An algebraic correctness criterion for intuitionistic proof-nets

Philippe de Groote

Projet Calligramme
INRIA-Lorraine & CRIN-C.N.R.S.
615, rue du Jardin Botanique - B.P. 101
54602 Villers-lès-Nancy Cedex – FRANCE
e-mail: degroote@loria.fr

1 Introduction

We consider intuitionistic fragments of multiplicative linear logic for which we define appropriate notions of proof-nets.

Intuitionistic proof-nets may be easily defined by first introducing intuitionistic (or polarised) proof-structures [1, 5] and then by using any usual correctness criterion [2, 3]. Nevertheless, when using a criterion such as Girard's or Danos-Regnier's, one does not take any advantage of the intuitionistic nature of the polarised proof-nets. Indeed, the aforementioned criteria have been formulated in the classical framework.

In this paper, we formulate a new criterion, which is intrinsically intuitionistic. This criterion consists in decorating the proof-structures with algebraic terms that must obey some constraints reminiscent of phase semantics. These constraints are defined according to the polarities of the proof-structure, which explains the intuitionistic nature of our criterion.

We first state our criterion for intuitionistic implicative multiplicative linear logic (that is the fragment of linear logic whose only connective is "$\multimap$"). Then we explain how to accommodate the multiplicative conjunction "$\otimes$". Finally, we adapt our criterion to the non-commutative case, i.e., the Lambek calculus [8]. In this last case, the criterion is particularly interesting, as we explain at the end of the paper.

2 Implicative linear logic

We first consider the intuitionistic implicative multiplicative fragment of linear logic (which we call implicative linear logic, for short). This fragment, which concerns the only connective "$\multimap$" (linear implication), obeys the following grammar:

$$\mathcal{F} \;::=\; \mathcal{A} \mid \mathcal{F} \multimap \mathcal{F}$$

where $\mathcal{A}$ is the alphabet of atomic formulas.

The deduction rules are specified by the sequent calculus that follows.

Identity rules

$$A \vdash A \quad \text{(ident)} \qquad\qquad \frac{\Gamma \vdash A \quad A, \Delta \vdash B}{\Gamma, \Delta \vdash B} \quad \text{(cut)}$$

Logical rules

$$\frac{\Gamma \vdash A \quad B, \Delta \vdash C}{A \multimap B, \Gamma, \Delta \vdash C} \quad (\multimap \text{left}) \qquad\qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \multimap B} \quad (\multimap \text{right})$$

Structural rule

$$\frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, B, A, \Delta \vdash C} \quad \text{(Exchange)}$$

3 Intuitionistic proof-structures

In order to define a notion of proof-structure for implicative linear logic, we first introduce the notion of polarised multiplicative formula. Let $\mathcal{A}^+$ and $\mathcal{A}^-$ stand respectively for $\mathcal{A} \times \{+\}$ and $\mathcal{A} \times \{-\}$. For any $a \in \mathcal{A}$, we write a^+ (respectively, a^-) for $\langle a, + \rangle$ (respectively, $\langle a, - \rangle$). Polarised formulas ($\mathcal{PN}$) are defined as follows:

$$\begin{array}{rcl} \mathcal{PN} & ::= & \mathcal{P} \mid \mathcal{N} \\ \mathcal{P} & ::= & \mathcal{A}^+ \mid \mathcal{N} \parr \mathcal{P} \\ \mathcal{N} & ::= & \mathcal{A}^- \mid \mathcal{P} \otimes \mathcal{N} \end{array}$$

where $\mathcal{P}$ and $\mathcal{N}$ are respectively called *positive* and *negative* formulas.

In fact, by interpreting a^- as a^- (and a^+ as a itself), the polarised formulas form a proper subset of the formulas of classical multiplicative linear logic, and the notion of *positive* and *negative* polarities correspond to Danos' notion of *output* and *input* formulas [1]. Hence, by translating the formulas of implicative linear logic into polarised formulas, we will get a notion of proof-structure adapted to implicative linear logic.

Consider the following positive and negative translations:

$$\begin{array}{lcll} (a)^+ & = & a^+ & \text{(when } a \text{ is atomic)} \\ (A \multimap B)^+ & = & A^- \parr B^+ & \\ & & & \\ (a)^- & = & a^- & \text{(when } a \text{ is atomic)} \\ (A \multimap B)^- & = & A^+ \otimes B^- & \end{array}$$

These translations allow each intuitionistic sequent "$\Gamma \vdash A$" to be transformed into the sequence of polarised formulas "$(\Gamma)^-, (A)^+$". Then, by combining Girard's notion of link with the above translations, one obtains the polarised links given in Figure 1, where negative and positive polarities are emphasised by black and white circles, respectively.

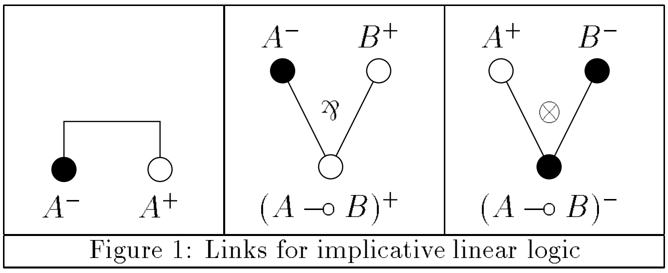

Figure 1: Links for implicative linear logic

The above links are respectively called *axiom-link*, *heterogeneous par-link* and *heterogeneous tensor-link*. The formulas A^- and A^+ are defined to be the conclusions of the axiom-link; the formula $(A \multimap B)^+$ is defined to be the conclusion of the par-link while the formulas A^- and B^+ are defined to be its premises; one defines the conclusion and the premises of the tensor-link similarly.

Finally, an *intuitionistic proof-structure* is defined to be a set of (occurrences of) polarised formulas connected by polarised links, such that:

1. every (occurrence of a) formula is a conclusion of exactly one link and is a premise of at most one link;
2. the resulting graph is connected;
3. the resulting graph as exactly one positive conclusion (i.e., exactly one occurrence of a positive formula that is not the premise of any link).

Remark that condition 3, in the above definition, corresponds to the fact that the succedent of any positive intuitionistic sequent is made of exactly one formula. Proof-structures corresponding to graphs whose vertices are (occurrences of) formulas, we will freely use the terminology of graph theory in the sequel. In particular, we will write $P = \langle V, E \rangle$ for a proof-structure P whose set of vertices is V, and set of edges is E.

Given an intuitionistic proof-structure, we define its *principal inputs* to be its negative conclusions (i.e., the negative vertices that are not the premises of any link) together with those vertices that appear as the negative premises of its heterogeneous par-links. This notion of principal input correspond to the notion of (free or bound) variable in the λ-calculus.

4 An algebraic correctness criterion

Let $\mathbf{M} = \langle M, \cdot, 1 \rangle$ be some freely generated commutative monoid *with sufficiently many generators* (in a technical sense that will be made precise in the sequel).

We define a proof-net to be an intuitionistic proof-structure $\langle V, E \rangle$ together with an application $\rho : V \to M$ such that:

1. the values assigned by ρ to the principal inputs are pairwise coprime (i.e., do not have any common factor);
2. the values assigned by ρ obey the constraints given in Figure 2, i.e.:
   (a) the values assigned to the two conclusions of an axiom-link must be equal,

(b) the value assigned to the positive premise of a par-link must be equal to the product of the value assigned to its negative premise with the value assigned to its conclusion

(c) the value assigned to the negative premise of a tensor-link must be equal to the product of the value assigned to its positive premise with the value assigned to its conclusion;

3. the value assigned to the positive conclusion of the proof-structure is equal to the product of the values assigned to its negative conclusions.

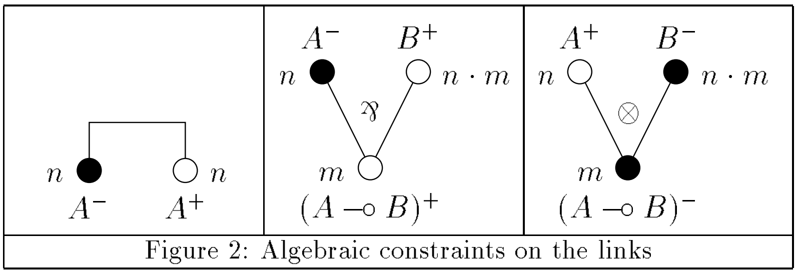

Figure 2: Algebraic constraints on the links

Condition 1, in the above definition of a proof-net, cannot be satisfied if the considered monoid does not have, at least, as many generators as there are principal inputs in the proof-structure. This explains what we meant by *sufficiently many generators*. Practically we will work with the strictly positive integers and the usual multiplication.

As an example, consider the proof-structure given in Figure 3:

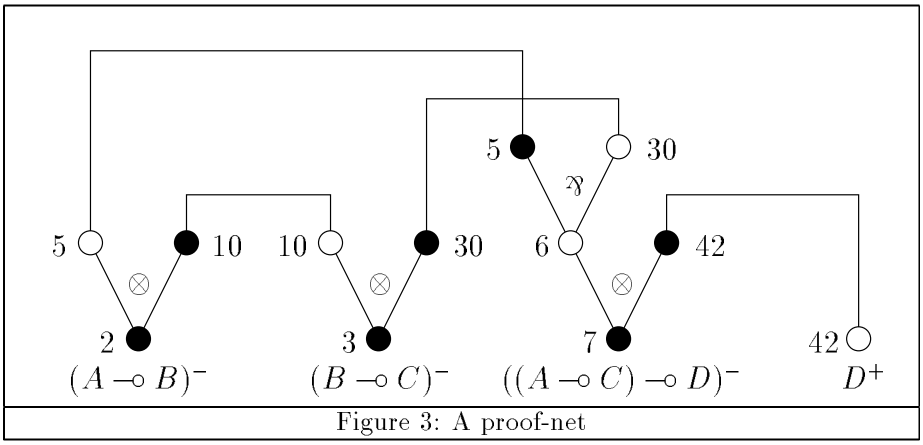

Figure 3: A proof-net

This proof-structure is a proof-net: the values assigned to the principal inputs $(2, 3, 5, 7)$ are pairwise coprime; the algebraic constraints of Figure 2 are satisfied for each link; it is the case that $2 \cdot 3 \cdot 7 = 42$.

In order to show that our definition of an intuitionistic proof-net makes sense, we must prove that:

1. any formal derivation of a sequent $\Gamma \vdash A$ may be transformed into a proof-net whose conclusions are $(\Gamma)^-, (A)^+$;

2. any proof-net whose conclusions are $(\Gamma)^-, (A)^+$ may be *sequentialised* into a formal derivation of the sequent $\Gamma \vdash A$.

Establishing Property 1 consists of a routine induction whose details are left to the reader. Property 2, which amounts to Girard's sequentialisation theorem, will be proven in Section 6.

5 A dynamic view of the criterion

Given some proof-structure how can we check whether it is (or is not) a proof-net? In other words, how can we prove that there exist, for that proof-structure, a valuation ρ satisfying the constraints in which our criterion consists?

Consider again Figure 3 and try to figure out how the given valuation could have been found. Here is a possible solution:

- assign pairwise coprime numbers $(2, 3, 5, 7)$ to the principal inputs of the proof-structure;
- propagate 5 along the axiom link;
- knowing the values assigned to the positive premise (5) and to the conclusion (2) of the left-most tensor-link, assign $10 = 5 \cdot 2$ to its negative premise;
- by steps similar to the previous ones, assign $30 = 10 \cdot 3$ to the negative premise of the second tensor-link, and propagate this value along the axiom;
- check that 30 is divisible by 5 and, consequently, assign 6 to the conclusion of the par-link;
- this allows the value assigned to the premise of the last tensor-link to be computed as $42 = 6 \cdot 7$;
- propagate 42 along the axiom-link and check that $42 = 2 \cdot 3 \cdot 7$.

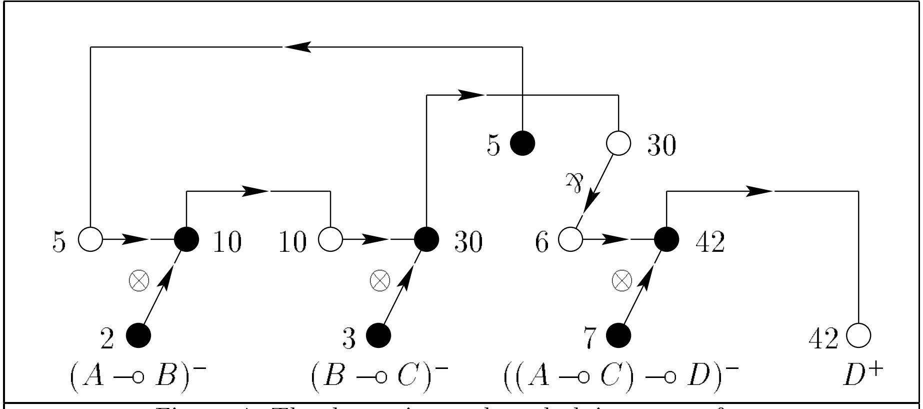

Figure 4: The dynamic graph underlying a proof-net

It can be proven that the above procedure obeys a general algorithm. Any proof-net may be assigned a valuation ρ by propagating the values assigned to its principal inputs. This propagation follows the paths of a directed graph that we call the *dynamic graph underlying the proof-net.* Figure 4 exemplifies this concept.

The notion of dynamic graph may be easily defined by introducing a notion of switch:

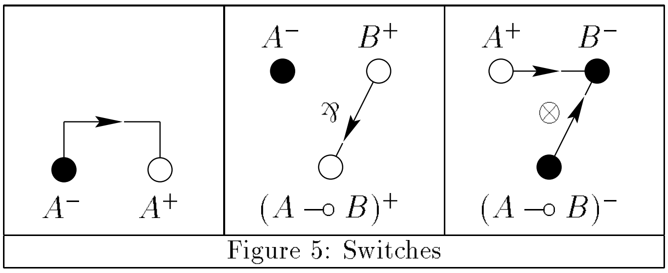

Figure 5: Switches

The dynamic graph underlying a proof-net (or a proof-structure) is defined to be the directed graph obtained by replacing each link of the proof-net by the corresponding switch.

Our dynamic graphs correspond (up to their orientation) to the paths of Lamarche in [5], which he derives from his game semantics [6].

Important properties of the dynamic graphs are given by the following lemmas.

Lemma 5.1 *Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a proof-net, and let $\langle A_1, \ldots A_n\rangle \in V^n$ be a path in the dynamic graph underlying P such that:*

1. *A_1 is a principal input of P;*
2. *in the case that A_1 is the input premise of a heterogeneous par-link, the path does not go through the corresponding output premise.*

Then, $\rho(A_1)$ divides $\rho(A_i)$ for any $i \leq n$.

Proof (sketch). A straightforward induction on the length of the path. □

Lemma 5.2 *The dynamic graph underlying a proof-net is acyclic.*

Proof (sketch). By induction on the number of links. The cases of a single axiom and of a conclusive par are immediate. For the case of a conclusive tensor, one uses Lemma 5.1 to derive a contradiction. □

The acyclicity of the dynamic graphs allows the following property to be established.

Lemma 5.3 *Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a proof-net, and let $A, B \in V$ be such that $\rho(A)$ and $\rho(B)$ are not coprime. Then, there exists a path connecting A and B in the dynamic graph underlying P.*

Proof (sketch). Because $\rho(A)$ and $\rho(B)$ are not coprime, there exist a principal input I such that $\rho(I)$ divides both $\rho(A)$ and $\rho(B)$. It is easy to prove that there exist two path connecting I to $\rho(A)$ and $\rho(B)$ respectively. Moreover one of these paths must be a sub-path of the other. □

Using the two lemmas above, we may prove that the checking algorithm sketched at the beginning of this section is general. Another consequence of Lemma 5.3 is the following.

Lemma 5.4 *The premises of any heterogeneous par-link occurring in a proof-net are connected by a path of the underlying dynamic graphs. This path goes from the negative premise to the positive one.* □

This last lemma will be useful when establishing the sequentialisation property.

6 Sequentialisation

Our sequentialisation proof follows the method of the *splitting tensor* [3, 4].

Given a proof-net, we define a *splitting tensor* to be a tensor-link such that:

1. its conclusion is not a premise of any other link (in other words, its conclusion is one of the conclusions of the proof-net);
2. the value assigned to its positive premise is equal to the product of the values assigned to some of the negative conclusions of the proof-net

The next lemma justifies the above definition.

Lemma 6.1 *Let P be a proof-net that contains a splitting tensor. Then, removing this tensor-link splits P into two disconnected proof-nets.*

Proof (sketch). It is immediate that the splitting tensor splits the graph underlying P into two disconnected subgraphs G_1 and G_2. Therefore, if the splitting tensor does not split the proof-net, there must exist a par-link one premise of which belongs to G_1 and the other premise of which belongs to G_2. But then, by Lemma 5.4, there would exist a path going from one of the premises of this par to the other one. Because G_1 and G_2 are connected only by the switch corresponding to the splitting tensor, this path would go through this switch. But this, by Lemma 5.1, conflicts with Condition 2 in the definition of a splitting tensor. □

The key lemma of the sequentialisation proof is the following.

Lemma 6.2 *Let P be a proof-net whose no conclusion is the conclusion of a par-link. If P contains at least one tensor-link then it contains a splitting tensor.*

Proof (sketch). Since P does not contain any conclusive par, its output conclusion must be the output conclusion of an axiom link. Consider the input conclusion (say A) of this axiom link. This input conclusion A must be the premise of some link (say l) otherwise P would only consists of one axiom link, which would contradict the fact that it contains at least one tensor-link. Because of Lemma 5.4, l cannot be a par-link, therefore, it is a tensor-link. Consider the conclusion of this tensor-link (which is an input conclusion) and iterate the same kind of argument. One eventually finds a conclusive tensor-link. It is easy to show that this tensor-link must be a splitting tensor. □

Proposition 6.3 *Any proof-net is sequentialisable.* □

7 Adding multiplicative conjunction

Intuitionistic multiplicative linear logic is obtained from implicative linear logic by adding the following formation rule:

$$\mathcal{F} \ ::= \ \mathcal{F} \otimes \mathcal{F},$$

together with the two inference rules that follows:

$$\frac{A, B, \Gamma \vdash C}{A \otimes B, \Gamma \vdash C}\ (\otimes \text{ left}) \qquad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B}\ (\otimes \text{ right})$$

Our correctness criterion may be easily adapted to intuitionistic multiplicative linear logic by enriching the free commutative monoid $\mathbf{M}$ with two operations, ${}^{\frac{1}{2}}(\cdot)$ and $(\cdot)^{\frac{1}{2}}$, that obey the following law:

$${}^{\frac{1}{2}}(n) \cdot (n)^{\frac{1}{2}} = n$$

Then, the notion of polarised formula of Section 3 is extended by the following rules:

$$\begin{array}{rcl} \mathcal{N} & ::= & \mathcal{N} \parr \mathcal{N} \\ \mathcal{P} & ::= & \mathcal{P} \otimes \mathcal{P}, \end{array}$$

which allows one to add the following clauses to the positive and negative translations of Section 3:

$$\begin{array}{rcl} (A \otimes B)^- & = & A^- \parr B^- \\ (A \otimes B)^+ & = & A^+ \otimes B^+. \end{array}$$

This gives rise to two additional kinds of links, which are respectively called *homogeneous par-link* and *homogeneous tensor-link*. These links together with the corresponding algebraic constraints and switches are given by Figure 6.

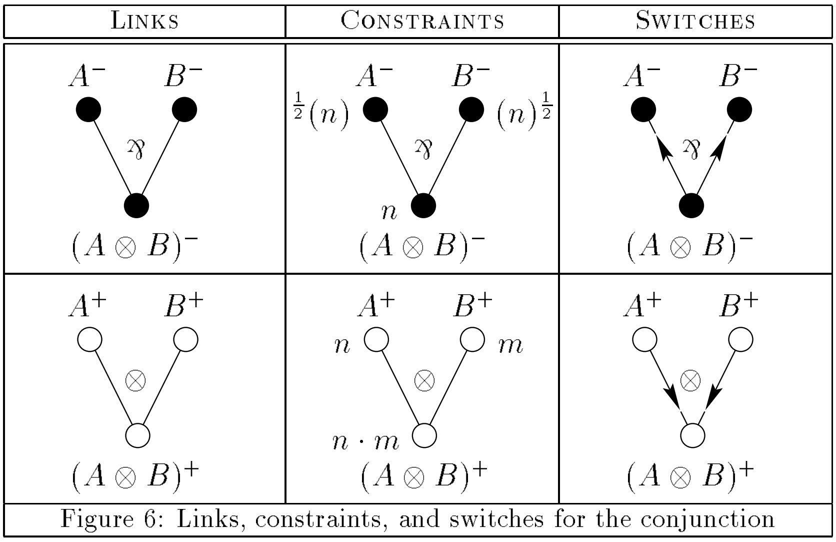

Figure 6: Links, constraints, and switches for the conjunction

The idea behind the adaptation of our criterion to the case of the multiplicative conjunction is straightforward. It is to be noted, however, that to adapt our sequentialisation proof to this new setting requires some work.

8 The non-commutative case: the Lambek calculus

By rejecting the exchange rule, which is is the only structural rule of intuitionistic multiplicative logic, one obtains a non-commutative logic known as the Lambek calculus [8].

The formulas of the Lambek calculus are built according to the following grammar:

$$\mathcal{F} \ ::= \ \mathcal{A} \ | \ \mathcal{F} \bullet \mathcal{F} \ | \ \mathcal{F} \setminus \mathcal{F} \ | \ \mathcal{F} / \mathcal{F}$$

where formulas of the form $A \bullet B$ correspond to conjunctions (or products), formulas of the form $A \setminus B$ correspond to direct implications (i.e., A *implies* B), and formulas of the form A/B to retro-implications (i.e., A *is implied by* B).

The deduction relation of the calculus is defined by means of the following system:

Identity rules

$$A \vdash A \quad \text{(ident)} \qquad\qquad \frac{\Gamma \vdash A \quad \Delta_1, A, \Delta_2 \vdash B}{\Delta_1, \Gamma, \Delta_2 \vdash B} \quad \text{(cut)}$$

Logical rules

$$\frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, A \bullet B, \Delta \vdash C} \quad (\bullet\ \text{left}) \qquad\qquad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \bullet B} \quad (\bullet\ \text{right})$$

$$\frac{\Gamma \vdash A \quad \Delta_1, B, \Delta_2 \vdash C}{\Delta_1, \Gamma, A \setminus B, \Delta_2 \vdash C} \quad (\setminus\ \text{left}) \qquad\qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \setminus B} \quad (\setminus\ \text{right})$$

$$\frac{\Gamma \vdash A \quad \Delta_1, B, \Delta_2 \vdash C}{\Delta_1, B/A, \Gamma, \Delta_2 \vdash C} \quad (/\ \text{left}) \qquad\qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash B/A} \quad (/\ \text{right})$$

In order to adapt our criterion to the Lambek calculus, it suffices to work in a freely generated monoid Σ^* (enriched with the left and right square roots, when the product is present) *that is not commutative*. Then, because the calculus is not commutative, one must carefully distinguish between the direct and the retro implication, between the left and the right premises of the corresponding links, and between left and right cancellation in the monoid.

The translation of the Lambek formulas into polarised formulas is the following:

$$\begin{array}{llll}
(a)^- & = a^- & (a)^+ & = a^+ \\
(A \setminus B)^- & = A^+ \otimes B^- & (A \setminus B)^+ & = B^+ \parr A^- \\
(A/B)^- & = A^- \otimes B^+ & (A/B)^+ & = B^- \parr A^+ \\
(A \bullet B)^- & = A^- \parr B^- & (A \bullet B)^+ & = B^+ \otimes A^+
\end{array}$$

This gives rise to the links, the constraints, and the switches of Figure 7 and 8.

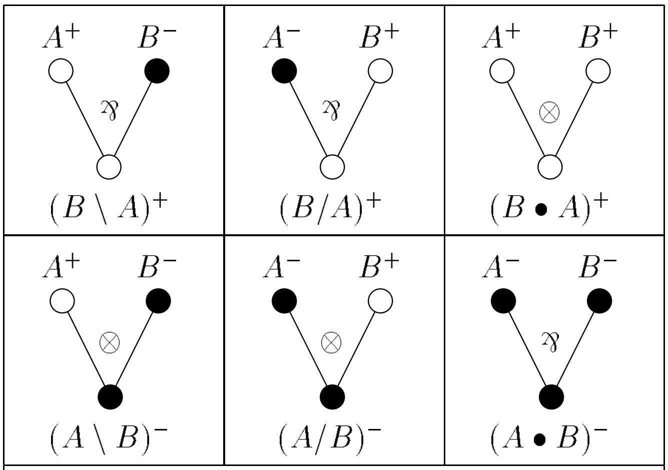

Figure 7: Links for the Lambek calculus

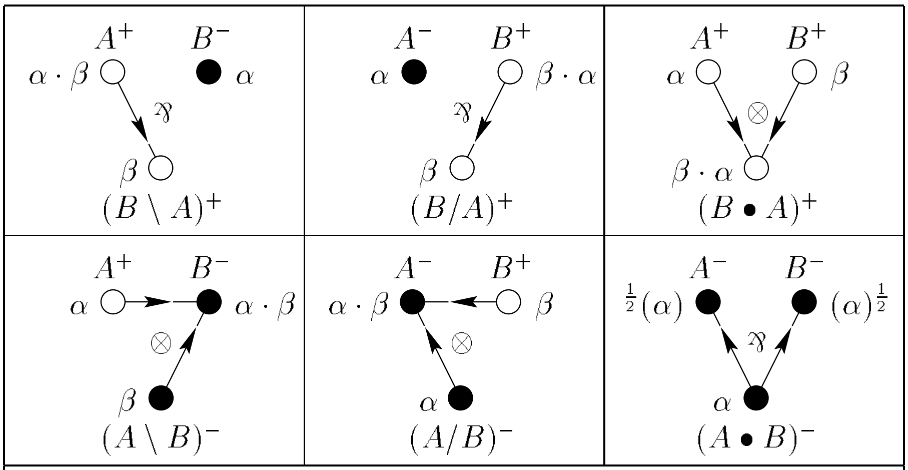

Figure 8: Constraints and switches for the Lambek calculus

9 Concluding remarks

As we said in the introduction, our criterion is intrinsically intuitionistic, which is also the case of Lamarche's [5]. Similarly, we could say that the non commutative version of our criterion is intrinsic to the Lambek calculus, which solves an open question raised by Retoré [7]. Indeed, in the literature, proof-nets for the Lambek calculus are defined in terms of conditions that ensure commutative correctness, together with an additional condition that ensures non-commutativity. The latter is, most often, a planarity condition [7, 9]. In contrast, when using our criterion, commutative correctness and non-commutativity are not checked independently.

In [9, Chap. III, §6, pp. 38–40], Roorda defines a way of decorating proof-nets that is almost identical to ours. He then observes that the existence of such a decoration is necessary, and raises the question whether it is sufficient (in fact, he conjectures it is not). Consequently, our paper solves Roorda's open question (in the unexpected sense).

Another difference between Roorda's work and ours lies in the dynamic interpretation of our criterion. Indeed, Roorda's decorating algorithm involves associative (commutative) unification. In this paper, we have avoided this unnecessary complexity by introducing the notion of *underlying dynamic graph* and the two *square root* operators.

References

[1] V. Danos. *Une application de la logique linéaire à l'étude des processus de normalisation et principalement du lambda calcul.* Thèse de doctorat, Université de Paris VII, 1990.

[2] V. Danos and L. Regnier. The structure of multiplicatives. *Archive for Mathematical Logic*, 28:181–203, 1989.

[3] J.-Y. Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.

[4] J.-Y. Girard. Quantifiers in linear logic II. Technical Report 19, Equipe de Logique Mathématique, Université de Paris VII, 1991.

[5] F. Lamarche. Proof nets for intuitionistic linear logic 1: Essential nets. Technical report, Imperial College, April 1994.

[6] F. Lamarche. Games semantics for full propositional linear logic. In *Ninth Annual IEEE Symposium on Logic in Computer Science.* IEEE Press, 1995.

[7] F. Lamarche and C. Retoré. Proof nets for the lambek calculus. In M. Abrusci, C. Casadio, and G. Sandri, editors, *Third Roma Workshop: Proofs and Linguistic Categories*, Rapporto di Ricerca del Dipartimento de Filosofia. Università di Bologna, 1996.

[8] J. Lambek. The mathematics of sentence structure. *Amer. Math. Monthly*, 65:154–170, 1958.

[9] D. Roorda. *Resource Logics: proof-theoretical investigations.* PhD thesis, University of Amsterdam, 1991.