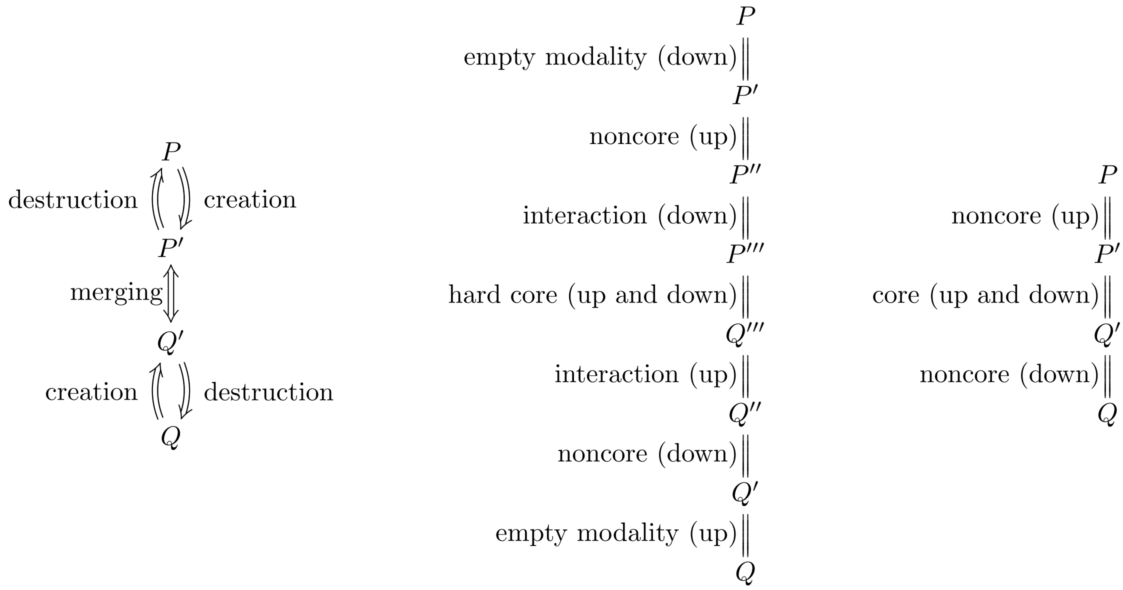


Figure 9: Readings of the decompositions

the top-down reading of a derivation, the creation part contains the rules e↓, g↑, b↑, w↓ and ai↓, and the destruction part consists of e↑, g↓, b↓, w↑ and ai↑. In the bottom-up reading, creation and destruction are exchanged.

This kind of decomposition (creation, merging, destruction) is quite typical for logical systems presented in the calculus of structures. It also hold for classical logic, for full propositional linear logic, and for non-commutative variants of linear logic.

The third decomposition allows a separation between hard core and noncore of the system[1], such that the up fragment and the down fragment of the noncore are not merged, as it is the case in the first and second decomposition. More precisely, we can separate the seven subsystems shown in the middle of Figure 9. The fourth decompostion is even stronger in this respect: it allows a complete separation between core and noncore, as shown on the right of Figure 9. This decomposition also plays a crucial rule for the cut elimination argument. Recall that cut elimination means to get rid of the entire up-fragment. Because of the decomposition, the elimination of the non-core up-fragment is now trivial. Furthermore, recall that for cut elimination in the sequent calculus, the most problematic cases are usually the ones where cut interacts with rules like contraction and weakening, and that in our system these rules appear as the non-core down rules. In the third decomposition these are *below* the actual cut rules (i.e., the core up rules, cf. Proposition 2.4.2) and can therefore no longer interfere with the cut elimination. This considerably simplifies the cut elimination argument.

2.5 Notes

The first cut elimination proof has been presented by Gentzen in [Gen34, Gen35]. A simplification of Gentzen's proof can be found in [GLT89]. For a variant of linear logic cut

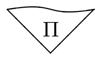
[1] We call *core* the set of rules needed to reduce the general i↓ and i↑ to their atomic versions, and *noncore* all others. The *hard core* are those core rules that are not e↓, e↑, ai↓, or ai↑.

elimination has first been proved by Lambek [Lam58]. For full linear logic it has been proved by Girard [Gir87]. For linear logic presented in the calculus of structures, the first direct proof of cut elimination was also based on rule permutation (similar to the sequent calculus) [Str03a, Str03b]. The idea of using splitting is due to Guglielmi [Gug07]. Decomposition has first been presented in [Str03b, Str03a]. The four decomposition theorems shown here are proved together in [SG09] for a richer logic. But the proof also applies to MELL.

3 What are proof nets?

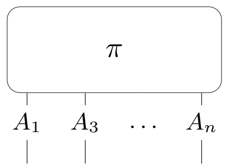
Today we learn about proof nets. The various notions of proof nets that exist in the literature can be grouped into two different *ideologies*:

Sequent Rule Ideology: A proof net is a graph in which every vertex represents an inference rule application in the corresponding sequent calculus proof, and every edge of the graph stands for a formula appearing in the proof. A sequent calculus proof with conclusion $\vdash A_1, A_2, \ldots, A_n$, written as



$$A_1, A_2, \ldots, A_n$$

is translated into a proof net with conclusions $A_1, A_2, \ldots, A_n$, written as



Flow Graph Ideology: A proof net consists of the formula tree/sequent forest of the conclusion of the proof, together with some additional graph structure capturing the "essence" of the proof (whatever that means).

For now, we will consider only multiplicative linear logic without units (MLL^-), for which the two ideologies yield the same notion of proof nets.

3.1 Unit-free multiplicative linear logic

Here is a set of inference rules for MLL^- given in the formalism of the *sequent calculus*:

$$\mathsf{id}\,\frac{}{\vdash A^\perp, A} \qquad \mathsf{exch}\,\frac{\vdash \Gamma, A, B, \Delta}{\vdash \Gamma, B, A, \Delta} \qquad \parr\,\frac{\vdash \Gamma, A, B, \Delta}{\vdash \Gamma, A \parr B, \Delta}$$
$$\otimes\,\frac{\vdash \Gamma, A \qquad \vdash B, \Delta}{\vdash \Gamma, A \otimes B, \Delta} \qquad \mathsf{cut}\,\frac{\vdash \Gamma, A \qquad \vdash A^\perp, \Delta}{\vdash \Gamma, \Delta} \tag{37}$$

We use the exchange rule explicit here (i.e., sequents are lists of formulas) because it helps understanding what is going on.

In the calculus of structures, The unit-free system looks as follows:

$$\mathsf{ai}\!\downarrow \frac{}{[a \parr a^\perp]} \qquad \mathsf{ai}\!\downarrow \frac{S\{B\}}{S\{B \otimes [a \parr a^\perp]\}} \qquad \mathsf{s}\, \frac{S\{[A \parr B] \otimes C\}}{S\{A \parr (B \otimes C)\}} \tag{38}$$

Because there are no units present, the ai↓ rule looks slightly different from what you have seen before, and there are two versions of it. We use the name MLS^- for the system in (38). We can drop the equations for the units and only keep the ones for associativity and commutativity.

$$\begin{array}{ccc} (A \otimes (B \otimes C)) = ((A \otimes B) \otimes C) & & (A \otimes B) = (B \otimes A) \\ [A \parr [B \parr C]] = [[A \parr B] \parr C] & & [A \parr B] = [B \parr A] \end{array} \tag{39}$$

The cut rule is

$$\mathsf{ai}\!\uparrow \frac{S\{B \parr (a \otimes a^\perp)\}}{S\{B\}} \tag{40}$$

For simplicity, we will also use the general versions of the interaction rules:

$$\mathsf{ai}\!\downarrow \frac{}{[A \parr A^\perp]} \qquad \mathsf{ai}\!\downarrow \frac{S\{B\}}{S\{B \otimes [A \parr A^\perp]\}} \qquad \mathsf{ai}\!\uparrow \frac{S\{B \parr (A \otimes A^\perp)\}}{S\{B\}} \tag{41}$$

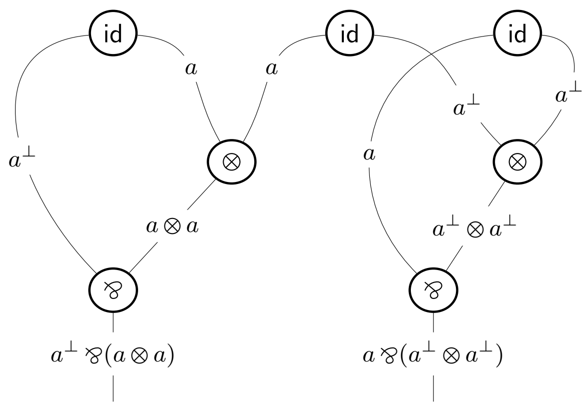
3.2 From sequent calculus to proof nets (Sequent Rule Ideology)

Although, morally, the concept of proof net should stand independently from any deductive formalism, the proof nets introduced by Girard very much depend on the sequent calculus. This is done inductively, rule instance by rule instance, as shown in Figure 10. Note that the exch-rule does not exactly follow the ideology.

3.2.1 Example The sequent calculus proof

$$\mathsf{\parr}\frac{\mathsf{exch}\frac{\otimes\frac{\mathsf{\parr}\frac{\otimes\frac{\mathsf{id}\frac{}{\vdash a^\perp, a} \quad \mathsf{id}\frac{}{\vdash a, a^\perp}}{\vdash a^\perp, a \otimes a, a^\perp}}{\vdash a^\perp \parr (a \otimes a), a^\perp} \quad \mathsf{id}\frac{}{\vdash a^\perp, a}}{\vdash a^\perp \parr (a \otimes a), a^\perp \otimes a^\perp, a}}{\vdash a^\perp \parr (a \otimes a), a, a^\perp \otimes a^\perp}}{\vdash a^\perp \parr (a \otimes a), a \parr (a^\perp \otimes a^\perp)} \tag{42}$$

is translated as



(43)

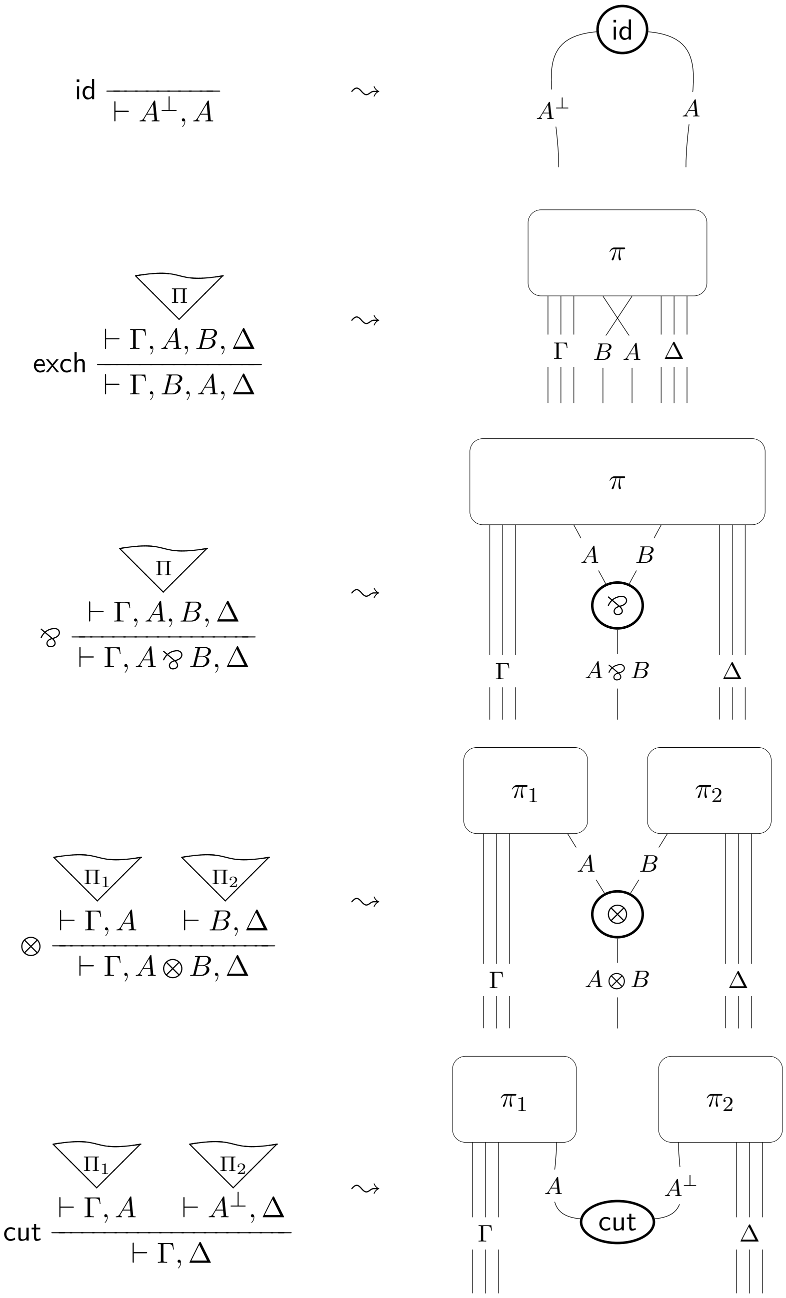


Figure 10: From sequent calculus to proof nets (sequent rule ideology)

3.3 From sequent calculus to proof nets (Flow Graph Ideology)

Let us no see how proof nets can be obtained by using the "flow graph ideology". The basic idea is to draw the "flow-graph" (or "coherence-graph") through the sequent calculus proof. This means that we trace all atom occurrences through the proof. The idea is quite simple,

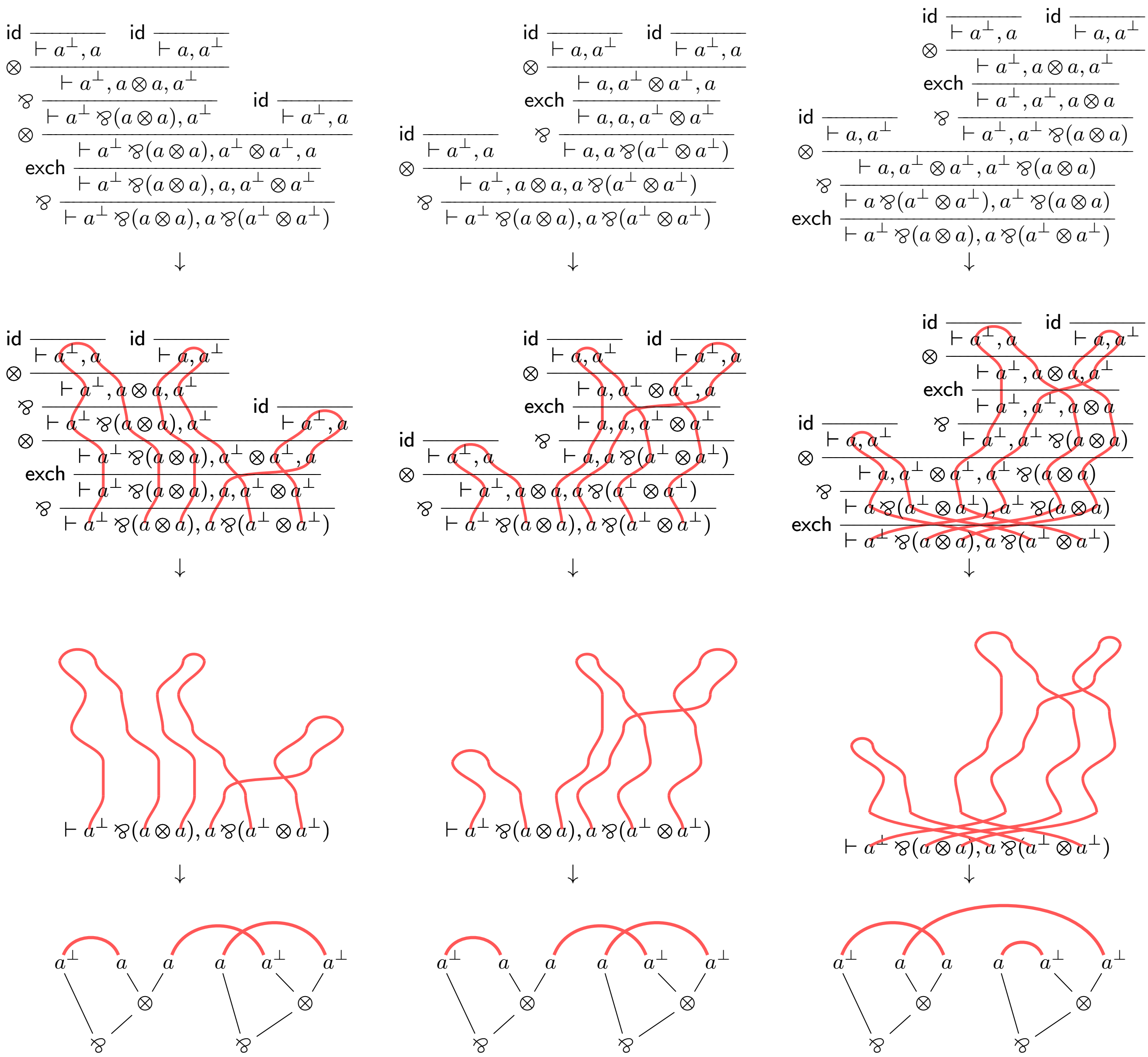


Figure 11: From sequent calculus to proof nets (flow graph ideology)

but the formal definitions tend to be messy. In these lecture notes, we show the idea via examples in Figure 11.

In Figure 12 we convert an example with cut into a proof net via the flow-graph method.

For dealing with cuts (without forgetting them!), we can prevent the flow-graph from flowing through the cut, i.e., by keeping the information that there is a cut. What is meant by this is shown in Figure 13.

It turns out that for MLL^- this method yields (modulo some trival change in notation) the same result as the method in Section 3.2. However, it should be emphazised that for richer logics the methods produce diffent notions of proof nets (see Section 5).

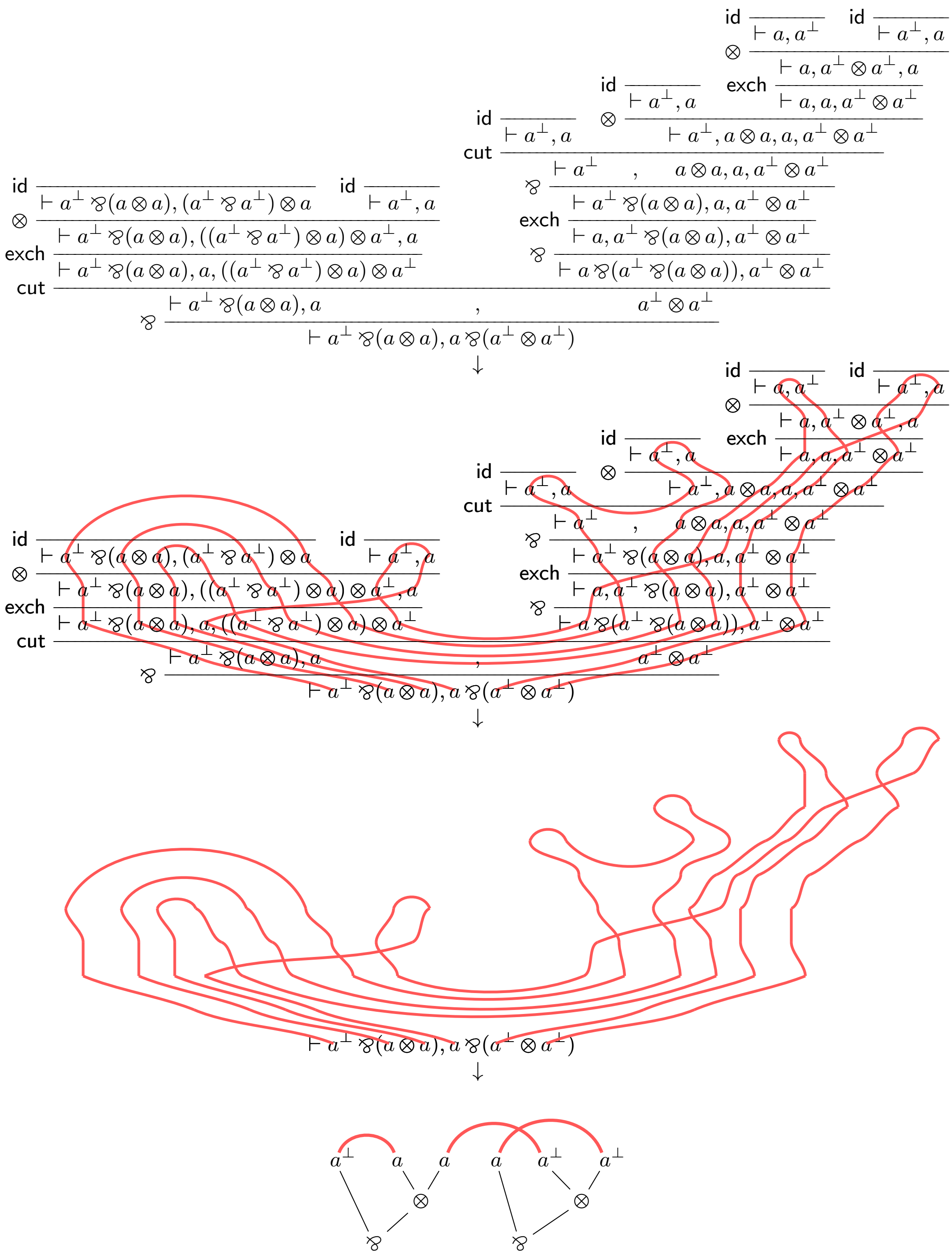


Figure 12: From sequent calculus to proof nets (flow graph ideology)

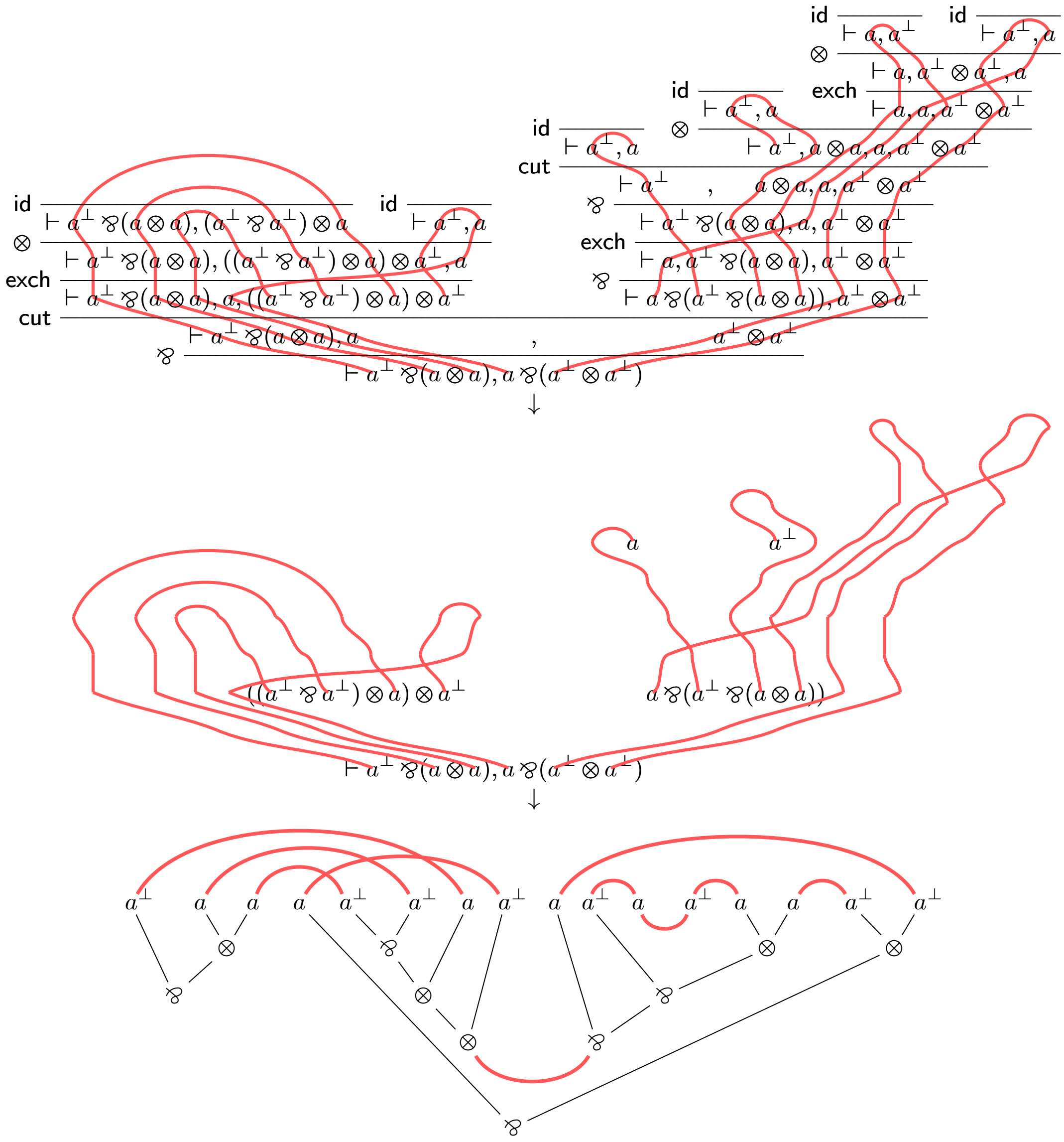


Figure 13: From sequent calculus to proof nets (flow graph ideology)

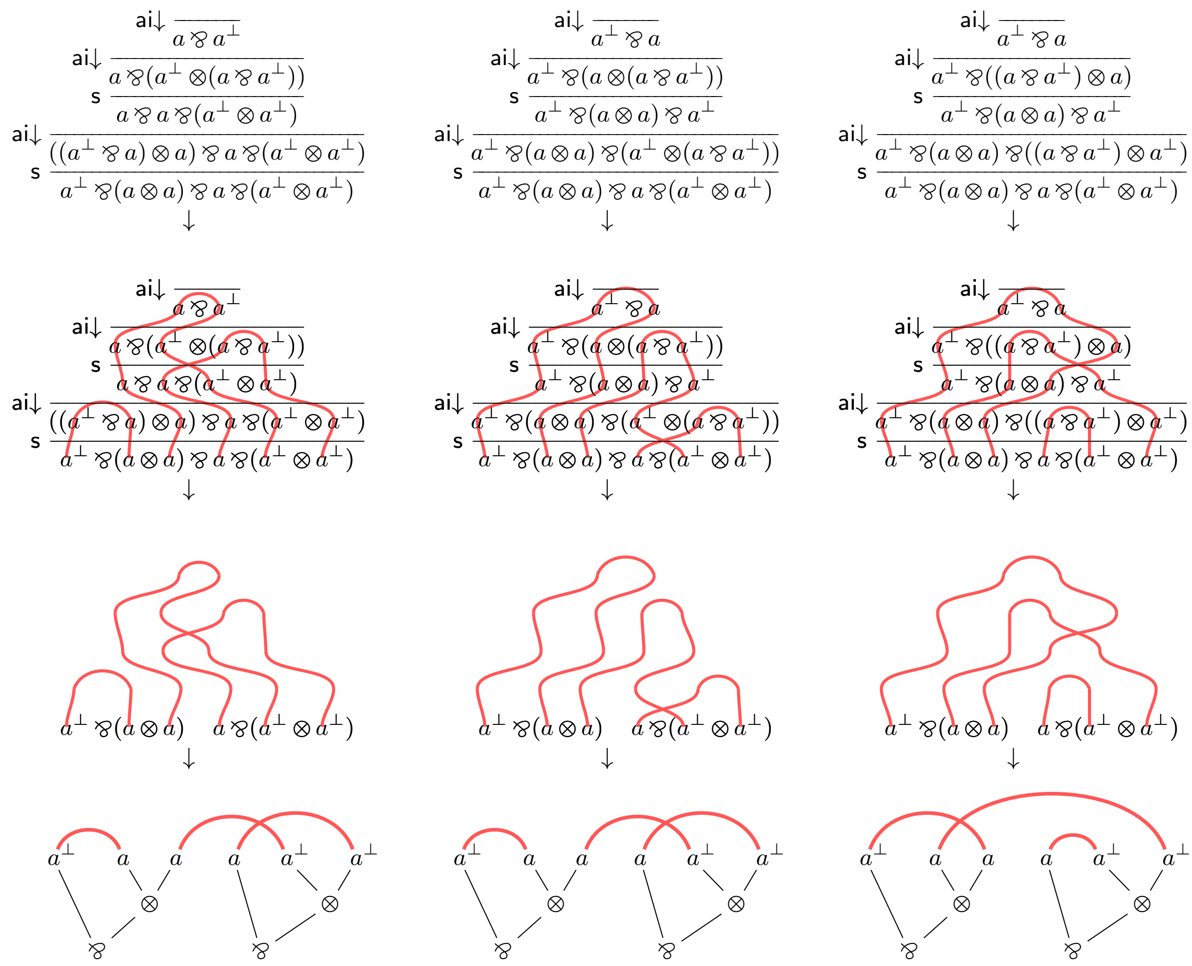


Figure 14: From calculus of structures to proof nets (flow graph ideology)

3.4 From the calculus of structures to proof nets

In this section we do the same as in the previous section. But this time, we start from MLS^- instead if MLL^-. But the result is exactly the same.

We simply trace the atoms through the derivation. Figures 14–16 show the calculus of structures version of Figures 11–13.

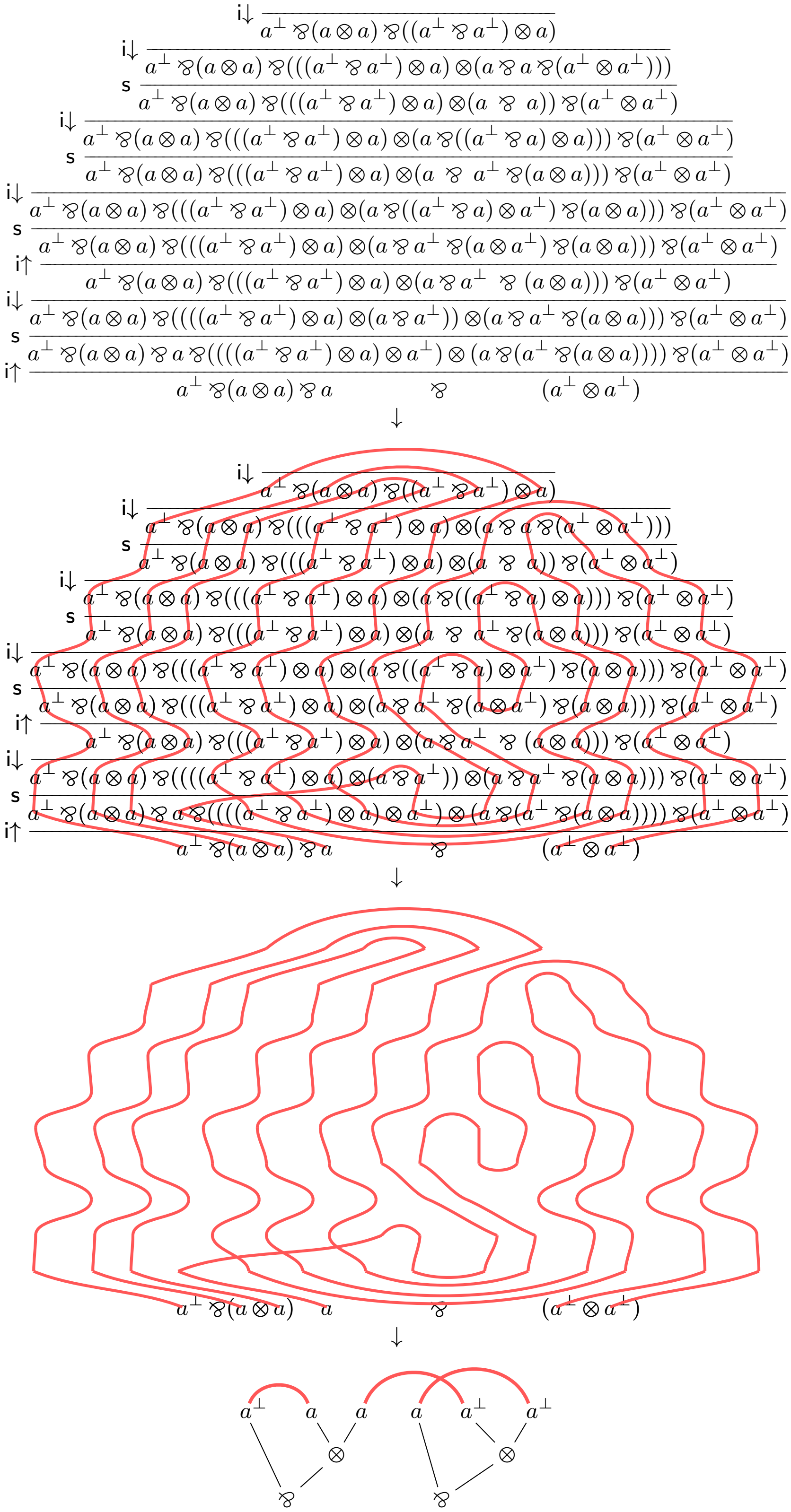


Figure 15: From calculus of structures to proof nets (flow graph ideology)

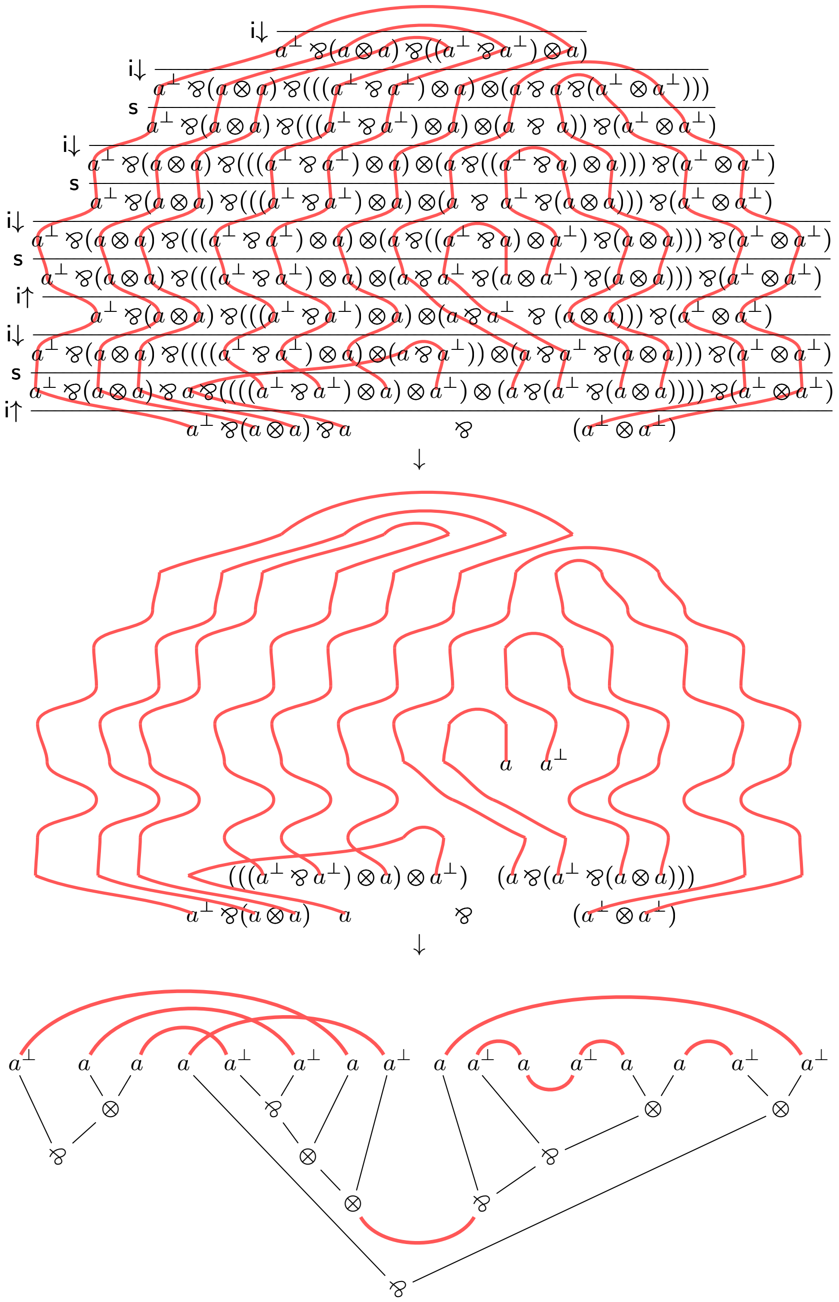
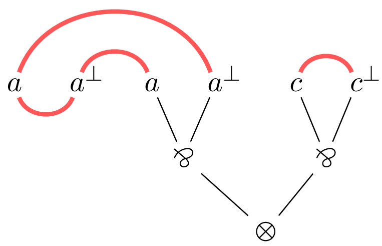


Figure 16: From calculus of structures to proof nets (flow graph ideology)

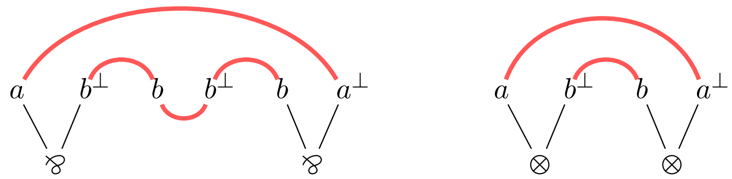
3.5 Correctness criteria

We have seen how we can obtain a proof net out of a formal proof in some deductive system. But what about the other way around? Suppose we have such a graph that looks like a proof net. Can we decide whether it really comes from a proof, and if so, can we recover this proof? Of course the answer is trivially yes because the graph is finite and we just need to check all proofs of that size. The interesting question is therefore, whether we can do it efficiently.

The answer is still yes, and it is done via so-called *correctness criteria*. For introducing the idea, we take the following graphs as running examples



(44)

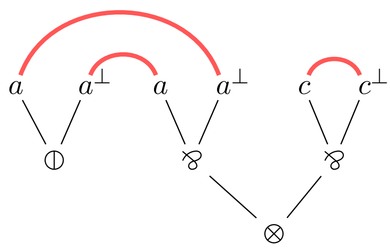


(45)

By playing around, you will notice that it is quite easy to find a proof (in sequent calculus or calculus of structures) that translates into the net in (44), but it seems impossible to find such proofs for the two examples in (45). We are now going to show that this is indeed impossible. For doing so, we need some formal definitions.

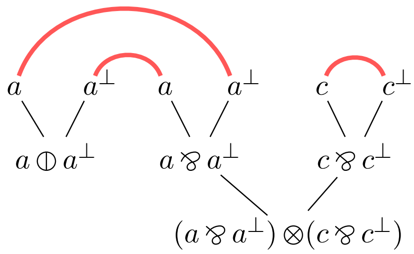
3.5.1 Definition A *pre-proof net* is a sequent forest Γ, possibly with cuts, together with a perfect matching of the set of leaves (i.e., the set of occurrences of propositional variables and their duals), such that only dual pairs are matched.

In this context, a cut must be seen as a special kind of formula $A \oplus A^\perp$, where $\oplus$ is a special connective which may occur only at the root of a formula tree in which the two direct subformulas are dual to each other. For example, (44) should be read as



(44')

Clearly, the examples in (44) and (45) are all pre-proof nets. In the following, we will think of an inner node (i.e., a non-leaf node) of the sequent forest labeled not only by the connective but by the whole subformula rooted by that connective. Our favorite example (44) should then be read as



(44")

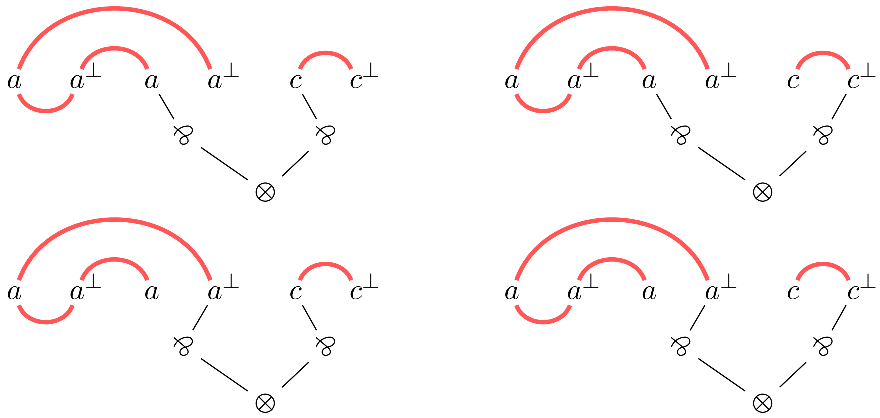
Although sometimes we think of pre-proof nets to be written as in (44"), we will keep writing them as in (44) for better readability.

3.5.2 Definition A pre-proof net π is called *sequentializable* iff there is a proof in the sequent calculus or in the calculus of structures that translates into π.

Originally, the term "sequentializable" was motivated by the name "sequent calculus". But we use it here also if the "sequentialization" is done in the calculus of structures.

3.5.3 Definition Let π be a pre-proof net. A *DR-switching* for π is a graph obtained from π by removing for every $\parr$-node one of the two edges connecting it to its children.

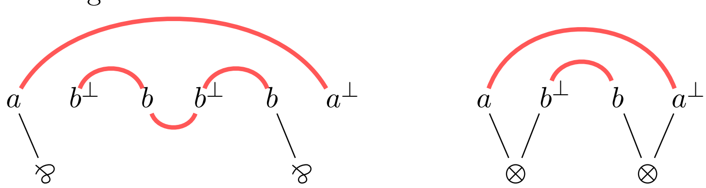
Clearly, if a pre-proof net contains n $\parr$-nodes, then there are 2^n switchings. Here are all 4 switchings for the example in (44):



(46)

3.5.4 Definition A pre-proof net *obeys the DR-switching criterion* (or, shortly, is *correct*) iff all its switchings are connected and acyclic.

As (46) shows, the pre-proof net in (44) is correct. The two pre-proof nets in (45) are not, as the following switchings show:



(47)

The first is not connected, and the second is cyclic.

In the following, we use the term *proof net* for those pre-proof nets which are correct, i.e., obey the switching criterion. The following theorem says that the proof nets are exactly those pre-proof nets that represent an actual proof.

3.5.5 Theorem *A pre-proof net is correct if and only if it is sequentializable.*

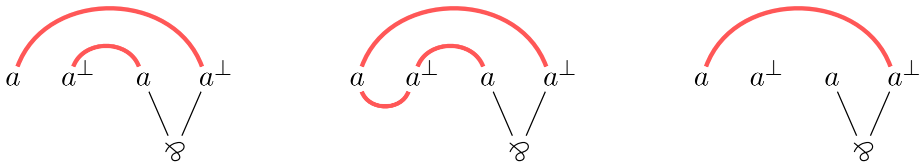
We will give two proofs of this theorem. The first uses the sequent calculus, and the second the calculus of structures. For the first proof, we need the following lemma:

3.5.6 Lemma *Let π be a proof net with conclusions $A_1, \ldots, A_n$. If all A_i have a $\otimes$ or a cut as root, then one of them is splitting, i.e., by removing that $\otimes$ (or $\oplus$), the net becomes disconnected.*

For proving this lemma, we need some more concepts.

3.5.7 Definition Let σ and π be pre-proof nets. We say σ is a *subprenet* of π, written as $\sigma \subseteq \pi$ if all formulas/cuts appearing in σ are subformulas of the formulas/cuts appearing in π, and the linking of σ is the restriction of the linking of π to the formulas/cuts in σ. We say σ is a *subnet* of π if $\sigma \subseteq \pi$, and σ and π are both correct. A *door* of σ is any formula that appears as conclusion of σ.

3.5.8 Example Consider the following three graphs:



The first two are subprenets of (44), the third one is not (because a link is missing). The second one is in fact a subnet of (44), but the first one is not (because it is not correct). The doors of the first example are a, $a^\perp$, and $a \parr a^\perp$. The doors of the second example are $a \oplus a^\perp$ and $a \parr a^\perp$.

3.5.9 Lemma *Let σ and ρ be subnets of some proof net π.*

(i) *The subprenet $\sigma \cup \rho$ is a subnet of π if and only if $\sigma \cap \rho \neq \emptyset$.*

(ii) *If $\sigma \cap \rho \neq \emptyset$ then $\sigma \cap \rho$ is a subnet of π.*

Proof: Intersection and union in the statement of that lemma have to be understood in the canonical sense: An edge/node/link appears in in $\sigma \cap \rho$ (resp. $\sigma \cup \rho$) if it appears in both, σ and ρ (resp. in at least one of σ or ρ). For giving the proof, let us first note that because in π every switching is acyclic, also in every subprenet of π every switching is acyclic, in particular also in $\sigma \cup \rho$ and $\sigma \cap \rho$. Therefore, we need only to consider the connectedness condition.

(i) If $\sigma \cap \rho = \emptyset$ then every switching of $\sigma \cup \rho$ must be disconnected. Conversely, if $\sigma \cap \rho \neq \emptyset$, then every switching of $\sigma \cup \rho$ must be connected (in every switching of $\sigma \cup \rho$ every node in $\sigma \cap \rho$ must be connected to every node in σ and to every node in ρ, because σ and ρ are both correct).

(ii) Let $\sigma \cap \rho \neq \emptyset$ and let s be a switching for $\sigma \cup \rho$. Then s is connected and acyclic by (i). Let s_σ, s_ρ, and $s_{\sigma\cap\rho}$, be the restrictions of s to σ, ρ, and $\sigma \cap \rho$, respectively. Now let A and B be two vertices in $\sigma \cap \rho$. Then A and B are connected by a path in s_σ because σ is correct, and by a path in s_ρ because ρ is correct. Since s is acyclic, the two paths must be the same and therefore be contained in $s_{\sigma\cap\rho}$. □

3.5.10 Lemma *Let π be a proof net, and let A be a subformula of some formula/cut appearing in π. Then there is a subnet σ of π, that has A as a door.*

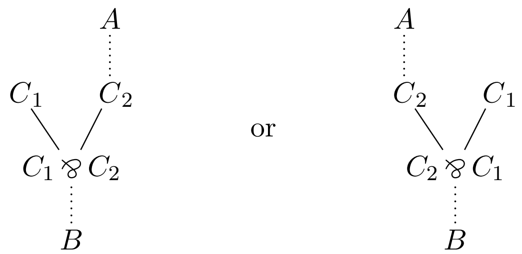
Proof: For proving this lemma, we need the following notation. Let π be a proof net, let A be some formula occurrence in π, and let s be a switching for π. Then we write $s(\pi, A)$ for the graph obtained as follows:

- If A is an immediate subformula of a formula occurrence B in π, and there is an edge from B to A in s, then remove that edge and let $s(\pi, A)$ be the connected component of (the remainder of) s that contains A.
- Otherwise let $s(\pi, A)$ be just s.

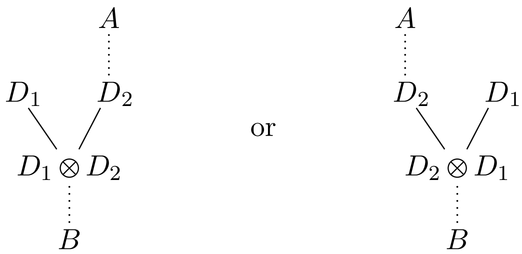
Now let

$$\sigma = \bigcap_s s(\pi, A)$$

where s ranges over all possible switchings of π. (Note that it could happen that formally σ is not a subprenet because some edges in the formula trees might be missing. We graciously add these missing edges to σ such that it becomes a subprenet.) Clearly, A is in σ. We are now going to show that A is a door of σ. By way of contradiction, assume it is not. This means there is ancestor B of A that is in $\bigcap_s s(\pi, A)$. Now choose a switching $\hat{s}$ such that whenever there is a $\bindnasrepma$ node between A and B, i.e.,



then $\hat{s}$ chooses C_1 (i.e., removes the edge between C_2 and its parent). Then there must be a $\otimes$ between A and B:



Otherwise B would not be in σ. Now suppose we have chosen the uppermost such $\otimes$. Then the path connecting A and D_1 in $\hat{s}(\pi, A)$ cannot pass through D_2 (by the definition of $\hat{s}(\pi, A)$). But this means that in $\hat{s}$ there are two distinct paths connecting A and D_1, which contradicts the acyclicity of $\hat{s}$.

Now we have to show that σ is a subnet. Let s be a switching for σ. Since σ is a subprenet of π, we have that s is acyclic. Now let $\tilde{s}$ be an extension of s to π. Then s is the restriction of $\tilde{s}(\pi, A)$ to σ, and hence connected. □

3.5.11 Definition Let π be a proof net, and let A be a subformula of some formula/cut appearing in π. The *kingdom of A in π*, denoted by kA, is the smallest subnet of π, that has A as a door. Similarly, the *empire of A in π*, denoted by eA, is the largest subnet of π, that has A as a door. We define $A \ll B$ iff $A \in kB$, where A and B can be any (sub)formula/cut occurrences in π.

An immediate consequence of Lemmas 3.5.9 and 3.5.10 is that kingdom and empire always exist.

3.5.12 Exercise Why?

3.5.13 Remark The subnet σ constructed in the proof of Lemma 3.5.10 is in fact the empire of A. But we will not need this fact later and will not prove it here.

3.5.14 Lemma *Let π be a proof net, and let A, A', B, and B' be subformula occurrences appearing in π, such that A and B are distinct, A' is immediate subformula of A, and B' is immediate subformula of B. Now suppose that $B' \in eA'$. Then we have that $B \notin eA'$ if and only if $A \in kB$.*

Proof: We have $B' \in eA' \cap kB$. Hence, $\sigma = eA' \cap kB$ and $\rho = eA' \cup kB$ are subnets of π. By way of contradiction, let $B \notin eA'$ and $A \notin kB$. Then ρ has A' as door and is larger than eA' because it contains B. This contradicts the definition of eA'. On the other hand, if $B \in eA'$ and $A \in kB$ then σ has B as door and is smaller than kB because it does not contain A. This contradicts the definition of kB. □

3.5.15 Lemma *Let π be a proof net, and let A and B be subformulas appearing in π. If $A \ll B$ and $B \ll A$, then either A and B are the same occurrence or they are dual atoms connected via an identity link.*

Proof: If a and $a^{\perp}$ are two dual atom occurrences connected by a link, then clearly $ka = ka^{\perp}$. Now let A and B be two distinct non-atomic formula occurrences in π with $A \in kB$ and $B \in kA$. Then $kA \cap kB$ is a subnet and hence $kA = kA \cap kB = kB$. We have two cases:

- If $A = A' \parr A''$ then the result of removing A from kB is still a subnet, contradicting the minimality of kB.
- If $A = A' \otimes A''$ then $kA = kA' \cup kA'' \cup \{A' \otimes A''\}$. Hence $B \in kA'$ or $B \in kA''$. This contradicts Lemma 3.5.14, which says that $B \notin eA'$ and $B \notin eA''$. □

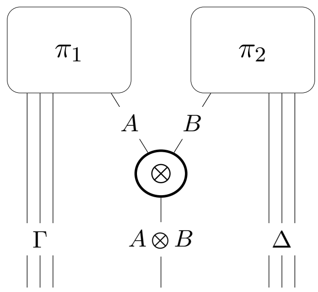
From Lemma 3.5.15 it immediately follows that $\ll$ is a partial order on the non-atomic subformula occurrences in π. We make crucial use of this fact in the following:

Proof of Lemma 3.5.6: Choose among the conclusions $A_1, \ldots, A_n$ (including the cuts) of π one which is maximal w.r.t. $\ll$. Without loss of generality, assume it is $A_i = A'_i \otimes A''_i$. We will now show that it is splitting, i.e., $\pi = \{A'_i \otimes A''_i\} \cup eA'_i \cup eA''_i$. By way of contradiction, assume $A'_i \otimes A''_i$ is not splitting. This means we have somewhere in π a formula occurrence B with immediate subformula B' such that (without loss of generality) $B' \in eA'_i$ and $B \notin eA'_i$. We also know that B must occur at or above some other conclusion, say $A_j = A'_j \otimes A''_j$. Hence $B \in kA_j$ and therefore $kB \subseteq kA_j$. But by Lemma 3.5.14 we have $A_i \in kB$ and therefore $A_i \in kA_j$, which contradicts the maximality of A_i w.r.t. $\ll$. □

Finally, we can prove Theorem 3.5.5.

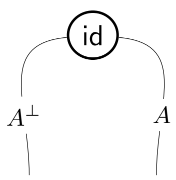
First Proof of Theorem 3.5.5: Let us first show that the (in the sequent calculus) sequentializable pre-proof nets are indeed correct. This is done by verifying that the id-rule yields correct nets (which is obvious) and that all other inference rules preserve correctness. For the exch-rule this is obvious. Let us now consider the $\otimes$-rule. By way of contradiction, assume that

are correct, but

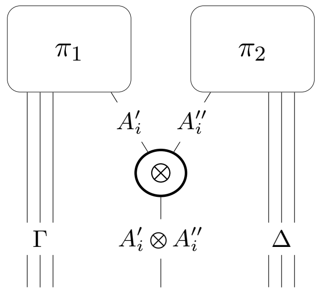


is not correct. This means there is a switching that is either disconnected or contains a cycle. Since a $\otimes$-node does not affect switchings, we conclude that the property of being disconnected or cyclic must hold for the same switching in one of π_1 or π_2. But this is a contradiction to the correctness of π_1 and π_2. For the the $\parr$-rule and the cut-rule we proceed similarly.

Conversely, let π be a correct pre-proof net. We proceed by induction on the size of π, i.e., the number n of $\parr$-, $\otimes$-, and cut-nodes in π, to construct a sequent calculus proof Π, that translates into π. If n is 0, then π must be of the shape



and we can apply the id-rule. Now let $n > 0$. If one of the conclusion formulas of π has a $\parr$-root, we can apply the $\parr$-rule and proceed by induction hypothesis. Now suppose all roots are $\otimes$ or cuts. Then we apply Lemma 3.5.6, which tells us, that there is one of them which splits the net. Assume, without loss of generality, that it is a $\otimes$-root, say $A_i = A'_i \otimes A''_i$. This means, the net is of the shape



and we can apply the $\otimes$-rule and proceed by induction hypothesis for π_1 and π_2. If the splitting root is a cut, we apply the `cut`-rule instead. □

Let us now see the second proof. For this, we need the following lemma:

3.5.16 Lemma *Let π be a proof net with conclusion*

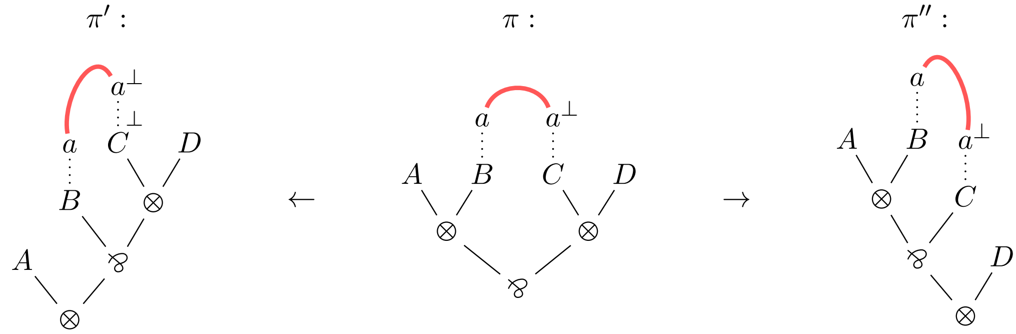
$$S\{(A \otimes B\{a\}) \parr (C\{a^\perp\} \otimes D)\} \quad ,$$

such that the a and the $a^\perp$ are paired up in the linking. Let π' and π'' be pre-proof nets with conclusions

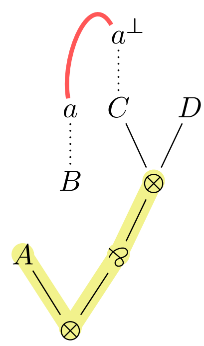
$$S\{A \otimes [B\{a\} \parr (C\{a^\perp\} \otimes D)]\} \qquad \text{and} \qquad S\{[(A \otimes B\{a\}) \parr C\{a^\perp\}] \otimes D\}$$

respectively, such that the linkings of π' and π'' (i.e., the pairing of dual atoms) are the same as the linking of π. Then at least one of π' and π'' is also correct.

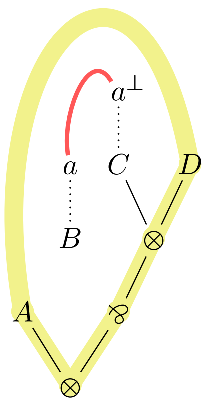
Proof: Let us visualize the information we have about π, π', and π'' as follows:



We proceed by way of contradiction, and assume that π is correct and that π' and π'' are both incorrect. If there is a switching s for π' (or π'') that is disconnected, then the same switching is also disconnected in π. Hence, we need to consider only the acyclicity condition. Suppose that there is a switching s' for π' that is cyclic. Then, in s' the $\parr$ below B must be switched to the right, and the cycle must pass through A, the root $\otimes$ and the $\parr$ as follows:

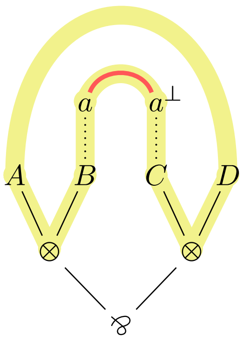


Otherwise we could construct a switching with the same cycle in π. If our cycle continues through D, i.e.,

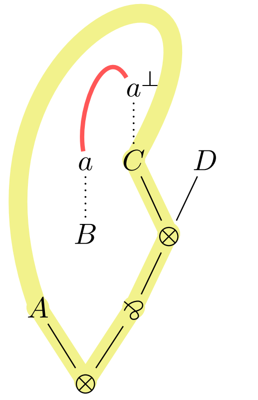


(48)

then we can use the path from A to D (that does not go through B or C, see Exercise 3.5.17) to construct a cyclic switching s in π as follows:

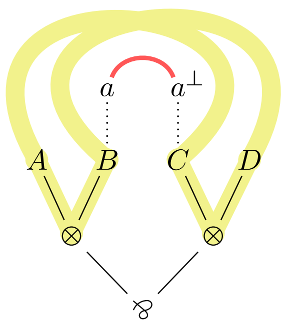


Hence, the cycle in s' goes through C, giving us a path from A to C, not passing through B (see Exercise 3.5.17):



(49)

By the same argumentation we get a switching s'' in π'' with a path from B to D, not going through C. From s' and s'', we can now construct a switching s for π with a cycle as follows:



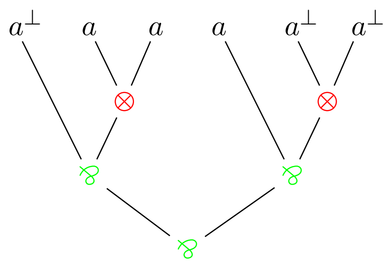
which contradicts the correctness of π. □

3.5.17 Exercise Explain why we can in (48) assume that the cycle does not go through B or C, and in (49) not through B.

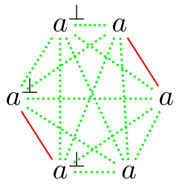
In our second proof of Theorem 3.5.5 we will also need the following concept:

3.5.18 Definition Let A be a formula. The *relation web* of A is the complete graph, whose vertices are the atom occurrences in A. An edge between two atom occurrences a and b is colored red, if the first common ancestor of them in the formula tree is a $\otimes$, and green if it is a $\parr$.

3.5.19 Example Consider the formula $[[a^\perp \parr (a \otimes a)] \parr [a \parr (a^\perp \otimes a^\perp)]]$. Its formula tree is the following:



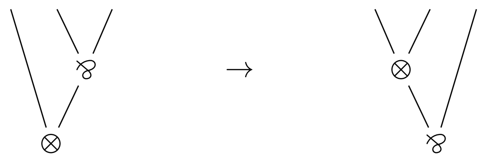
The relation web is therefore



where we use regular edges for red and dotted edges for green.

3.5.20 Definition The *degree of freedom* of a formula A, is the number of green edges in its relation web.

Second Proof of Theorem 3.5.5: Again, we start by showing that all rules preserve correctness. Here, the only interesting case is the switch rule (all others being trivial), which does the following transformation somewhere inside the net:



(50)

By way of contradiction, assume the net on the left is correct, and the one on the right is not. First, suppose there is a switching for the second net that is cyclic. If that cycle does not contain the $\otimes$-node shown on the right in (50), then this cycle is also present in the net on the left in (50). If our cycle contains the $\otimes$-node, then we can make the same cycle be present in the net on the left by switching the $⅋$-node to the left (i.e., removing the edge to the right). Now assume we have a disconnected switching for the net on the right. Then the same switching also disconnects the net on the left. Contradiction.

Conversely, assume we have a correct net π with conclusion F. For the time being, assume that π is cut-free. We proceed by induction on the degree of freedom of F. Pick inside F any pair of atoms that are linked together, say a and $a^\perp$. Then $F = S\{S_1\{a\} ⅋ S_2\{a^\perp\}\}$. Without loss of generality, we can assume that $S_1\{\ \}$ and $S_2\{\ \}$ are not $⅋$-contexts. We have the following cases:

- If $S_1\{\ \} = S_2\{\ \} = \{\ \}$, we can apply the rule $\mathsf{i}{\downarrow}$, and proceed by induction hypothesis.
- If $S_1\{\ \} \neq \{\ \}$ and $S_2\{\ \} = \{\ \}$, then $F = S\{(A \otimes B\{a\}) ⅋ a^\perp\}$ for some A and $B\{\ \}$. We can apply the switch rule to get $S\{A \otimes [B\{a\} ⅋ a^\perp]\}$, which is still correct (with the same linking as for F), but has smaller degree of freedom than F. The case where $S_1\{\ \} = \{\ \}$ and $S_2\{\ \} \neq \{\ \}$ is similar.
- If $S_1\{\ \} \neq \{\ \}$ and $S_2\{\ \} \neq \{\ \}$, then, without loss of generality, $F = S\{(A \otimes B\{a\}) ⅋ (C\{a^\perp\} \otimes D)\}$, for some A, $B\{\ \}$, $C\{\ \}$, D. By Lemma 3.5.16, we can apply the switch rule, since one of

  $$S\{A \otimes [B\{a\} ⅋ (C\{a^\perp\} \otimes D)]\} \quad \text{and} \quad S\{[(A \otimes B\{a\}) ⅋ C\{a^\perp\}] \otimes D\}$$

  is still correct. Since both of them have smaller degree of freedom than F, we can proceed by induction hypothesis.

If π contains cuts, we can replace inside π all cuts with $\otimes$, to get a formula F' such that there is a derivation

$$\begin{array}{c} F' \\ \mathsf{i}\!\uparrow\!\Big\Vert \\ F \end{array}$$

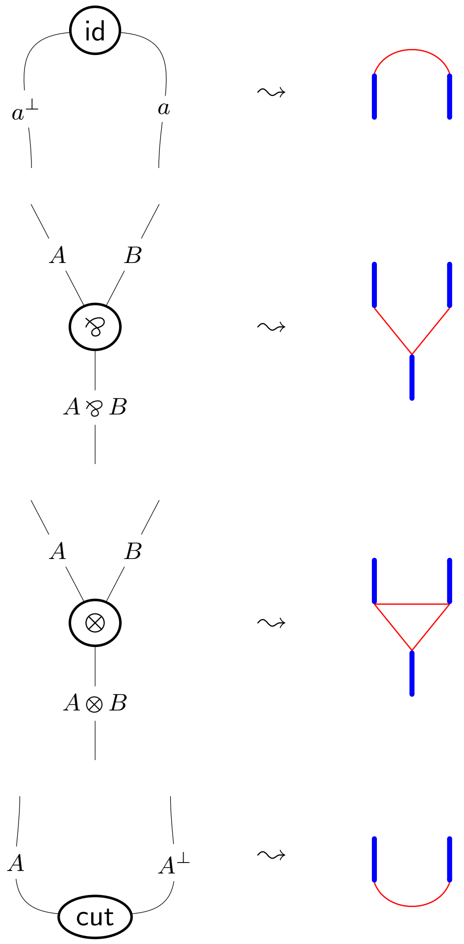
Then π becomes a cut-free net with conclusion F', and we can proceed as above. $\square$

Note that the two different proofs of Theorem 3.5.5 yield a stronger version of the equivalence between MLL^- and MLS^- that we established in the previous section.

3.5.21 Theorem *For every sequent calculus proof of* $\vdash A_1, A_2, \ldots, A_n$ *in* MLS^- *there is a proof in the calculus of structures in system* MLS^- *of* $[A_1 \parr A_2 \parr \cdots \parr A_n]$ *yielding the same proof net, and vice versa.*

A geometric or graph-theoretic criterion like the one in Definition 3.5.4 and Theorem 3.5.5 is called a *correctness criterion*. The desired properties are soundness and completeness, as stated in Theorem 3.5.5. For MLL^-, the literature contains quite a lot of such criteria, and it would go far beyond the scope of this lecture notes to attempt to give a complete survey. But nonetheless, we will show here two other correctness criteria.

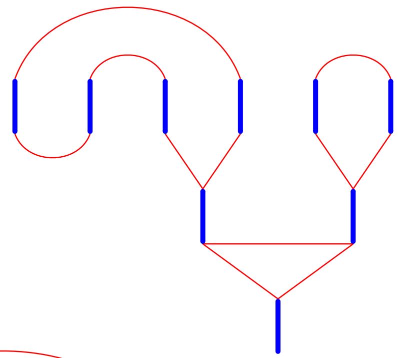
For the next one, we write the pre-proof nets in a different way:



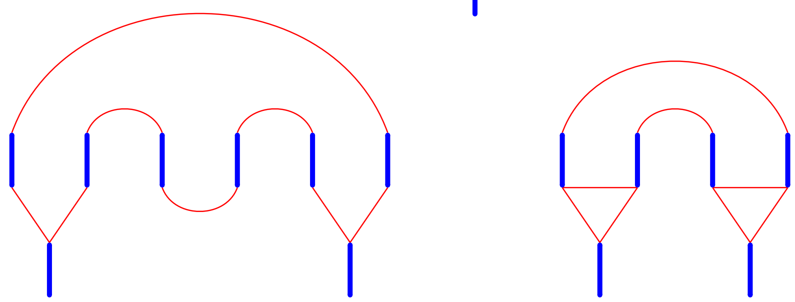
(51)

We call the resulting graphs *RB-graphs*. The R and B stand for Regular/Red and Bold/Blue. The main property of these graphs is that the blue/bold edges (in the following called *B-edges*) provide a bipartition of the set of vertices, i.e., every vertex in the RB-graph is connected to exactly one other vertex via a B-edge. The red/regular edges are in the following called *R-edges*.

Here are the examples from (44) and (45) written as RB-graphs:



(52)



(53)

3.5.22 Definition Let G be an RB-graph. An *Æ-path* in G is a path whose edges are alternating R- and B-edges, and that does not touch any vertex more than once. An *Æ-cycle* in G is a Æ-path from a vertex to itself, starting with a B-edge and ending with an R-edge.

The A and E stand for "alternating" and "elementary". The meaning of "alternating" should be clear, and the meaning of "elementary" is that the path or cycle must not cross itself.

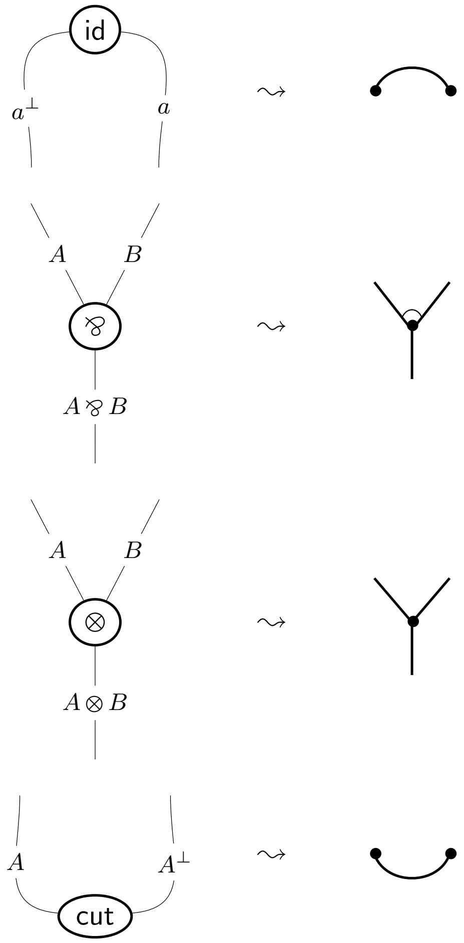
3.5.23 Definition A pre-proof net π *obeys the RB-criterion* (or shortly, is *RB-correct*) iff its RB-graph G_π contains no Æ-cycle and every pair of vertices in G_π is connected via an Æ-path.

3.5.24 Theorem *A pre-proof net is RB-correct if and only if it is a proof net.*

Proof: We show that a pre-proof net is RB-correct iff it obeys the switching criterion, which is easy: If there are two vertices in the RB-graph not connected by an Æ-path, then there is a switching yielding a disconnected graph, and vice versa. Similarly, the RB-graph contains an Æ-cycle if and only if we can provide a switching with a cycle. □

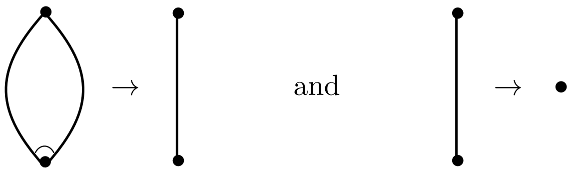
3.5.25 Exercise Work out the details of the previous proof.

For the third correctness criterion, we write our nets in yet another way:



(54)

Now consider the following two rewriting rules on these graphs:



(55)

It is important to note that in the first rule the two edges are between the same pair of vertices and are connected by an arc at exactly one of the two vertices. The second rule only applies if the two vertices on the lefthand side are distinct, and the edge is not connected to another edge by an arc.

3.5.26 Theorem *The reduction relation induced by the rules in* (55) *is terminating and confluent.*

Proof: Termination is obvious because at each step the size of the graph is reduced. Hence, it suffices to show local confluence to get confluence. But this is easy since there are no (proper) critical pairs. □

This means that for each pre-proof net we get a uniquely defined reduced graph, and the question is now how this graph looks like.

3.5.27 Exercise Apply the reduction relation defined in (55) to the nets in (44) and (45).

3.5.28 Definition A pre-proof net *obeys the contraction criterion* if its normal form according to the reduction relation defined in (55) is

$$\bullet$$

i.e., a single vertex without edges.

At this point rather unsurprisingly, we get:

3.5.29 Theorem *A pre-proof net obeys the contraction criterion if and only if it is a proof net.*

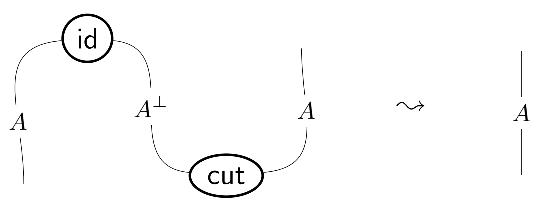
Proof: As before, we show this by showing the equivalence of the switching criterion and the contraction criterion. This is easy to see since both reductions in (55) preserve and reflect correctness according to the switching criterion. □

Before we leave the topic of correctness criteria, let us make some important observations on their complexity. The naive implementation of checking the switching criterion needs exponential time: if there are n par-links in the net, then there are 2^n switchings to check. However, checking the RB-criterion needs only quadratic runtime. To verify this is an easy graph-theoretic exercise. It is also easy to see that checking the contraction criterion can be done in quadratic time. But it is rather surprising that it can be done in linear time in the size of the net. This means that (in the case of MLL^-) when we go from a formal proof in a deductive system like the sequent calculus or the calculus of structures (whose correctness can trivially be checked in linear lime in the size of the proof) to the proof net, we do not lose any information. The proof net contains the *essence* of the proof, including the "deductive information". Unfortunately, MLL^- is (so far) the only logic (except some variants of it), for which this ideal of proof nets is reached.

3.6 Cut elimination

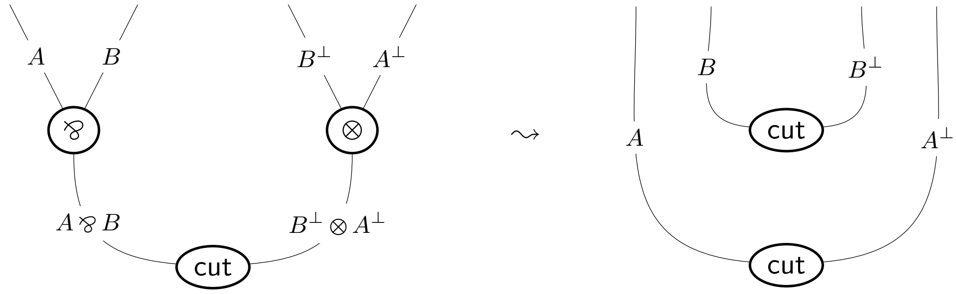
In Section 2 you have already seen two different proofs of cut elimination: one using the sequent calculus, and one using the calculus of structures. In this section, you will see yet another one, using proof nets.

Consider the following reduction rules on pre-proof nets with cuts:



(56)

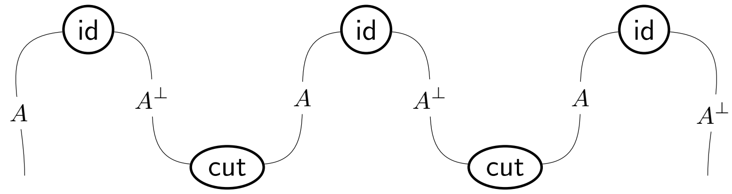
and



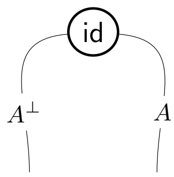
(57)

3.6.1 Theorem *The cut reduction relation defined by* (56) *and* (57) *terminates and is confluent.*

Proof: Showing termination is trivial because in every reduction step the size of the net decreases. For showing confluence, note that the only possibility for making a critical pair is when two cuts want to reduce with the same identity link. Then the situation must be of the shape:

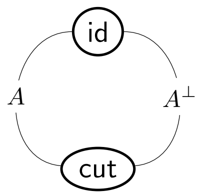


But no matter in which order and with which identity we reduce the cuts, the final result will always be



Hence we also have confluence. □

However, in principle, it could happen, that we end up in a situation like



where we cannot reduce any further. That something like this cannot happen if we start out with a correct net is ensured by the following theorem, which says that the cut reduction preserves correctness.

3.6.2 Theorem *Let* π *and* π' *be pre-proof nets such that* π *reduces to* π' *via the reductions* (56) *and* (57)*. If* π *is correct, then so is* π'*.*

Proof: For proving this, let us use the RB-correctness criterion. Written in terms of RB-graphs, the two reduction rules look as follows:

 (58)

and

 (59)

That the first rule preserves RB-correctness is obvious because it just shortens an existing path. For the second rule, we proceed by way of contradiction. First, assume that the graph on the right contains an Æ-cycle, while the one on the left does not. There are three possibilities:

1. The Æ-cycle does not contain one of the new B-R-B-paths. Then the same cycle is also present on the left. Contradiction.

2. The Æ-cycle contains exactly one of the new B-R-B-paths. Then, as before, the same cycle is also present on the left. Contradiction.

3. The Æ-cycle contains both of the new B-R-B-paths. Then we can construct an Æ-cycle on the left that comes in at the upper left corner, goes down through the $\otimes$-link, and goes out at the lower left corner. Again, we get a contradiction.

That Æ-path connectedness is preserved is shown in a similar way. □

3.6.3 Exercise Complete the proof of Theorem 3.6.2, i.e., show that if we apply (59) to an RB-correct net, then in the result every pair of vertices is connected by an Æ-path. Hint 1: Note that the two rightmost vertices in (59) must be connected by an Æ-path that does not touch the new B-R-B-paths (why?). Hint 2: You will need the fact that the first net is also Æ-cycle free.

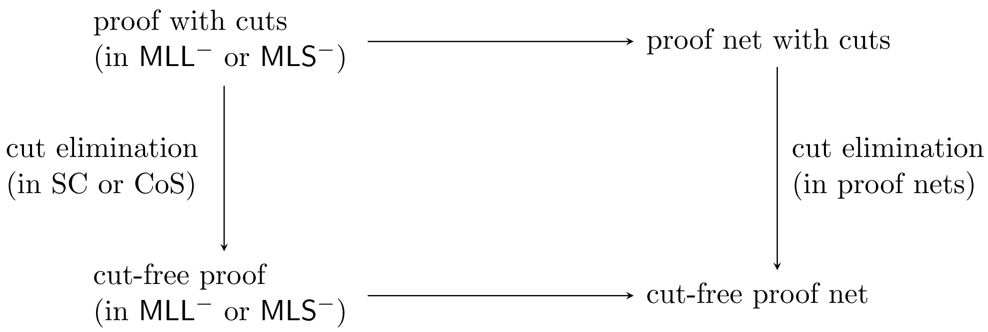
The important point of Theorem 3.6.2 is that it allows us to give a short proof of the cut elimination theorem for MLL^- and for MLS^-: Let Π be a proof with cuts in MLL^- given in the sequent calculus or the calculus of structures. We can translate Π into a proof net π, as described in Sections 3.2–3.4 and remove the cuts from the proof net as described above. This gives us a proof net π', which we can translate back to the sequent calculus or the calculus of structures. This works because removing the cuts from the proof net preserves the property of being correct (i.e., being a proof net), and translating back does not introduce any new cuts.

This raises an important question: Suppose we start out with a proof Π with cuts in MLL^- (given in sequent calculus or the calculus of structures). Now we could first remove the cuts as shown in the previous lecture for the sequent calculus and for the calculus of structures, and then translate the resulting cut-free proof Π' into a proof net π'_1. Alternatively, we could first translate Π into a proof net π, and then remove the cuts from π, to obtain the cut-free proof net π'_2. Do we get the same result? Is $\pi'_1 = \pi'_2$?

The answer is of course **yes**. To see this, note that the cut reduction steps in the sequent calculus either preserve the proof net (if the cut is just permuted up via a trivial rule permutation) or do exactly the same as the cut reduction steps for proof nets.

The same is true for the calculus of structures. The proof of the splitting lemma is designed such that it preserves the net. To make this formally precise would go beyond the scope of these lecture notes, but by comparing Figures 15 and 16 you should get the idea.

We can summarize this by the following commuting diagram:



(60)

Our basic introduction into the theory of proof nets for unit-free multiplicative linear logic is now finished. However, a very important and fundamental question has not yet been mentioned:

3.6.4 Big Question Let π and π' be two proof nets such that π' is obtained from π by applying some cut reduction steps. Do π and π' represent the *same* proof?

One can safely say that in the simple case of unit-free multiplicative linear logic the answer is **yes**. However, when it comes to richer fragments of linear logic, or classical logic, the answer for this question is far from clear.

3.7 Notes

The terminology of “proof nets” and “bureaucracy” is due to Girard. He introduced proof nets along with sequent calculus presentation for linear logic in [Gir87]. He essentially followed the sequent rule ideology for obtaining his proof nets. The concept of coherence graph is based in the work of Eilenberg, Kelly, and MacLane [EK66, KM71], who also provided the acyclicity condition and observed that it is preserved by composition, i.e., cut elimination. The terminology “flow-graph” is due to Buss [Bus91].[2]

The notion of “correctness criterion” is also due to Girard. In [Gir87] he gave the “long-trip-criterion” that we did not present here. The splitting tensor theorem (our Lemma 3.5.6) also first appeared in [Gir87]. The proof given in Section 3.5 follows the presentation of Bellin and van de Wiele in [BvdW95], who also discuss in more detail the relation between proof nets and trivial rule permutations. Another well-written short discussion on this issue can be found in [Laf95]. Our second proof of Theorem 3.5.5 (i.e., the one using the calculus of structures) follows the presentation in [Str03a]. However, the result is already implicit present in the work of [DHPP99] and [Ret97].

[2]Strictly speaking, coherence graphs and flow graphs are not the same thing. But in the simple case of MLL$^-$, the two notions coincide.

The switching criterion (Definition 3.5.4 and Theorem 3.5.5) is due to Danos and Regnier [DR89]. For this reason the switching criterion is in the literature also called Danos-Regnier-criterion or DR-criterion. However, the contraction criterion is also due to Danos and Regnier[3] and should therefore also be called DR-criterion. See [Moo02, Pui01] for a more recent investigation of the contraction criterion. That (a version of) the contraction criterion can be checked in linear time in the size of the net has been discovered by Guerrini [Gue99]. The RB-correctness criterion has been found by Retoré [Ret93, Ret99, Ret03], who provided a detailed analysis of proof nets using RB-graphs in various forms.

4 What does category theory have to to with proof theory?

Assume, we accept the following postulates about proofs:

(i) for every proof f of conclusion B from hypothesis A (denoted by $f\colon A \to B$) and every proof g of conclusion C from hypothesis B (denoted by $g\colon B \to C$) there is a uniquely defined composite proof $g \circ f$ of conclusion C from hypothesis A (denoted by $g \circ f\colon A \to C$),

(ii) this composition of proofs is associative,

(iii) for each formula A there is an identity proof $1_A\colon A \to A$ such that for $f\colon A \to B$ we have $f \circ 1_A = f = 1_B \circ f$, i.e, it behaves as identity w.r.t. composition.

Under these assumptions the proofs are the arrows in a category whose objects are the formulas of the logic. What remains is to provide the right axioms for the "category of proofs".

4.1 Star-Autonomous categories (without units)

In this section we will introduce the concept of star-autonomous categories, because they are the categories of proofs for multiplicative linear logic.

We do not presuppose any knowledge of category theory. We introduce what we need on the way along. It is not much anyway. Let us now add more axioms to (i)–(iii) above, that are specific to logic and do not hold in general in categories:

(iv) Whenever we have a formula A and formula B, then $A \otimes B$ is another formula. For two proofs $f\colon A \to C$ and $g\colon B \to D$ we have a uniquely defined proof $f \otimes g\colon A \otimes B \to C \otimes D$, such that for all $h\colon C \to E$ and $k\colon D \to F$, we have

$$(h \otimes k) \circ (f \otimes g) = (h \circ f) \otimes (h \circ g)\colon A \otimes B \to E \otimes F \quad . \tag{61}$$

Using category theoretical language, Axiom (iv) just says that $\otimes$ is a bifunctor. What does this mean? Consider the following two derivations (using the notation from the calculus of

[3] It first appears in Danos' thesis [Dan90], but he insists that it is joint work with Regnier.

structures):

$$\begin{array}{c} A\otimes B \\ {\scriptstyle f\otimes B}\,\Vert \\ C\otimes B \\ {\scriptstyle C\otimes g}\,\Vert \\ C\otimes D \end{array} \qquad \text{and} \qquad \begin{array}{c} A\otimes B \\ {\scriptstyle A\otimes g}\,\Vert \\ A\otimes D \\ {\scriptstyle f\otimes D}\,\Vert \\ C\otimes D \end{array} \tag{62}$$

In the left one we use first f to go from A to C, and do nothing to B,[4] and then use g to go from B to D (and do nothing to C). In the right derivation, we first use g to go from B to D, and then f to go from A to C. Equation (61) says that the two derivations with premise $A\otimes B$ and conclusion $C\otimes D$ in (62) represent the same proof, denoted by $f\otimes g$. Mathematicians came up with a very clever way of writing an equation between objects as in (62), namely, via *commuting diagrams*. Instead of writing the two derivations in (62) and saying they are equal, we write:

$$\text{The diagram} \qquad \begin{array}{ccc} A\otimes B & \xrightarrow{A\otimes g} & A\otimes D \\ {\scriptstyle f\otimes B}\Big\downarrow & & \Big\downarrow{\scriptstyle f\otimes D} \\ C\otimes B & \xrightarrow[C\otimes g]{} & C\otimes D \end{array} \qquad \text{commutes .}$$

From the proof theoretical viewpoint, this equation is indeed wanted. The difference between the two derivations in (62) is an artefact of syntactic bureaucracy. The kind of bureaucracy in exhibited in (62) is called *bureaucracy of type A*. This implies that there must also be a *bureaucracy of type B*. Consider the following two derivations:

$$\begin{array}{c} A\otimes(B\parr C) \\ {\scriptstyle f\otimes(B\parr C)}\,\Vert \\ \mathsf{s}\,\dfrac{A'\otimes(B\parr C)}{(A'\otimes B)\parr C} \end{array} \qquad \text{and} \qquad \begin{array}{c} \mathsf{s}\,\dfrac{A\otimes(B\parr C)}{(A\otimes B)\parr C} \\ {\scriptstyle (f\otimes B)\parr C}\,\Vert \\ (A'\otimes B)\parr C \end{array} \tag{63}$$

In the left one we first use the proof f, taking us from A to A' (and doing nothing to B and C), and then we apply the switch rule. In the derivation on the right we first apply the switch rule, and then do f. Clearly the two are essentially the same and should be identified eventually. Let us write this as commuting diagram:

$$\begin{array}{ccc} A\otimes(B\parr C) & \xrightarrow{\mathsf{s}_{A,B,C}} & (A\otimes B)\parr C \\ {\scriptstyle f\otimes(B\parr C)}\Big\downarrow & & \Big\downarrow{\scriptstyle (f\otimes B)\parr C} \\ A'\otimes(B\parr C) & \xrightarrow[\mathsf{s}_{A',B,C}]{} & (A'\otimes B)\parr C \end{array} \tag{64}$$

Using category theoretical language, equation (64) says precisely that the morphism $\mathsf{s}_{A,B,C}\colon A\otimes(B\parr C) \to (A\otimes B)\parr C$ is *natural in A*. Of course, in the end, we should have that switch is natural in all three arguments.

Before we can continue with our list of axioms, we need another category theoretical concept. Suppose we have two formulas A and B and proofs $f\colon A\to B$ and $g\colon B\to A$.

[4] More precisely, it is the identity 1_B taking us from B to B.

If we have for some reason that $f \circ g = 1_B$ and $g \circ f = 1_A$, then we say that A and B are *isomorphic*. In this case f and g are *isomorphisms*. The following axiom shows two examples:

(v) For all formulas A, B, and C, we postulate the existence of proofs

$$\begin{aligned} \alpha_{A,B,C}\colon A \otimes (B \otimes C) &\to (A \otimes B) \otimes C \\ \sigma_{A,B}\colon A \otimes B &\to B \otimes A \end{aligned} \tag{65}$$

which are isomorphisms, and which are natural in all arguments,[5] and which obey the following equations:

$$\begin{array}{ccc} A \otimes (B \otimes (C \otimes D)) & \xrightarrow{A \otimes \alpha_{B,C,D}} & A \otimes ((B \otimes C) \otimes D) \\ \downarrow{\scriptstyle \alpha_{A,B,C \otimes D}} & & \downarrow{\scriptstyle \alpha_{A,B \otimes C,D}} \\ (A \otimes B) \otimes (C \otimes D) & & (A \otimes (B \otimes C)) \otimes D \\ & {\scriptstyle \alpha_{A \otimes B,C,D}} \searrow \quad \swarrow {\scriptstyle \alpha_{A,B,C} \otimes D} & \\ & ((A \otimes B) \otimes C) \otimes D & \end{array} \tag{66}$$

$$\begin{array}{ccc} A \otimes (B \otimes C) & \xrightarrow{A \otimes \sigma_{B,C}} & A \otimes (C \otimes B) \\ \downarrow{\scriptstyle \alpha_{A,B,C}} & & \downarrow{\scriptstyle \alpha_{A,C,B}} \\ (A \otimes B) \otimes C & & (A \otimes C) \otimes B \\ \downarrow{\scriptstyle \sigma_{A \otimes B,C}} & & \downarrow{\scriptstyle \sigma_{A,C} \otimes B} \\ C \otimes (A \otimes B) & \xrightarrow[\alpha_{C,A,B}]{} & (C \otimes A) \otimes B \end{array} \tag{67}$$

$$\begin{array}{ccc} A \otimes B & \xrightarrow{\sigma_{A,B}} & B \otimes A \\ & {\scriptstyle 1_{A \otimes B}} \searrow \quad \swarrow {\scriptstyle \sigma_{B,A}} & \\ & A \otimes B & \end{array} \tag{68}$$

What we have defined so far, could be called a *symmetric monoidal category without unit.* This terminology is not standard, because the notion has not much been used in mathematics.

[5] At this point you should start to see why it makes sense to use the category theoretical language. Without it, we would have, for example, to postulate for all formulas A, B, and C another proof $\alpha^{-1}_{A,B,C}$ such that the two derivations

$$\begin{array}{c} A \otimes (B \otimes C) \\ {\scriptstyle \alpha_{A,B,C}} \| \\ (A \otimes B) \otimes C \\ {\scriptstyle \alpha^{-1}_{A,B,C}} \| \\ A \otimes (B \otimes C) \end{array} \qquad \text{and} \qquad \begin{array}{c} (A \otimes B) \otimes C \\ {\scriptstyle \alpha^{-1}_{A,B,C}} \| \\ A \otimes (B \otimes C) \\ {\scriptstyle \alpha_{A,B,C}} \| \\ (A \otimes B) \otimes C \end{array}$$

are both doing nothing (i.e., are equal to the identity proof). Furthermore, we would need a lot of equations in the form of (63), in order to express the naturality.

What is standard is the notion of *monoidal category* and *symmetric monoidal category* (the first one being without the σ), which additionally have a distinguished *unit object* $\mathbf{1}$ and natural isomorphisms $\lambda_A\colon \mathbf{1}\otimes A \to A$ and $\varrho_A\colon A\otimes\mathbf{1}\to A$ obeying the equations

$$\begin{array}{ccc} A\otimes(\mathbf{1}\otimes B) & \xrightarrow{\alpha_{A,\mathbf{1},B}} & (A\otimes\mathbf{1})\otimes B \\ & {\scriptstyle A\otimes\lambda_B}\searrow \quad \swarrow{\scriptstyle \varrho_A\otimes B} & \\ & A\otimes B & \end{array} \quad\text{and}\quad \begin{array}{ccc} \mathbf{1}\otimes A & \xrightarrow{\sigma_{\mathbf{1},A}} & A\otimes\mathbf{1} \\ & {\scriptstyle \lambda_A}\searrow \quad \swarrow{\scriptstyle \varrho_A} & \\ & A & \end{array} \tag{69}$$

An important property of monoidal categories is MacLane's *coherence theorem.* Stated in terms of proofs, it says the following:

4.1.1 Theorem *Let $n\geq 1$ and $A_1,\ldots,A_n$ be formulas. Now let B and C be formulas built from $A_1,\ldots,A_n$ by using $\otimes$ such that every A_i appears exactly once in B and C. If Axioms* (i)–(v) *hold, then all proofs from B to C formed with the available data are equal. This proof always exists, is an isomorphism, and is natural in all n arguments.*

We will not give a proof here.

For being able to really speak about logic and proofs, we need negation, which is introduced by the following axioms:

(vi) For every formula A there is another formula $A^\perp$, and for every proof $f\colon A\to B$, there is another proof $f^\perp\colon B^\perp\to A^\perp$ such that $1_A^\perp = 1_{A^\perp}\colon A^\perp\to A^\perp$ and such that $(g\circ f)^\perp = f^\perp\circ g^\perp\colon C^\perp\to A^\perp$ for every $f\colon A\to B$ and $g\colon B\to C$.

(vii) For every formula A and proof $f\colon A\to B$ we have that $A^{\perp\perp}=A$ and $f^{\perp\perp}=f$. (More precisely, the mapping $A^{\perp\perp}\to A$ is the identity on A).

Spoken in category theoretical terms, Axiom (vi) says that $(-)^\perp$ is a *contravariant endofunctor*. With this, we can define the $\parr$ via $A\parr B = (A^\perp\otimes B^\perp)^\perp$. Axiom (vii) says that if we flip around a derivation twice, we get back where we started from.[6] It also allows us to conclude that the $\parr$ that we just defined has the same properties as postulated for the $\otimes$ in (iv) and (v), i.e., it is a bifunctor and carries a monoidal structure (without unit).

4.1.2 Exercise Formulate the statements of Axioms (iv) and (v) for the $\parr$ defined via $A\parr B=(A^\perp\otimes B^\perp)^\perp$, and show that they follow from (i)–(vii).

Before stating our final postulates about proofs, let us introduce the following notation. For two formulas A and B, we write $\mathrm{Hom}(A,B)$ for the set of proofs from A to B, and we write $h^{\mathbb{1}}(B)$ for the set of proofs of B that have no premise.[7]

[6] What we impose here is also called *strictness*, and does usually not hold. For example, the double dual of a vector space is usually not the space itself. Even in the finite dimensional case we only have a natural isomorphism between A and $A^{\perp\perp}$.

[7] The reason for this notation is the following: $\mathrm{Hom}(A,B)$ is in fact the value of the functor $\mathrm{Hom}(-,-)$ in two arguments. The functor $\mathrm{Hom}(A,-)$ in one argument is also written as h^A. If there is a proper unit $\mathbf{1}$ then the proofs of A are the elements of the set $\mathrm{Hom}(\mathbf{1},A)$, i.e., $h^{\mathbf{1}}$ is a functor mapping every formula to its set of proofs. In $h^{\mathbb{1}}$, the unit is *virtual*.

(viii) For all formulas A, B, and C, there is a bijection

$$\varphi\colon \mathrm{Hom}(A \otimes B, C) \to \mathrm{Hom}(A, B^{\perp} \mathbin{⅋} C) \tag{70}$$

which is natural in all three arguments.

(ix) For all formulas A and B, we have a bijection

$$\varphi\colon h^{\mathbb{1}}(A^{\perp} \mathbin{⅋} B) \to \mathrm{Hom}(A, B) \tag{71}$$

which is natural in both arguments and respects the monoidal structure.

In the case with units, Axiom (viii) would complete the definition of a **-autonomous category*. It essentially says that we are allowed to do *currying* and *uncurrying*. To see this, note that linear logic knows the connective $\multimap$, standing for *linear implication*, defined via $A \multimap B = A^{\perp} \mathbin{⅋} B$.[8] Equation (70) now says that we can jump freely back and forth between proofs $A \otimes B \to C$ and $A \to B \multimap C$.[9]

Since we do not have units, we also need (ix), which says that the proofs of $A \multimap B$ are the same as the proofs $A \to B$. To be precise, we need to give additional equation saying that $h^{\mathbb{1}}$ is a functor, i.e., every proof $f\colon A \to B$ is mapped to a function $h^{\mathbb{1}}(f)\colon h^{\mathbb{1}}(A) \to h^{\mathbb{1}}(B)$ such that composition and identity are preserved. Furthermore, the $h^{\mathbb{1}}$ needs to go well along with the monoidal structure, to say what that means exactly would take us too far astray. But to give you an idea of the problem, let us figure out how we could construct a proof $B \to (A \mathbin{⅋} A^{\perp}) \otimes B$, corresponding to the rule $\mathsf{i}{\downarrow}$ in (38), by using the axioms (i)–(ix). If we had a unit $\mathbf{1}$ together with the equations (69), then it would be easy: we could start out with $\lambda_A\colon \mathbf{1} \otimes A \to A$, apply (70) to get

$$\hat{\lambda}_A = \varphi(\lambda_A)\colon \mathbf{1} \to A \mathbin{⅋} A^{\perp}$$

By (iv), we can form a proof $\hat{\lambda}_A \otimes 1_B\colon \mathbf{1} \otimes B \to (A \mathbin{⅋} A^{\perp}) \otimes B$. We can precompose this with $\lambda_B^{-1}\colon B \to \mathbf{1} \otimes B$, to get

$$(\hat{\lambda}_A \otimes 1_B) \circ \lambda_B^{-1}\colon B \to (A \mathbin{⅋} A^{\perp}) \otimes B$$

Constructing this map without using the unit requires heavy category theoretical machinery that we are not going to show here. See Section 4.2 for references.

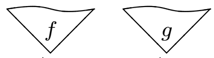
4.1.3 Exercise We mentioned switch in (63) and (64) but we did not postulate it in (i)–(ix). In this exercise you are asked to construct $\mathsf{s}_{A,B,C}\colon A \otimes (B \mathbin{⅋} C) \to (A \mathbin{⅋} B) \otimes C$, corresponding to the switch rule in (28) or Figure 6, by using (i)–(viii). Hint: Start with the identity $B \otimes C \to B \otimes C$ and apply (70). You will also need the associativity of ⅋ that you have constructed in Exercise 4.1.2.

The purpose of Axioms (i)–(ix) is that they precisely describe the mathematical structure spanned by cut-free proof nets for MLL^{-}. Ideally this should mean two things:

[8] As in classical logic, "A implies B" is the same as "not A or B".

[9] If you have never seen currying, think of a function f in two arguments, denoted by $f\colon A \times B \to C$. This is essentially the same as a function $f'\colon A \to B \to C$, taking and argument from the set A and returning a function $B \to C$ which asks for an element of B to finally return the result in C.

First, the proof nets for MLL^- that we discussed in the previous sections form a category: The objects are the formulas and the maps $A \to B$ are the cut-free proof nets with conclusion $\vdash A^\perp, B$ and the composition $g \circ f$ of two maps $f\colon A \to B$ and $g\colon B \to C$ is defined by eliminating the cut from



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

In the calculus of structures, this corresponds to performing the composition

$$\begin{array}{c} A \\ \| \\ B \\ \| \\ C \end{array} \quad \to \quad \begin{array}{c} A \\ \| \\ C \end{array}$$

It is easy to verify that this category, denoted by **PN**, obeys (i)–(ix) (where $h^{\mathbb{1}}(A)$ is just the set of cut-free proof nets with conclusion A).

Second, the the category **PN** should be the free category with this property. This means that whenever there is a category $\mathscr{C}$, obeying (i)–(ix), then there is a uniquely defined functor (i.e., map that preserves all the structure defined in (i)–(ix)) from **PN** to $\mathscr{C}$.

Another way of seeing this is that we can trivially translate proofs in the sequent calculus or the calculus of structures into the free *-autonomous category (without units), by simply following the syntax. If we do this to two proofs Π_1 and Π_2, we get the same map in the category, if and only if Π_1 and Π_2 yield the same proof net after cut elimination.

In other words, if you have no objections against any of the Axioms (i)–(ix), you must answer the Big Question 3.6.4 with **yes**.

But there is also a **but**: Let us emphasize that this yes is valid only for MLL^-. What we have said in this section does **not** allow us to draw any conclusions about any other logic.

4.1.4 Open Problem *There is a "creative tension" between algebra and proof theory: A star-autonomous category is a well-defined object, but it contains the unit, which cause problems for proof nets. This is the reason why we considered only unit-free proof nets. To describe these algebraically, we introduced unit-free star-autonomous categories. However, the axioms we gave are not quite right, because we do not have a theorem saying that the category* **PN** *is indeed the free star-autonomous category without units, as we desire. The problem is to find the right axioms making such a theorem true.*

4.2 Notes

The observation that cut elimination is composition in a category is due to Lambek [Lam68, Lam69]. The terminology "coherence" is due to MacLane. In [Mac63] he proves the "coherence theorem" for symmetric monoidal categories. See also [Mac71].

Star-autonomous categories have been discovered by Barr [Bar79]. That there is a relation to linear logic was discovered immediately after the introduction of linear logic (see, e.g., [Laf88, See89]). Blute [Blu93] was the first to note that the category of proof nets is actually the free *-autonomous category without units. However, no complete proof was given; there was no proper definition of a *-autonomous category without units. That there is in fact a non-trivial mathematical problem to give such a definition was observed only 12 years later, but then by three research groups independently at the same time [LS05a, DP05, HHS05]. The most in-depth treatment is [HHS05]. We used here the notation of [LS05a].

The terminology of "Formalism A" and "Formalism B" is due to Guglielmi [Gug04a, Gug04b]. See also [Hug04, McK05, Str09, Str07] for the relation between deep inference and category theory.

5 What is the problem of proof nets for classical logic?

In this section we are trying to do the same for classical propositional logic as we did for multiplicative linear logic in Section 3. In order to better understand the problems that we are going to encounter with proof nets for classical logic, let us first have a look at intuitionistic logic.

5.1 From intuitionistic logic to classical logic

In intuitionistic logic the law of the excluded middle does not hold, and $\neg\neg A$ does not imply A. The natural deduction system NJ for intuitionistic logic is obtaind from NK by removing the rule $\neg\neg$E [Gen34]. The sequent system LJ fo intuitionistic logic is the same as LK, with the restriction that the right-hand side of a sequent can contain at most one formula. This means in particular that the contraction rule can no longer be applied on the right [Gen34].

5.1.1 Exercise Try to prove the law of excluded middle, i.e., the formula $\neg A \vee A$ in NJ and LJ. Why does it fail?

If we write the natural deduction rules $\to$E and $\to$I in the sequent style way:

$$\to\mathrm{I}\,\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \qquad \text{and} \qquad \to\mathrm{E}\,\frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

they are the same as the typing rules for the simply typed λ-calculus:

$$\mathsf{abs}\,\frac{\Gamma, x\colon A \vdash u\colon B}{\Gamma \vdash \lambda x.u\colon A \to B} \qquad \text{and} \qquad \mathsf{app}\,\frac{\Gamma \vdash u\colon A \to B \quad \Gamma \vdash v\colon A}{\Gamma \vdash uv\colon B}$$

We will not go into further details here. The inportant fact to know is that this is the basis for the so-called *Curry-Howard-correspondence* (also known as *formulas-as-types-correspondence* and *proofs-as-programs-correspondence*). It is also called "isomorphism" because the normalization in natural deduction [Pra65] does the same as β-reduction in the λ-calculus.[10] If we add conjunction to the logic (or equivalently product types to the λ-calculus) we can use the proofs in natural deduction (or equivalently λ-terms) for specifying morphism in *cartesian closed categories* (short: *CCCs*). What makes things interesting is the fact that the identity

[10] One could also argue that we have here just two different syntactic presentations of the same mathematical objects.

forced on proofs by the notion of normalization in natural deduction (or equivalently the identity forced on λ-terms by normalization[11]) is exactly the same as the identity of morphism that is determined by the axioms of CCCs. For further details on this see [LS86]. Of course, this simple observation has been extended to more expressive logics and larger type systems (e.g., System F [Gir72], calculus of constructions [CH88], ...).

We have a very close and well-understood relationship between proofs in intuitionistic logic, simply typed lambda-terms, and morphisms in Cartesian closed categories. As we have seen in Sections 3 and 4, a similar relationship can be established for multiplicative linear logic (MLL), where proof nets take the role of the lambda-terms, and star-autonomous categories the role of Cartesian closed categories.

It is certainly desirable to have something similar for classical logic, which can be obtained from intuitionistic logic by adding the law of excluded middle, i.e., $A \vee \bar{A}$, or equivalently, an involutive negation, i.e., $\bar{\bar{A}} = A$. Adding this to a Cartesian closed category $\mathscr{C}$, means adding a contravariant functor $\overline{(-)}\colon \mathscr{C} \to \mathscr{C}$ such that $\bar{\bar{A}} \cong A$ and $\overline{(A \wedge B)} \cong \bar{A} \vee \bar{B}$ where $A \vee B = \bar{A} \to B$. However, if we do this we get a collapse: all proofs of the same formula are identified, which leads to a rather boring proof theory. This observation is due to André Joyal, and a proof and discussion can be found in [LS86, Gir91, Str07].

Here we will not show the category theoretic proof of the collapse, but will quickly explain the phenomenon in terms of the sequent calculus (the argumentation is due to Yves Lafont [GLT89, Appendix B]). Suppose we have two proofs Π_1 and Π_2 of a formula B in some sequent calculus system. Then we can form, with the help of the rules weakening, contraction, and cut, the following proof of B:

$$\mathsf{cont}\,\dfrac{\mathsf{cut}\,\dfrac{\mathsf{weak}\,\dfrac{\overset{\Pi_1}{\vdash B}}{\vdash B, A} \qquad \mathsf{weak}\,\dfrac{\overset{\Pi_2}{\vdash B}}{\vdash \bar{A}, B}}{\vdash B, B}}{\vdash B} \tag{72}$$

If we apply cut elimination to this proof, we get either

$$\mathsf{cont}\,\dfrac{\mathsf{weak}\,\dfrac{\overset{\Pi_1}{\vdash B}}{\vdash B, B}}{\vdash B} \qquad \text{or} \qquad \mathsf{cont}\,\dfrac{\mathsf{weak}\,\dfrac{\overset{\Pi_2}{\vdash B}}{\vdash B, B}}{\vdash B} \tag{73}$$

depending on a nondeterministic choice. On the other hand, if we want the nice relationship between deductive system and category theory, we need a confluent cut elimination, which means that the two proofs in (73) must be the same. Consequently, we have to equate Π_1 and Π_2. Since there was no initial condition on Π_1 and Π_2, we conclude that any two proofs of B must be equal.

[11] β-reduction, η-expansion, and α-conversion

The problem with weakening, which could in fact be solved by using the mix-rule

$$\mathsf{mix}\ \frac{\vdash \Gamma \quad \vdash \Delta}{\vdash \Gamma, \Delta} \quad , \tag{74}$$

is not the only one. We run into similar problems with the contraction rule. If we try to eliminate the cut from

$$\mathsf{cut}\ \frac{\mathsf{cont}\ \dfrac{\overset{\Pi_1}{\vdash \Gamma, A, A}}{\vdash \Gamma, A} \qquad \mathsf{cont}\ \dfrac{\overset{\Pi_2}{\vdash \bar{A}, \bar{A}, \Delta}}{\vdash \bar{A}, \Delta}}{\vdash \Gamma, \Delta} \quad . \tag{75}$$

we again have to make a nondeterministic choice. In Section 5.2, we will see a concrete example for this.

There are several possibilities to cope with these problems. Clearly, we have to drop some of the equations that we would like to hold between proofs in classical logic. But which ones should go?

There are now essentially three different approaches, and all three have their advantages and disadvantages.

1. The first says that the axioms of Cartesian closed categories are essential and cannot be dispensed with. Instead, one sacrifices the duality between $\wedge$ and $\vee$. The motivation for this approach is that a proof system for classical logic can now be seen as an extension of the λ-calculus and the notion of normalization does not change. One has a term calculus for proofs, namely Parigot's $\lambda\mu$-calculus [Par92] and a denotational semantics [Gir91]. An important aspect is the computational meaning in terms of continuations [Thi97, SR98]. There is a well explored category theoretical axiomatization [Sel01], and, of course, a theory of proof nets [Lau03], which is based on the proof nets for multiplicative exponential linear logic (MELL).

2. The second approach considers the perfect symmetry between $\wedge$ and $\vee$ to be an essential facet of Boolean logic, that cannot be dispensed with. Consequently, the axioms of Cartesian closed categories and the close relation to the λ-calculus have to be sacrificed. More precisely, the conjunction $\wedge$ is no longer a Cartesian product, but merely a tensor-product. Thus, the Cartesian closed structure is replaced by a star-autonomous structure, as it it known from linear logic. However, the precise category theoretical axiomatization is much less clear than in the first approach (see [FP04, LS05a, McK05, Str07, Lam07]).

3. The third approach keeps the perfect symmetry between $\wedge$ and $\vee$, as well as the Cartesian product property for $\wedge$. What has to be dropped is the property of being closed, i.e., there is no longer a bijection between the proofs of

$$A \vdash B \to C \qquad \text{and} \qquad A \wedge B \vdash C \quad ,$$

which means we lose currying. This approach is studied in [DP04, CS09].

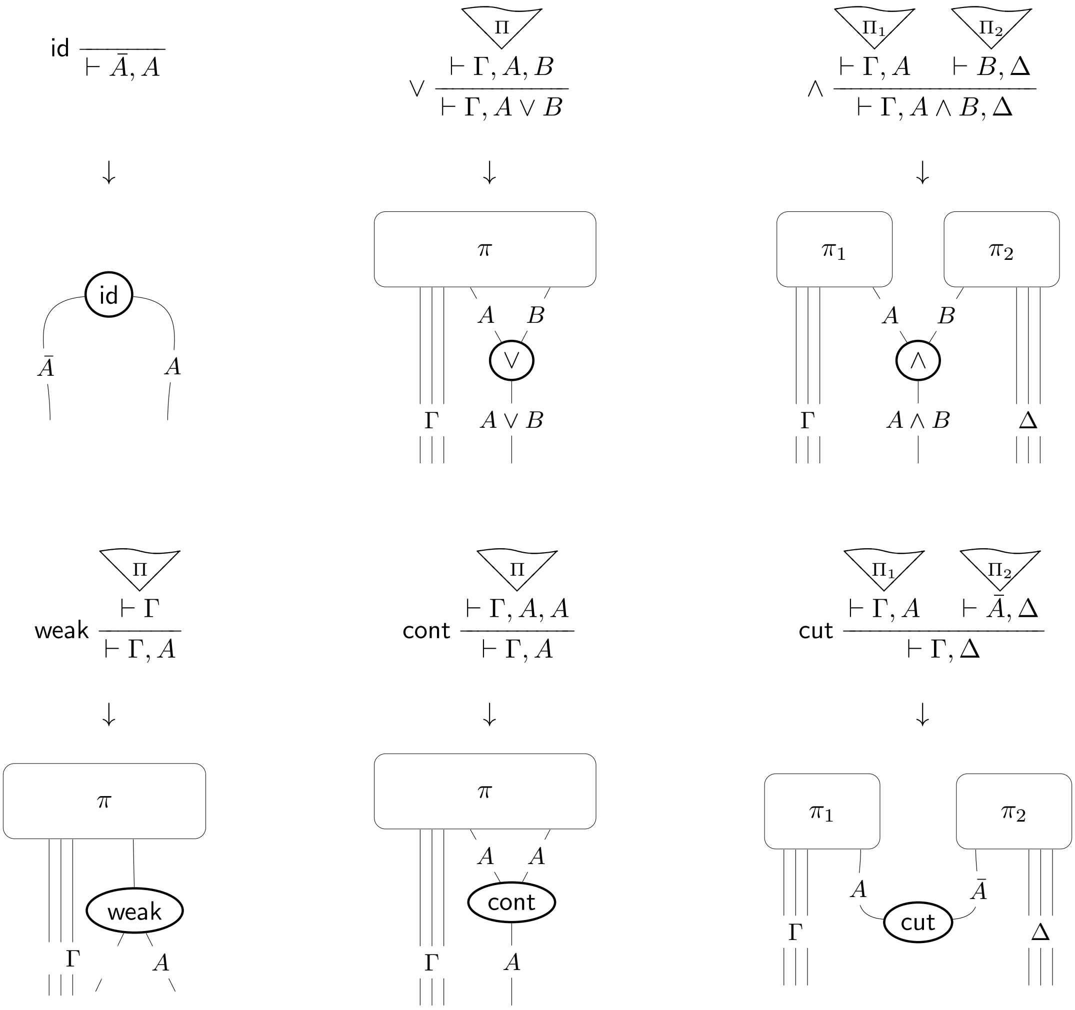


Figure 17: From sequent calculus to proof nets (sequent rule ideology)

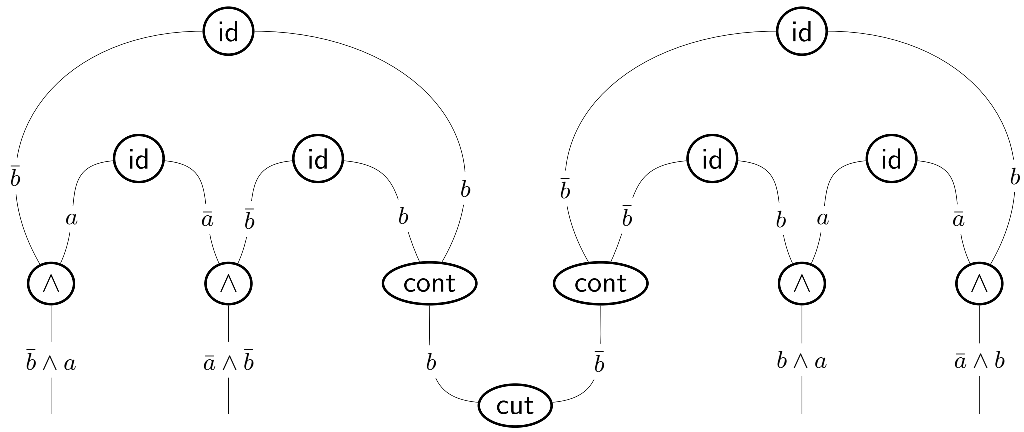
Here, we only focus on the second approach, and discuss what happens when we apply the two "ideologies" introduced in Section 3. As mentioned before, for MLL^-, the two ideologies produce the same notion of proof nets. However, for classical logic the situation is very different.

5.2 Sequent calculus rule based proof nets

Consider again the one-sided sequent system for classical logic shown in Figure 5. In Figure 17 we show how these rules can be translated into proof nets via the sequent rule ideology. That this can be done has first been indicated by Girard [Gir91], and detailed out by Robinson [Rob03]. For simplicity, we consider here the outputs to be unordered and ignore the exchange rule. Here is an example of a sequent calculus proof

$$
\mathsf{cut}\,\dfrac{\mathsf{cont}\,\dfrac{\wedge\,\dfrac{\wedge\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash \bar{b}, b}\quad \mathsf{id}\,\dfrac{}{\vdash a, \bar{a}}}{\vdash \bar{b}\wedge a, \bar{a}, b}\quad \mathsf{id}\,\dfrac{}{\vdash \bar{b}, b}}{\vdash \bar{b}\wedge a, \bar{a}\wedge\bar{b}, b, b}}{\vdash \bar{b}\wedge a, \bar{a}\wedge\bar{b}, b}\qquad \mathsf{cont}\,\dfrac{\wedge\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash \bar{b}, b}\quad \wedge\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash a, \bar{a}}\quad \mathsf{id}\,\dfrac{}{\vdash \bar{b}, b}}{\vdash \bar{b}, a, \bar{a}\wedge b}}{\vdash \bar{b}, \bar{b}, b\wedge a, \bar{a}\wedge b}}{\vdash \bar{b}, b\wedge a, \bar{a}\wedge b}}{\vdash \bar{b}\wedge a, \bar{a}\wedge\bar{b}, b\wedge a, \bar{a}\wedge b} \tag{76}
$$

and its translation into a proof net:

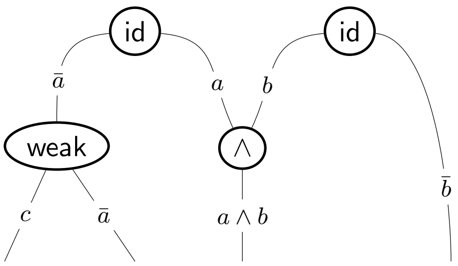


(77)

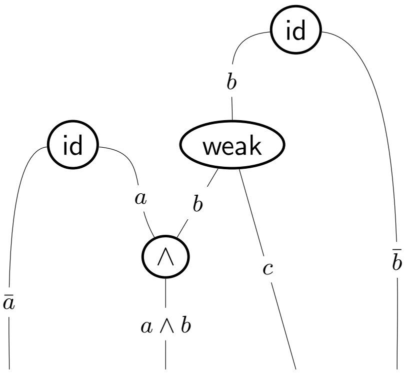
The advantage of the sequent-rule-ideology is that all the correctness criteria for MLL proof nets hold unchanged. For example, the switching criterion (see Section 3.5), where contraction nodes are treated as $\vee$-nodes, and weakening nodes as $\wedge$-nodes, does hold. There are however two main disadvantages of the sequent-rule-ideology. The first is that certain proofs are distinguished that should be identified according the rule-permutability-argument. To see a very simple example, consider the following three sequent calculus proofs:

$$
\wedge\,\dfrac{\mathsf{weak}\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash \bar{a}, a}}{\vdash c, \bar{a}, a}\quad \mathsf{id}\,\dfrac{}{\vdash b, \bar{b}}}{\vdash c, \bar{a}, a\wedge b, \bar{b}}
\qquad
\mathsf{weak}\,\dfrac{\wedge\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash \bar{a}, a}\quad \mathsf{id}\,\dfrac{}{\vdash b, \bar{b}}}{\vdash \bar{a}, a\wedge b, \bar{b}}}{\vdash c, \bar{a}, a\wedge b, \bar{b}}
\qquad
\wedge\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash \bar{a}, a}\quad \mathsf{weak}\,\dfrac{\mathsf{id}\,\dfrac{}{\vdash b, \bar{b}}}{\vdash c, b, \bar{b}}}{\vdash c, \bar{a}, a\wedge b, \bar{b}} \tag{78}
$$

They differ from each other only via some trivial rule permutation, and should therefore be identified. But they can be translated into five different proof nets. Two of them are shown below:



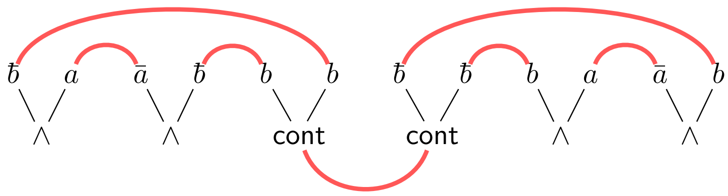
and



(79)

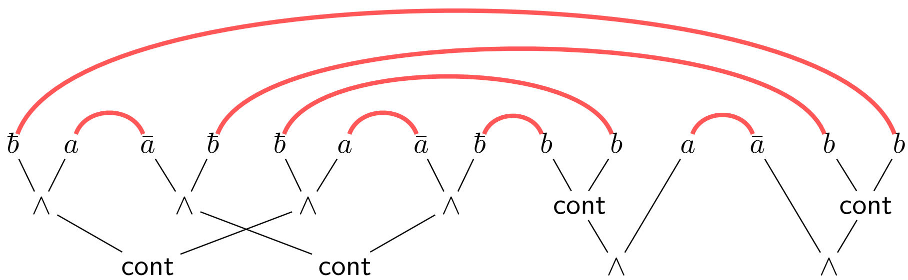
The problem is that there is no canonical choice of where to attach the weakening. A possible solution could be to leave the weakenings unconnected, but this would break the correctness criteria.

The second disadvantage of the sequent-rule-ideology is related to cut elimination. In the introduction we have seen already the problem with weakening. Let us now have a closer look at contraction, when it appears at both sides of a cut, as shown in the example in (76) and (77). For typesetting reasons, let us use the more compact notation:



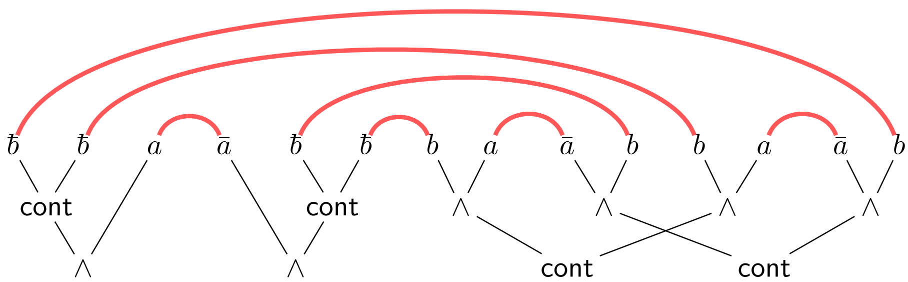
(80)

We have here an example for the general case in (75). If we want to eliminate the cut from (80), we have to make a nondeterministic choice, which subproof we duplicate. As outcome we get either



(81)

or



(82)

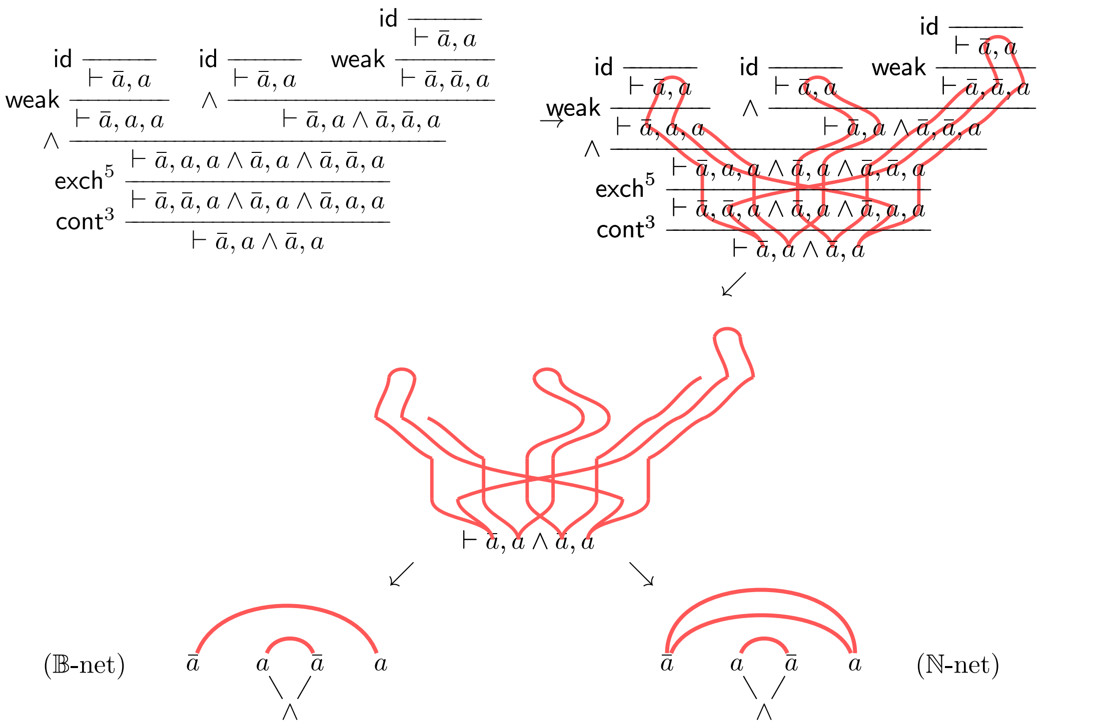


Figure 18: From sequent calculus to proof nets (flow graph ideology)

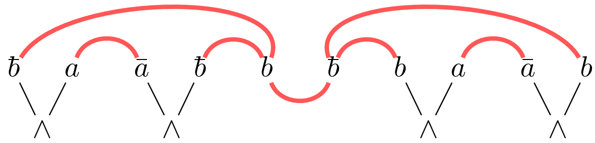
In [Gir91], Girard argues that for this reason it is impossible to have a confluent notion of cut elimination for proof nets for classical logic. Of course, his argumentation is valid only for proof nets following the sequent-rule-ideology.

Thus, for changing the situation with cut elimination, one has to change the ideology.

5.3 Flow graph based proof nets

The basic idea is to draw the flow graph [Bus91] of the proof as indicated in Figure 18. The important question is what information should be kept. In [LS05b] there are two proposals. The first takes the sequent forest and adds an edge between a pair of dual atoms if they are connected by a path in the flow graph. This yields the $\mathbb{B}$-nets of [LS05b], and an example is shown on the lower left of Figure 18. The second approach also keeps the number of paths between two atoms. The result is called $\mathbb{N}$-nets in [LS05b]. This is denoted by either labeling the edge between the two atoms by a natural number, or by drawing multiple edges, as shown on the lower right of Figure 18. In both cases it can happen that some atoms have no mate, i.e., live celibate, and that some atoms have more than one mate, i.e., live polygamous. This is the main difference to MLL^- proof nets, where every single atom lives monogamous.

Cuts are shown as special edges between the roots of the formula trees, as in this example, which is obtained from the sequent proof in (76):



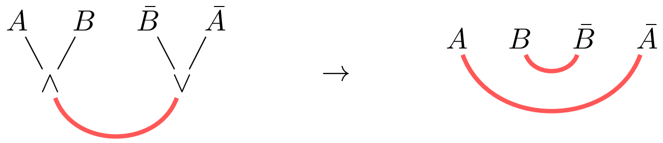
(83)

The disadvantage of the flow-graph-ideology is that the correctness criteria from linear logic are no longer available. However, for $\mathbb{B}$-nets there is a correctness criterion that is similar to the criterion for matings [And76] and matrix proofs [Bib81]: A $\mathbb{B}$-net is the translation of a sequent proof if and only if each of its conjunctive prunings contains at least one axiom link edge, where a conjunctive pruning for π is obtained from π by deleting for each of its $\wedge$-nodes one of the two subtrees including the outgoing axiom link edges.

The main problem with this criterium is that checking it takes exponential time in the size of the input. This means that checking a given proof is as expensive as finding the proof from scratch.

Furthermore, this criterion does not work for $\mathbb{N}$-nets because it does not take into account how often an axiom link edge is used, and it is an open problem to find some correctness criterion for $\mathbb{N}$-nets.

Let us now look at cut elimination. Reducing cuts on compound formulas is exactly the same as in Section 3.6:

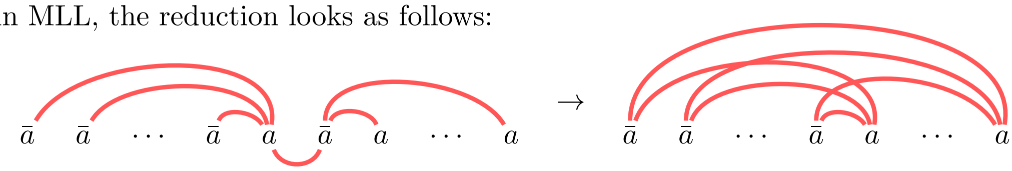


(84)

For the cut reduction on atomic cuts, we have to be careful, since the atoms can be connected to many other atoms (or no other atoms). Instead of simply having:

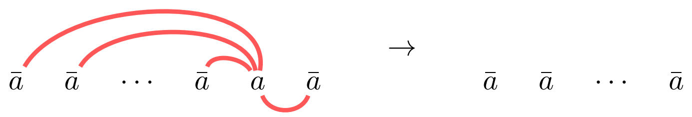
(85)

as in MLL, the reduction looks as follows:



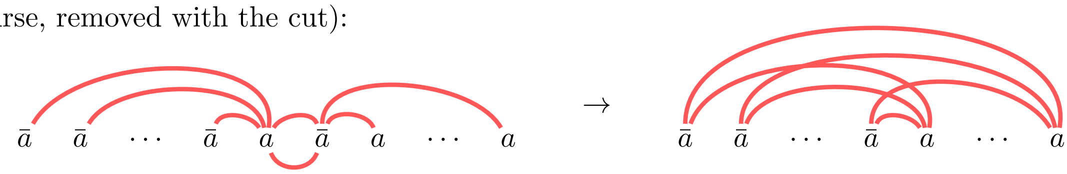
(86)

If one of the two cut atoms is celibate, no link remains:



(87)

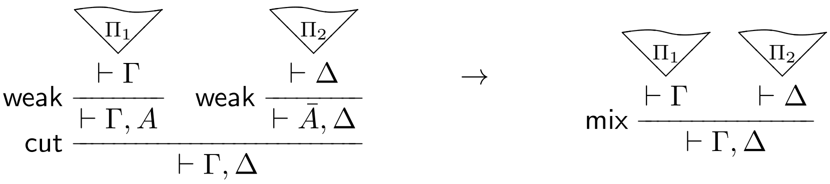
If the two cut atoms are linked together, then this link is ignored in the reduction (and, of course, removed with the cut):



We certainly have termination of the cut reduction. The interesting observation is that for $\mathbb{B}$-nets, the cut reduction preserves correctness and is confluent.

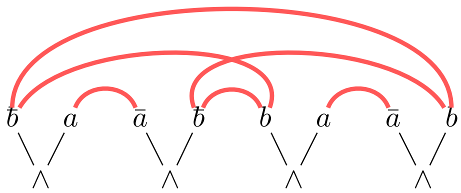
The natural question that arises now is: How does this confluent cut elimination relate to the non-confluent cut elimination in the sequent calculus?

Let us look again at the two problematic cases (72) and (75). The problem with weakening (72) can easily be solved by using the mix-rule in the sequent calculus:



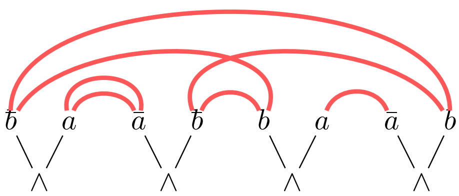
Both subproofs Π_1 and Π_2 are kept in the reduced net, and in $\mathbb{B}$-nets and $\mathbb{N}$-nets it is done in the same way.

For the contraction case (75) the situation is less obvious. Consider again the proof net in (83), which corresponds to the sequent calculus proof in (76). If we apply the cut reduction (86), we obtain the following result:

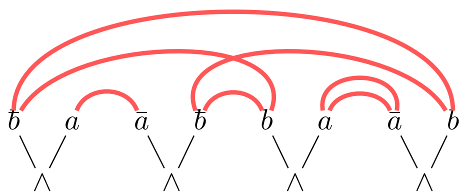


(88)

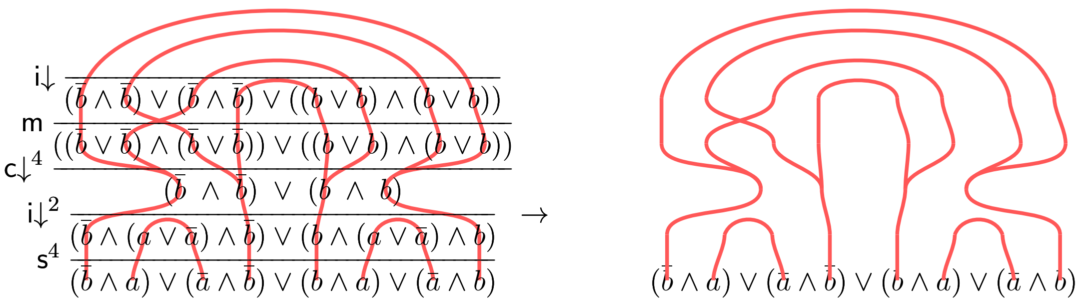
which is exactly the $\mathbb{B}$-net obtained from the sequent proofs corresponding to (81) and (82). This correspondence makes crucial use of the fact that we deliberately forget how often an identity link is used in the proof. As $\mathbb{N}$-nets, the proofs in (81) and (82) would be represented by



and

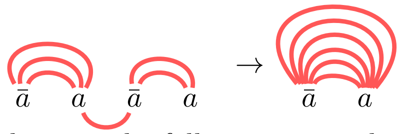


respectively (see [LS05b] for further details). However, although it is not possible to have (88) as $\mathbb{N}$-net of a sequent proof, it can be obtained as a $\mathbb{N}$-net of a proof in the calculus of structures, more precisely in system SKS, as presented in:

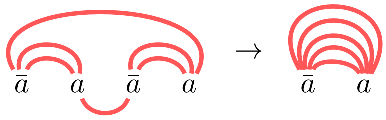


This means that any correctness criterion for ℕ-nets must depend on the chosen deductive system.

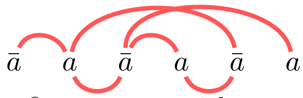
The non-confluence of cut-reduction for ℕ-nets has the following reason. When we reduce an atomic cut, we have to multiply the number of edges, and if there are already some links between the remaining pair of atoms, then these links have to be added. For example



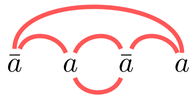
and



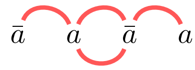
Consider now the following example:



Depending on which cut we reduce first, we get either



or



If we reduce the remaining cut, we get

or

respectively. The solution for circumventing this problem is to reduce atomic cuts only in unproblematic situations like (85) and (87), and leave all atomic cuts like (86) unreduced, as it is done for C-nets in [Str09]. C-nets are a variant of ℕ-nets that are considered cut-free if they contain only atomic cuts that touch a contraction on both sides. In this way C-nets can also capture the size of a proof, because the reduction (86) is the only one which causes an exponential blow-up of the proof. C-nets can also be used as coherence graphs for SKS-derivations. The same approach is taken by the recently developed atomic flows [GG08].

References

[And76] Peter B. Andrews. Refutations by matings. *IEEE Transactions on Computers*, C-25:801–807, 1976.

[Bar79] Michael Barr. **-Autonomous Categories*, volume 752 of *Lecture Notes in Mathematics*. Springer, 1979.

[Bib81] Wolfgang Bibel. On matrices with connections. *Journal of the ACM*, 28:633–645, 1981.

[Blu93] Richard Blute. Linear logic, coherence and dinaturality. *Theoretical Computer Science*, 115:3–41, 1993.

[Brü03] Kai Brünnler. *Deep Inference and Symmetry for Classical Proofs*. PhD thesis, Technische Universität Dresden, 2003.

[BT01] Kai Brünnler and Alwen Fernanto Tiu. A local system for classical logic. In R. Nieuwenhuis and A. Voronkov, editors, *LPAR 2001*, volume 2250 of *LNAI*, pages 347–361. Springer, 2001.

[Bus91] Samuel R. Buss. The undecidability of k-provability. *Annals of Pure and Applied Logic*, 53:72–102, 1991.

[BvdW95] Gianluigi Bellin and Jacques van de Wiele. Subnets of proof-nets in MLL^-. In J.-Y. Girard, Y. Lafont, and L. Regnier, editors, *Advances in Linear Logic*, volume 222 of *London Mathematical Society Lecture Notes*, pages 249–270. Cambridge University Press, 1995.

[CH88] Thierry Coquand and Gérard P. Huet. The calculus of constructions. *Information and Computation*, 76(2/3):95–120, 1988.

[CS09] J. Robin B. Cockett and Luigi Santocanale. On the word problem for ΣΠ-categories, and the properties of two-way communication. In *Computer Science Logic, CSL'09*, volume 5771 of *Lecture Notes in Computer Science*, pages 194–208. Springer, 2009.

[Dan90] Vincent Danos. *La logique linéaire appliquée l'étude de divers processus de normalisation (principalement du λ-calcul)*. Thèse de Doctorat, Université Paris VII, 1990.

[DHPP99] H. Devarajan, Dominic Hughes, Gordon Plotkin, and Vaughan R. Pratt. Full completeness of the multiplicative linear logic of Chu spaces. In *14th IEEE Symposium on Logic in Computer Science (LICS 1999)*, 1999.

[DP04] Kosta Došen and Zoran Petrić. *Proof-Theoretical Coherence*. KCL Publ., London, 2004.

[DP05] Kosta Došen and Zoran Petrić. Proof-net categories. preprint, Mathematical Institute, Belgrade, 2005.

[DR89] Vincent Danos and Laurent Regnier. The structure of multiplicatives. *Annals of Mathematical Logic*, 28:181–203, 1989.

[EK66] Samuel Eilenberg and Gregory Maxwell Kelly. A generalization of the functorial calculus. *Journal of Algebra*, 3(3):366–375, 1966.

[FP04] Carsten Führmann and David Pym. Order-enriched categorical models of the classical sequent calculus. To appear in *J. of Pure and Applied Algebra*, 2004.

[Gen34] Gerhard Gentzen. Untersuchungen über das logische Schließen. I. *Mathematische Zeitschrift*, 39:176–210, 1934.

[Gen35] Gerhard Gentzen. Untersuchungen über das logische Schließen. II. *Mathematische Zeitschrift*, 39:405–431, 1935.

[GG08] Alessio Guglielmi and Tom Gundersen. Normalisation control in deep inference via atomic flows. *Logical Methods in Computer Science*, 4(1:9):1–36, 2008.

[Gir72] Jean-Yves Girard. *Interprétation fonctionelle et élimination des coupures de l'arithmétique d'ordre supérieur*. PhD thesis, Université Paris VII, 1972.

[Gir87] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.

[Gir91] Jean-Yves Girard. A new constructive logic: Classical logic. *Math. Structures in Comp. Science*, 1:255–296, 1991.

[GLT89] Jean-Yves Girard, Yves Lafont, and Paul Taylor. *Proofs and Types*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1989.

[Göd31] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[GS01] Alessio Guglielmi and Lutz Straßburger. Non-commutativity and MELL in the calculus of structures. In Laurent Fribourg, editor, *Computer Science Logic, CSL 2001*, volume 2142 of *LNCS*, pages 54–68. Springer-Verlag, 2001.

[Gue99] Stefano Guerrini. Correctness of multiplicative proof nets is linear. In *LICS*, pages 454–463, 1999.

[Gug04a] Alessio Guglielmi. Formalism A. note, April 2004.

[Gug04b] Alessio Guglielmi. Formalism B. note, December 2004.

[Gug07] Alessio Guglielmi. A system of interaction and structure. *ACM Transactions on Computational Logic*, 8(1), 2007.

[HA28] David Hilbert and Wilhelm Ackermann. *Grundzüge der theoretischen Logik*, volume XXVII of *Die Grundlehren der Mathematischen Wissenschaften*. Verlag von Julius Springer, 1928.

[HHS05] Robin Houston, Dominic Hughes, and Andrea Schalk. Modelling linear logic without units (preliminary results). Preprint, 2005.

[Hil22] David Hilbert. Die logischen Grundlagen der Mathematik. *Mathematische Annalen*, 88:151–165, 1922.

[Hug04] Dominic Hughes. Deep inderence proof theory equals categorical proof theory minus coherence. preprint, 2004.

[KM71] Gregory Maxwell Kelly and Saunders Mac Lane. Coherence in closed categories. *J. of Pure and Applied Algebra*, 1:97–140, 1971.

[Laf88] Yves Lafont. The linear abstract machine. *Theoretical Computer Science*, 59(1–2):157–180, 1988.

[Laf95] Yves Lafont. From proof nets to interaction nets. In J.-Y. Girard, Y. Lafont, and L. Regnier, editors, *Advances in Linear Logic*, volume 222 of *London Mathematical Society Lecture Notes*, pages 225–247. Cambridge University Press, 1995.

[Lam58] Joachim Lambek. The mathematics of sentence structure. *American Mathematical Monthly*, 65:154–169, 1958.

[Lam68] Joachim Lambek. Deductive systems and categories. I: Syntactic calculus and residuated categories. *Math. Systems Theory*, 2:287–318, 1968.

[Lam69] Joachim Lambek. Deductive systems and categories. II. standard constructions and closed categories. In P. Hilton, editor, *Category Theory, Homology Theory and Applications*, volume 86 of *Lecture Notes in Mathematics*, pages 76–122. Springer, 1969.

[Lam07] François Lamarche. Exploring the gap between linear and classical logic. *Theory and Applications of Categories*, 18(18):473–535, 2007.

[Lau03] Olivier Laurent. Polarized proof-nets and $\lambda\mu$-calculus. *Theoretical Computer Science*, 290(1):161–188, 2003.

[LS86] Joachim Lambek and Phil J. Scott. *Introduction to higher order categorical logic*, volume 7 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 1986.

[LS05a] François Lamarche and Lutz Straßburger. Constructing free Boolean categories. In *LICS'05*, pages 209–218, 2005.

[LS05b] François Lamarche and Lutz Straßburger. Naming proofs in classical propositional logic. In Paweł Urzyczyn, editor, *TLCA'05*, volume 3461 of *LNCS*, pages 246–261. Springer, 2005.

[Mac63] Saunders Mac Lane. Natural associativity and commutativity. *Rice University Studies*, 49:28–46, 1963.

[Mac71] Saunders Mac Lane. *Categories for the Working Mathematician.* Number 5 in Graduate Texts in Mathematics. Springer, 1971.

[McK05] Richard McKinley. Classical categories and deep inference. In *Structures and Deduction 2005 (Satellite Workshop of ICALP'05)*, 2005.

[Moo02] Richard Moot. *Proof Nets for Linguistic Analysis.* PhD thesis, Utrecht Institute of Linguistics OTS, Utrecht University, 2002.

[Par92] Michel Parigot. $\lambda\mu$-calculus: An algorithmic interpretation of classical natural deduction. In *LPAR 1992*, volume 624 of *LNAI*, pages 190–201. Springer-Verlag, 1992.

[Pra65] Dag Prawitz. *Natural Deduction, A Proof-Theoretical Study.* Almquist and Wiksell, 1965.

[Pui01] Quintijn Puite. *Sequents and Link Graphs.* PhD thesis, University of Utrecht, 2001.

[Ret93] Christian Retoré. *Réseaux et Séquents Ordonnés.* PhD thesis, Université Paris VII, 1993.

[Ret97] Christian Retoré. Pomset logic: A non-commutative extension of classical linear logic. In Ph. de Groote and J. R. Hindley, editors, *Typed Lambda Calculus and Applications, TLCA'97*, volume 1210 of *LNCS*, pages 300–318. Springer, 1997.

[Ret99] Christian Retoré. Handsome proof-nets: R&B-graphs, perfect matchings and series-parallel graphs. Rapport de recherche 3652, INRIA, 1999. Appeared as [Ret03].

[Ret03] Christian Retoré. Handsome proof-nets: perfect matchings and cographs. *Theoretical Computer Science*, 294(3):473–488, 2003.

[Rob03] Edmund P. Robinson. Proof nets for classical logic. *Journal of Logic and Computation*, 13:777–797, 2003.

[See89] R.A.G. Seely. Linear logic, *-autonomous categories and cofree coalgebras. *Contemporary Mathematics*, 92, 1989.

[Sel01] Peter Selinger. Control categories and duality: on the categorical semantics of the lambda-mu calculus. *Math. Structures in Comp. Science*, 11:207–260, 2001.

[SG09] Lutz Straßburger and Alessio Guglielmi. A system of interaction and structure IV: The exponentials and decomposition, 2009. To appear in ACM ToCL.

[SR98] Thomas Streicher and Bernhard Reus. Classical logic, continuation semantics and abstract machines. *J. of Functional Programming*, 8(6):543–572, 1998.

[Str03a] Lutz Straßburger. *Linear Logic and Noncommutativity in the Calculus of Structures*. PhD thesis, Technische Universität Dresden, 2003.

[Str03b] Lutz Straßburger. MELL in the Calculus of Structures. *Theoretical Computer Science*, 309(1–3):213–285, 2003.

[Str07] Lutz Straßburger. On the axiomatisation of Boolean categories with and without medial. *Theory and Applications of Categories*, 18(18):536–601, 2007.

[Str09] Lutz Straßburger. From deep inference to proof nets via cut elimination. *Journal of Logic and Computation*, 2009. To appear.

[Thi97] Hayo Thielecke. *Categorical Structure of Continuation Passing Style*. PhD thesis, University of Edinburgh, 1997.

[TS00] Anne Sjerp Troelstra and Helmut Schwichtenberg. *Basic Proof Theory*. Cambridge University Press, second edition, 2000.