An algebraic correctness criterion for intuitionistic multiplicative proof-nets

Philippe de Groote

UMR n^o 7503 LORIA - INRIA
Campus Scientifique - BP 239
F-54506 Vandœuvre lès Nancy Cedex - France

degroote@loria.fr

Abstract. We consider intuitionistic fragments of multiplicative linear logic for which we define appropriate notions of proof-nets. These are based on a correctness criterion that consists of decorating the nodes of a proof-structure with monoidal terms that must obey constraints reminiscent of phase semantics.

1 Introduction

Intuitionistic proof-nets may be easily defined by first introducing intuitionistic (or polarized) proof-structures [1, 6] and then by using any of the usual correctness criterion [2, 4]. 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 polarized 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 of 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.

The paper is organized as follows:

In Section 2 we provide a short review of intuitionistic multiplicative linear logic.

In Section 3 we define a notion of intuitionistic proof-structure by introducing notions of polarized formula and polarized links.

In Section 4, we restrict our attention to the purely implicative fragment of multiplicative linear logic. We first show how to decorate a sequential derivation à la Gentzen with elements of a commutative monoid. From this we derive our correctness criterion. We then prove that any proof-structure that obeys our criterion may be sequentialised into a sequent calculus derivation. To this end, we introduce the central notion of dynamic graph underlying a proof-net.

In Section 5, we show how to extend our criterion in order to allow for the multiplicative conjunction. The idea is to enrich the commutative monoid of Section 4 with two operations: a left and a right square root.

Section 6 explains how to accommodate our criterion to the Lambek calculus (i.e., to the non-commutative case) by considering non-commutative monoids.

We conclude in Section 7.

A preliminary short version of this paper appeared as [3].

2 Intuitionistic multiplicative linear logic

The intuitionistic fragment of multiplicative linear logic (IMLL) concerns only the connectives "$\multimap$" (linear implication) and "$\otimes$" (multiplicative conjunction). Its formulas obey the following grammar:

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

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

The deduction relation of IMLL is specified by means of 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

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

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

Structural rule

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

By restricting the above system to the only connective "$\multimap$", we obtain the implicative fragment of intuitionistic multiplicative linear logic. We will refer to this very simple fragment as IILL.

3 Intuitionistic proof-structure

Multiplicative proof-structures and proof-nets have been introduced by Girard [4] as the appropriate syntax for proofs in classical multiplicative linear logic (which is the fragment concerned with the two connectives $\otimes$ and $\parr$, respectively, the multiplicative conjunction and disjunction). One possible way of adapting the notion of proof-structure to the intuitionistic case is to provide a translation of intuitionistic multiplicative linear logic into classical multiplicative linear logic. To this end, one introduces a notion of polarized 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, $\langle a, - \rangle$).

Definition 3.1 (Polarized formulas) *Polarized formulas ($\mathcal{PN}$) are defined as follows:*

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

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

In fact, by interpreting a^- as $a^\perp$ (i.e. *"not a"*) and a^+ as a itself, the polarized 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 intuitionistic multiplicative linear logic into polarized formulas, we obtain a notion of proof-structure adapted to IMLL.

Consider the following positive and negative translations:

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

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

These translations, which are nothing but direct applications of De Morgan's laws (including the definition of implication in terms of disjunction and negation: $A \multimap B = A^\perp \parr B$), allow each intuitionistic sequent "$\Gamma \vdash A$" to be transformed into a classical sequent of polarized formulas "$\vdash (\Gamma)^-, (A)^+$". It is then straightforward to prove that $\Gamma \vdash A$ is intuitionistically derivable if and only if $\vdash (\Gamma)^-, (A)^+$ is classically derivable.

Further, by combining Girard's notion of link with the above translations, one obtains the polarized links given in Figure 1, where negative and positive polarities are emphasised by black and white circles, respectively.

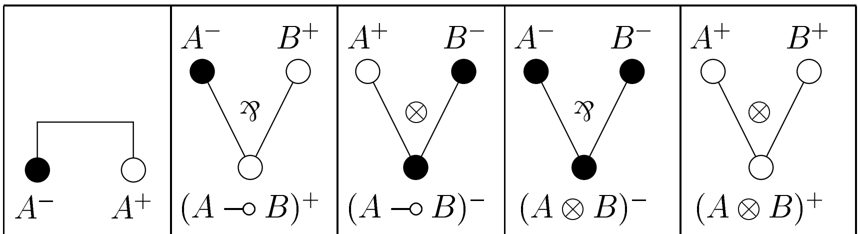

Figure 1: Links for intuitionistic multiplicative linear logic

The above links are respectively called *axiom-link*, *heterogeneous par-link*, *homogeneous par-link*, *heterogeneous tensor-link* and *homogeneous 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 heterogeneous par-link while the formulas A^- and B^+ are defined to be its premises; one defines the conclusion and the premises of the other links similarly.

The notion of polarized links allows the notion of an intuitionistic proof-structure to be defined.

Definition 3.2 (Intuitionistic proof-structure) *An intuitionistic proof-structure is defined to be a set of (occurrences of) polarized formulas connected by polarized 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 has 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.

Consider a given proof-structure $P = \langle V, E \rangle$. As implicit in Definition 3.2, the formulas occurring in P that are not the premise of any link are called the *conclusions* of the proof-structure. A par-link or tensor-link whose conclusion is a conclusion of P is called a *conclusive link* (of P). Let L be such a conclusive link. To remove L from P consists of removing the conclusion of L from V, and the two edges linking this conclusion to the premises of L from E. It is immediate that the graph obtained by removing L from P still satisfies Condition 1 of Definition 3.2. Such graphs, which correspond to the structures one obtains by dropping Conditions 2 and 3 in Definition 3.2, will be called *pseudo proof-structure.*

The negative (respectively, positive) formulas occurring as vertices of a proof-structure will be called the *input nodes* (respectively, *output nodes*) of the proof-structure. Given an intuitionistic proof-structure, we define its *principal inputs* to be its negative conclusions 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. When needed, we will distinguish between the *outer* and the *inner* principal inputs. The outer principal inputs of a proof-structure are defined to be its negative conclusions; they correspond to the notion of free-variable. The inner principal inputs of a proof-structure are defined to be the negative premises of its heterogeneous par-links; they correspond to the notion of bound-variable.

4 Intuitionistic proof-nets: the implicative case

4.1 Decorating formulas with algebraic terms

Our correctness criterion consists of decorating the nodes of a proof-structure with algebraic terms, in such a way that this decoration ensures that the proof-structure is actually a proof-net. In order to introduce the idea that is behind this principle, we first make a pedagogical *détour* through the sequent calculus.

Girard's phase semantics interprets the formulas of linear logic as subsets of a commutative monoid. Consequently, one may see linear logic as a typing system for the terms of such a monoid. At the syntactic level, this point of view is reflected by the following system (which concerns IILL only):

$$\alpha : A \vdash \alpha : A$$

$$\frac{\Gamma \vdash \gamma : A \quad \alpha \cdot \gamma : B, \Delta \vdash \alpha \cdot \gamma \cdot \delta : C}{\alpha : A \multimap B, \Gamma, \Delta \vdash \alpha \cdot \gamma \cdot \delta : C} \qquad \frac{\alpha : A, \Gamma \vdash \alpha \cdot \beta : B}{\Gamma \vdash \beta : A \multimap B}$$

where Roman upper case letters stand for formulas, and Greek lower case letters for monoidal terms.

It is straightforward to prove that any ILLL derivable sequent may be decorated with algebraic terms according to the above system, in such a way that the product of the terms assigned to the formulas of the antecedent is equal to the term assigned to the conclusion. As an example, consider the following derivation.

$$\dfrac{\dfrac{\dfrac{c : A \vdash c : A \quad c \cdot a : B \vdash c \cdot a : B}{c : A, a : A \multimap B \vdash c \cdot a : B}}{a : A \multimap B \vdash a : A \multimap B} \qquad a \cdot b : C \vdash a \cdot b : C}{a : A \multimap B, b : (A \multimap B) \multimap C \vdash a \cdot b : C}$$

This derivation gives rise to the following decorated proof-structure.

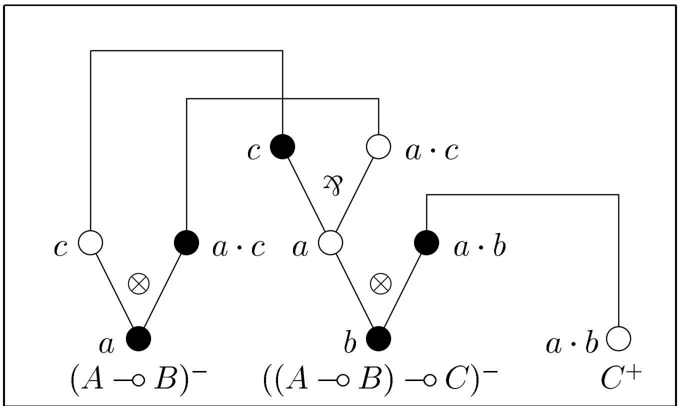

Figure 2: A decorated proof-structure

The above example suggests the algebraic decorations of the links given by Figure 3. These decorations, which will act as algebraic constraints on the links, are the keystone of our definition of an intuitionistic proof-net.

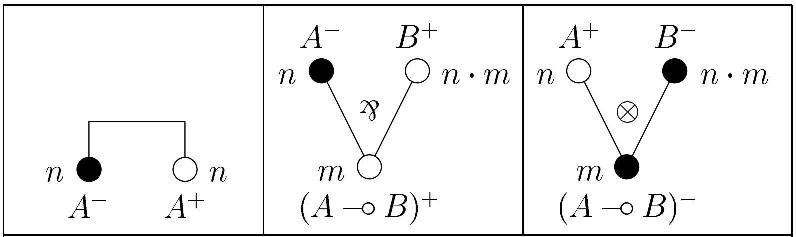

Figure 3: Algebraic constraints on the links

We are now in a position to introduce our criterion.

4.2 An algebraic 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 below). We define an implicative proof-net as follows.

Definition 4.1 (Implicative intuitionistic proof-net) *An implicative intuitionistic proof-net is an implicative intuitionistic proof-structure $\langle V, E \rangle$ together with a mapping $\rho : V \to M$ 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 3, 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.*

The values assigned to the principal inputs of a proof-net are called its *principal values.* As we distinguish between outer and inner principal inputs, we distinguish between *outer* and *inner principal values.* We also define an *outer value* to be an algebraic term that can be factored into outer principal values. These different concepts will be illustrated by an example.

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 may work with the strictly positive integers and the usual multiplication. As an illustration, consider the proof-structure given in Figure 4:

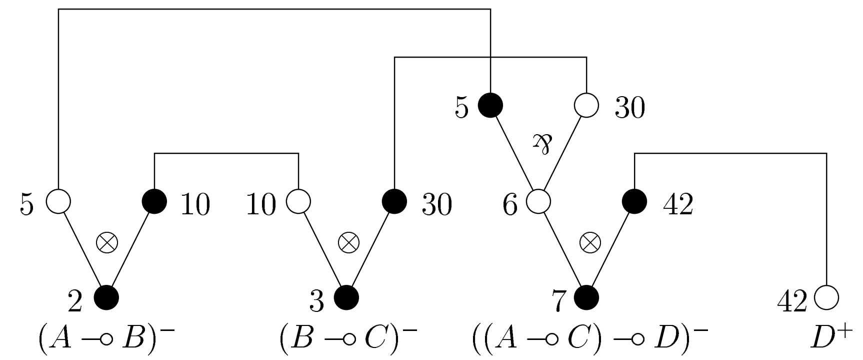

Figure 4: A proof-net

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

In the above example, the outer principal values of the proof net are 2, 3 and 7. There is only one inner principal value, namely, 5. Finally, 2, 3, 6, 7 and 42 are outer values, while 5, 10 and 30 are not.

In order to show that our definition of an implicative 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 4.4.

We end this section by introducing the notion of pseudo proof-net. This notion will only be used in the course of some proofs.

Definition 4.2 (pseudo proof-net) *An implicative intuitionistic pseudo proof-net is an implicative intuitionistic pseudo proof-structure $\langle V, E \rangle$ together with an application $\rho : V \to M$ such that:*

1. *the value assigned by ρ to the inner principal inputs are pairwise coprime;*
2. *the value assigned by ρ to the outer principal inputs $A_1, A_2, \ldots$ may be factored as $\rho(A_i) = \alpha_i \cdot \beta_i$ in such a way that*
   (a) *each α_i is coprime with all the values assigned to the inner principal inputs;*
   (b) *the α_i's are pairwise coprime;*
3. *the values assigned by ρ obey the constraints given in Figure 3.*

The factors α_i appearing in the above definition will be called the outer principal values of the pseudo proof-net.

Clearly, any proof-net is a pseudo proof-net. Moreover, any pseudo proof-net satisfies the following property whose proof is left to the reader.

Lemma 4.3 *Let P be a pseudo proof-net and let L be some conclusive link of P. Then the structure obtained by removing L from P is a pseudo proof-net.* □

This lemma allow us to establish a property of a proof-net by seeing it as a pseudo proof-net and then proceeding by induction on the number of links.

4.3 A dynamic view of the criterion

In order to establish that any proof-net may be turned into a sequential derivation, we need to introduce the central notion of the *dynamic graph underlying a proof-net* (or a proof structure). To this end, we first answer the following natural question: "given some proof-structure how can we check whether it is or not a proof-net?" In other words, how can we prove that there exists, for that proof-structure, a valuation ρ satisfying the constraints of Definition 4.1?

Consider again Figure 4 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 $42 = 2 \cdot 3 \cdot 7$.

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 5 exemplifies this concept.

The notion of dynamic graph may be easily defined by introducing the notion of switch given by Figure 6. These switches are clearly in one-one-correspondence with the axiom-link, the heterogeneous par-link, and the heterogeneous tensor-link, respectively. The notion of dynamic graph is then defined as follows.

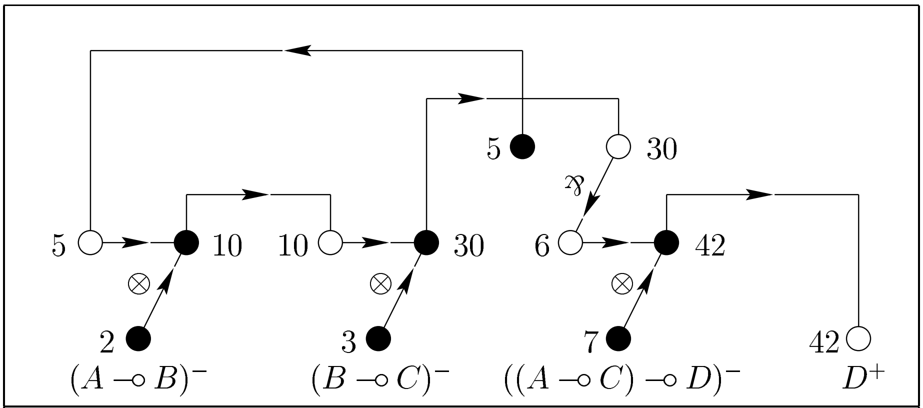

Figure 5: The dynamic graph underlying a proof-net

Definition 4.4 (Dynamic graph underlying a proof-net) *The dynamic graph underlying a proof-net (or proof-structure) is defined to be the directed graph obtained by replacing each link of the proof-net (or proof-structure) by the corresponding switch.*

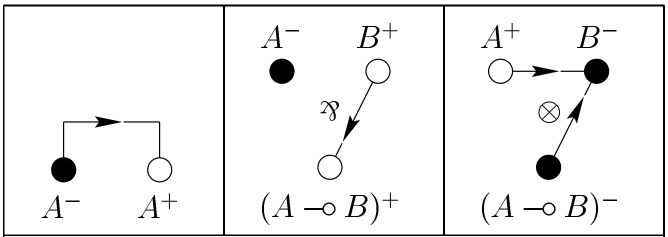

Figure 6: Switches

Given a proof-structure, a dynamic path is defined to be a sequence of edges that corresponds to an elementary path in the dynamic graph underlying the proof-structure.

Our dynamic graphs correspond (up to their orientation) to the paths of Lamarche [6], which he derives from his game semantics [7].

The dynamic graph underlying a proof-structure induces a preorder relation on the nodes of this proof-structure. In the case of an implicational proof-net, we will prove that this preorder is actually an order (with a top element). More precisely, in the implicational case, the dynamic graph underlying a proof-net is a tree. The remainder of this section is devoted to the proof of this property (together with the proofs of some related lemmas and corollaries).

Lemma 4.5 *Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a (pseudo) proof-net, let α be a principal value of P, and let $\langle A_1, \ldots A_n\rangle \in V^n$ be a dynamic path of P, such that:*

1. *$\rho(A_1) = \alpha^q \cdot \beta$ for some natural number q and some algebraic term β.*
2. *in case α is the inner principal value assigned to the negative premise of some heterogeneous par-link, the conclusion of this par-link does not belong to the dynamic path.*

Then, α^q divides $\rho(A_i)$ for any $1 \leq i \leq n$.

Proof. A straightforward induction on the length of the path. Note that the co-primality conditions of Definitions 4.1 and 4.2 are needed to make the induction work when the path goes through a switch corresponding to a heterogeneous par-link. □

Lemma 4.6 *The dynamic graph underlying a proof-net is acyclic.*

Proof. Let P be any pseudo proof-net. We prove, by induction on the number of links in P, that the dynamic graph underlying P is acyclic.

If P consists only of axiom-links then the dynamic graph is trivially acyclic.

When P contains at least one conclusive par-link, the induction is straightforward.

Consider the case where P contains a conclusive tensor T. By the induction hypothesis, the dynamic graph underlying the pseudo proof-net obtained by removing T from P is acyclic. Therefore, if the dynamic graph underlying P is not acyclic, there must exist a dynamic path from the negative premise of T to the positive one. Let $\alpha \cdot \beta$ be the term assigned to the conclusion of T, α being an outer principal value, and let γ be the term assigned to the positive premise of T. We may factor γ as $\alpha^q \cdot \gamma'$ in such a way that α does not divide γ'. Then, the value assigned to the negative premise of T must be $\alpha^{q+1} \cdot \beta \cdot \gamma'$. But, by Lemma 4.5, α^{q+1} should divide $\alpha^q \cdot \gamma'$, which contradicts the fact that α does not divide γ'. □

The preceding lemma establishes that the preorder induced by the dynamic graph underlying a proof-net is actually an order. It remains to prove that the dynamic graph is connected in order to show that it is a tree. This property is obtained as a direct consequence of the next lemma.

Lemma 4.7 *Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a proof-net, let $A \in V$ be a principal input of P, and let $B \in V$ be any node such that $\rho(A)$ divides $\rho(B)$. Then there exists a dynamic path from A to B.*

Proof. A straightforward induction on the well-founded order induced by the dynamic graph underlying P. □

As direct consequences of this lemma, we get the two following properties.

Lemma 4.8 *There exists a dynamic path from any input conclusion of a proof-net to the output conclusion.* □

Lemma 4.9 *In any proof-net, there exists a dynamic path from any input premise of a heterogeneous par-link to the output premise.* □

This last property ensures that the dynamic graph underlying a proof-net is connected.

4.4 Sequentialisation

Our sequentialisation proof follows the method of the *splitting tensor* [4, 5]. We will prove that any proof-net whose conclusive links are tensor-links includes, among these, a splitting tensor, i.e., a conclusive tensor-link whose removal splits the proof-net into two disconnected components. To this end, we first define an abstract notion of splitting tensor.

Definition 4.10 (Splitting tensor) *Given a proof-net, we define a splitting tensor to be a conclusive tensor-link whose positive premise is assigned an outer value.*

We now prove that this abstract notion of a splitting tensor coincides with the intended notion.

Lemma 4.11 *Let P be a proof-net that contains a (splitting) tensor. Then, removing the switch associated to this tensor-link splits the dynamic graph underlying P into two disconnected components.*

Proof. This is immediate since the dynamic graph underlying an implicative proof-net is a tree. □

Lemma 4.12 *Let P be a proof-net that contains a splitting tensor T. Then, removing this tensor-link splits P into two disconnected proof-nets.*

Proof. By Lemma 4.11, the splitting tensor splits the dynamic graph underlying P into two disconnected subgraphs, say G_1 and G_2. Without loss of generality, consider that the output premise of T belongs to G_1 and that its input premise belongs to G_2. Now if the splitting tensor T does not split the proof-net, there must exist a par-link, say L, one premise of which belongs to G_1 and the other premise of which belongs to G_2. But then, by Lemma 4.9, there would exist a dynamic path connecting the input premise of L to its output premise. Since G_1 and G_2 are connected only by the switch corresponding to the splitting tensor T, this path would go through this switch and, therefore, there would exist a path from the input premise of L to the output premise of T. But then, by Lemma 4.5, the output premise of T cannot be assigned an outer value, which conflicts with the definition of a splitting tensor.

Let P_1 and P_2 be the proof-structures corresponding to G_1 and G_2, respectively. It remains to show that these two disconnected proof-structures are actually proof-nets.

Condition 1 of Definition 4.1 is satisfied by P_1 because all its principal inputs are principal inputs of P. To show that Condition 1 is also satisfied by P_2, we must show that the value assigned to the input premise of T, say α, is coprime with all the values assigned to the other principal inputs of P_2. This is indeed the case because $\alpha = a \cdot \beta$, where a is the value assigned to the conclusion of T, and β is the value assigned to the output premise of T. Now, by the definition of a splitting tensor and by Lemma 4.7, β is a product of values assigned to principal inputs of P_1. Therefore α is a product of values that are coprime with all the values assigned to the other principal inputs of P_2.

Condition 2 is clearly satisfied by both components.

By Lemma 4.8, any input conclusion of P is connected to its output conclusion by a dynamic path. Consequently the input conclusions of P may be partitioned into three classes: the ones that are connected to the output of P through the switch associated to T (these input conclusions are the input conclusions of P_1); the input conclusion of T itself; the other input conclusions (which belong to P_2). This observation, together with the fact that P is a proof-net (which therefore satisfies Condition 3 of Definition 4.1), implies that both P_1 and P_2 satisfy Condition 3. □

We now prove that any proof-net without a conclusive par-link contains a splitting tensor or consists of a single axiom link.

Lemma 4.13 *Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a proof-net, and let $A \in V$ be an input node such that:*

1. *A is not a principal input;*
2. *$\rho(A)$ is an outer value.*

Then P contains a splitting tensor.

Proof. By induction on the order induced by the dynamic graph underlying P. Since A is not a principal input, it must be the negative premise of some heterogeneous tensor-link T. If this tensor-link is a conclusive link, we are done because $\rho(A)$ is an outer value, and so must be the value assigned to the positive premise of T. Otherwise, consider the conclusion of T, which is an input node satisfying hypotheses 1 and 2, and apply the induction hypothesis. □

Lemma 4.14 *Let P be a proof-net without conclusive par-link. If P contains at least one tensor-link then it contains a splitting tensor.*

Proof. Since P does not contain a conclusive par-link, 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, otherwise P would only consists of one axiom link, which would contradict the fact that it contains at least one tensor-link. Therefore A satisfies the hypotheses of Lemma 4.13, and consequently P contains a splitting tensor. □

We are now in a position of proving the sequentialisation property.

Proposition 4.15 *Any proof-net P is sequentialisable.*

Proof. We proceed by induction on the number of links in the proof-net. If P consists of one single axiom-link then it is clearly sequentialisable. When P contains at least one conclusive par-link, it is easy to see that the proof-structure obtained by removing this par-link is a proof-net, which is sequentialisable by the induction hypothesis. Finally, if P does not consist of one axiom-link, and does not contain any conclusive par-link, we apply Lemma 4.14. □

5 Intuitionistic proof-nets: the multiplicative case

5.1 Adapting the criterion

In order to adapt our criterion to IMLL, we enrich the free commutative monoid $\mathbf{M}$ with two operations, ${}^{\frac{1}{2}}(\cdot)$ and $(\cdot)^{\frac{1}{2}}$, that obey the following law:

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

In such a free structure, the notions of division, factor, and coprimality remain standard. We say that α divides β (or is a factor of β) if and only if there exists some γ such that $\beta = \gamma \cdot \alpha$. Then, two values are said to be coprime if they do not have any common factor. The values that can be factored into a product of generator are called *proper monoidal values.*

In the preceding section, we used the words *value* and *term* almost as though they were synonymous. Here we will use the word *term* in order to stress a syntactic point of view, and we define a *canonical term* to be a term in normal form according to Equation (sqrt) seen as a rewriting rule (modulo associativity and commutativity). We also define the following relation of *occurrence*: a value α occurs in a value β if and only if the canonical term denoting α is a subterm of the canonical term denoting β (modulo associativity and commutativity).

The above algebraic apparatus allows us to define the following algebraic constraints on the homogeneous links.

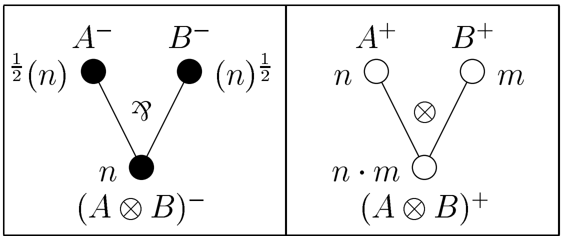

Figure 7: Constraints for the conjunction

Further, in order to adapt the notion of dynamic graph underlying a proof-net, we introduce the following switches.

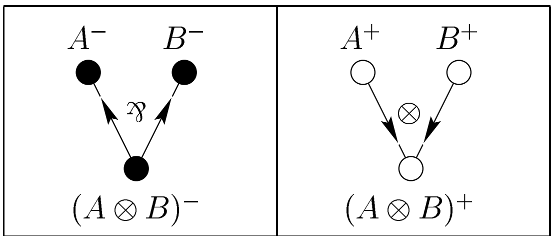

Figure 8: Switches for the conjunction

Then, Definition 4.1 is adapted to the case of *multiplicative intuitionistic proof-nets* as follows.

Definition 5.1 (Multiplicative intuitionistic proof-net) *A multiplicative intuitionistic proof-net is a multiplicative intuitionistic proof-structure $\langle V, E\rangle$ together with a mapping $\rho : V \to M$ such that:*

1. *the dynamic graph underlying $\langle V, E\rangle$ is acyclic;*[1]
2. *the values assigned by ρ to the principal inputs are proper monoidal values;*
3. *the values assigned by ρ to the principal inputs are pairwise coprime;*
4. *the values assigned by ρ obey the constraints given in both Figures 3 and 7;*
5. *the value assigned to the positive conclusion of the proof-structure is equal to the product of the values assigned to its negative conclusions.*

The notion of principal value, of inner or outer principal value, and of outer value are kept unchanged. We define a quasi-outer principal value to be a value denoted by a term in which there is no occurrence of any inner principal value.

Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a (pseudo) proof-net, let L be a conclusive homogeneous par-link of P, and let α be the principal value assigned to the conclusion of L by ρ. To remove L from P consists of:

1. removing L from $\langle V, E\rangle$;
2. selecting two proper monoidal values β and δ that are coprime and pairwise coprime with all the principal values of P;
3. for each node $A \in V$, replacing in $\rho(A)$ each occurrence of $^{\frac{1}{2}}\alpha$ (respectively, $\alpha^{\frac{1}{2}}$) by β (respectively, δ), except if there exists $B \in V$ with a dynamic path from B to A and such that $\rho(B) = \alpha$;
4. replacing, in each value assigned by ρ, the remaining occurrences of α by $\beta \cdot \delta$.

The remainder of this section is devoted to technical lemmas that will be needed in the sequel. We first state the two lemmas corresponding to Lemmas 4.5 and 4.7.

Lemma 5.2 *Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a proof-net, let α be a principal value of P, and let $\langle A_1, \ldots A_n\rangle \in V^n$ be a dynamic path of P, such that:*

1. *α occurs in $\rho(A_1)$.*
2. *in case α is the inner principal value assigned to the negative premise of some heterogeneous par-link, the conclusion of this par-link does not belong to the dynamic path.*

Then, α occurs in $\rho(A_i)$ for any $1 \leq i \leq n$.

Proof. A straightforward induction on the length of the path. □

Lemma 5.3 *Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a proof-net, let $A \in V$ be a principal input of P, and let $B \in V$ be any node such that $\rho(A)$ occurs in $\rho(B)$. Then there exists a dynamic path from A to B.*

Proof. A straightforward induction on the well-founded order induced by the dynamic graph underlying P. □

[1] This condition is actually necessary. The existence of a valuation satisfying the constraints of Figures 3 and 7 no longer implies the acyclicity of the dynamic graph.

This lemma implies that Lemmas 4.8 and 4.9 remain valid for the multiplicative proof-nets.

The next lemma concerns the homogeneous par-links occurring in a proof-net.

Lemma 5.4 *Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a proof-net, let $A \in V$ be the conclusion of some homogeneous par-link of P, and let $B \in V$ be any node such that:*

- *there is no dynamic path from B to A,*
- *$\frac{1}{2}\rho(A)$ (respectively, $\rho(A)^{\frac{1}{2}}$) divides $\rho(B)$.*

Then all the dynamic paths leaving the left (respectively, right) premise of A may be extended into dynamic paths going through B.

Proof. By induction on the well-founded order induced by the dynamic graph underlying P.

If B is the output conclusion of an axiom-link or the output conclusion of a heterogeneous par-link, the induction is straightforward.

If B is the left (respectively, right) premise of a homogeneous par-link L, it must be the case that $\rho(B) = \frac{1}{2}\rho(A)$ (respectively, $\rho(B) = \rho(A)^{\frac{1}{2}}$). Then, if the conclusion of L is A itself, we are done. Otherwise, we apply the induction hypothesis.

If B is the output conclusion of a homogeneous tensor-link T, we have that $\rho(B) = \alpha \cdot \beta$, where α and β are the two values assigned to the two output premises of T. If $\frac{1}{2}\rho(A)$ (respectively, $\rho(A)^{\frac{1}{2}}$) divides either α or β, the induction is straightforward. Otherwise, it must be the case that the canonical terms denoting α and β have the forms $\alpha' \cdot \frac{1}{2}\gamma$ and $\beta' \cdot \gamma^{\frac{1}{2}}$ (with $\frac{1}{2}\rho(A)$ (respectively, $\rho(A)^{\frac{1}{2}}$) occurring in γ), and that the product $\alpha \cdot \beta$ may be rewritten according to equation (sqrt) as follows:

$$\alpha' \cdot \tfrac{1}{2}\gamma \cdot \beta' \cdot \gamma^{\frac{1}{2}} \to \alpha' \cdot \beta' \cdot \gamma \to^{*} \delta \cdot \varepsilon = \rho(B) \qquad (1)$$

where δ is the canonical term denoting $\frac{1}{2}\rho(A)$ (respectively, $\rho(A)^{\frac{1}{2}}$). Hence, there exists a heterogeneous par-link L whose conclusion is assigned the value γ. Then, by induction hypothesis, all the dynamic paths leaving the left premise of L reach one of the premises of T and all the dynamic paths leaving the right premise of L reach the other premise of T. Now, if $\frac{1}{2}\rho(A)$ (respectively, $\rho(A)^{\frac{1}{2}}$) divides γ, we apply again the induction hypothesis and we are done. Otherwise, we use an auxiliary induction on the number of rewriting steps in (1) in order to iterate the same reasoning.

The case where B is the input premise of a heterogeneous tensor-link is similar to the previous one. □

As an immediate consequence of the above lemma, we have the following property: if two homogeneous par-links are assigned the same value then all the paths leaving one of these links must reach the other link. This implies that the structure obtained by removing a conclusive homogeneous par-link from a proof-net is still a proof-net.

5.2 Sequentialisation

In order to adapt the sequentialisation proof of Section 4.4, we first adapt the notion of splitting tensor.

Definition 5.5 (Splitting tensor) *Given a proof-net, we define a splitting tensor to be either a conclusive heterogeneous tensor-link whose positive premise is assigned an outer value, or a conclusive homogeneous tensor-link whose both premises are assigned outer values.*

The remainder of this section follows, step by step, the structure of Section 4.4.

Lemma 5.6 *Let P be a proof-net that contains a splitting tensor T. Then, removing the switch associated to this splitting tensor splits the dynamic graph underlying P into two disconnected components.*

Proof. Suppose it is not the case. Then, there would exist a homogeneous par-link L whose one premise (say, the left one) would be connected to (one of) the output premise(s) of T, and whose other premise would not. Let α be the value assigned to the conclusion of L. Then it is easy to show, using Lemma 5.4, that $\frac{1}{2}\alpha$ would occur in the value assigned to the output premise of T, which contradicts the fact that T is a splitting tensor. □

Lemma 5.7 *Let P be a proof-net that contains a splitting tensor T. Then, removing this tensor-link splits P into two disconnected proof-nets.*

Proof. The proof is similar to the one of Lemma 4.12, using Lemmas 5.6, 5.2, and 5.3, instead of Lemmas 4.11, 4.5, and 4.7. □

Lemma 5.8 *Let $P = \langle\langle V, E\rangle, \rho\rangle$ be a proof-net that does not contain a conclusive par-link, and let $A \in V$ be an input node such that:*

1. *A is not a principal input;*
2. *$\rho(A)$ is a quasi-outer value.*

Then P contains a splitting tensor.

Proof. By induction on the order induced by the dynamic graph underlying P. Since A is not a principal input, it is either one of the negative premises of some homogeneous par-link L, or the negative premise of some heterogeneous tensor-link T.

In the first case, consider the conclusion of L, which must be assigned a quasi-outer value. Since P does not contain any conclusive par-link, this conclusion cannot be a principal input. Therefore, one may apply the induction hypothesis.

In the second case, if T is not a conclusive link, one applies the induction hypothesis on the conclusion of T. Otherwise, when T is a conclusive link, consider the value (say α) assigned to the output premise of T. If α is an outer value, then we are done, for T is a splitting tensor. If α is not an outer value, then it may be factored as $\beta \cdot \gamma^{\frac{1}{2}}$ (or $\beta \cdot \frac{1}{2}\gamma$), for some β and γ. Then, there must exist some homogeneous par-link whose conclusion is assigned the value γ, and one may apply the induction hypothesis on the conclusion of this par-link. □

Lemma 5.9 *Let P be a proof-net without a conclusive par-link. If P contains at least one tensor-link then it contains a splitting tensor.*

Proof. Since P does not contain any conclusive par-link, its output conclusion is either the conclusion of a homogeneous tensor-link or the output conclusion of an axiom link.

In the first case, consider the values (say α and β) assigned to the premises of the homogeneous tensor-link. If α and β are outer values, then the homogeneous tensor-link is a splitting tensor. Otherwise, it must be the case that α and β may be factored as $\alpha' \cdot \frac{1}{2}\gamma$ and $\beta' \cdot \gamma\frac{1}{2}$. This implies that there exists a homogeneous par-link whose conclusion is assigned the value γ. The conclusion of this par-link satisfies the hypotheses of Lemma 5.8, and consequently P contains a splitting tensor.

The second case is similar to the proof of Lemma 4.14, using Lemma 5.8 instead of Lemma 4.13. □

Proposition 5.10 *Any proof-net P is sequentialisable.*

Proof. The proof is similar to the one of Proposition 4.15, using Lemma 5.9 instead of Lemma 4.14. □

6 Intuitionistic proof-nets: the non-commutative case

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 [9].

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

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

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

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

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

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

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 polarized formulas as follows:

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

This gives rise to the links, the constraints, and the switches of Figure 9 and 10.

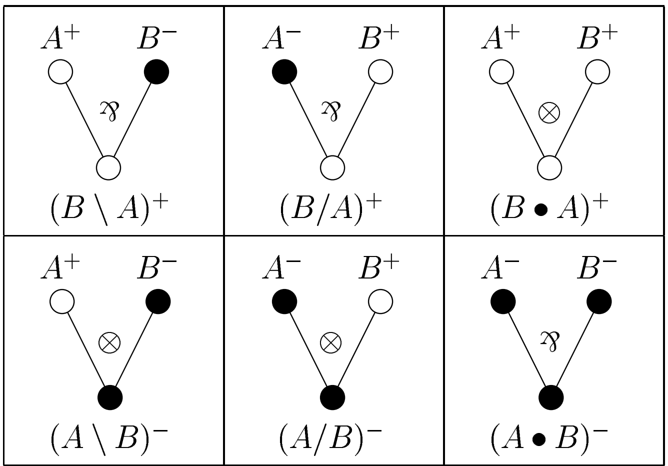

Figure 9: Links for the Lambek calculus

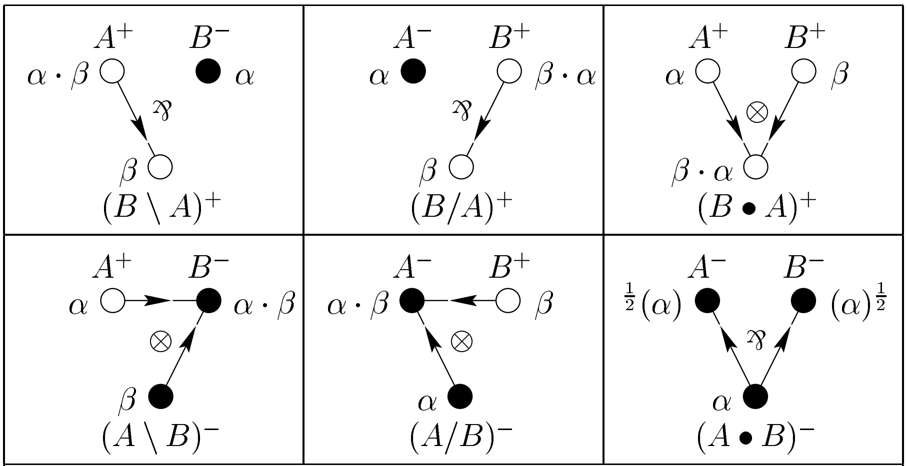

Figure 10: Constraints and switches for the Lambek calculus

To adapt our sequentialisation proof to the Lambek calculus is straightforward. We leave the details to the interested reader.

7 Concluding remarks

As we said in the introduction, our criterion is intrinsically intuitionistic, which is also the case of Lamarche's [6]. 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 [8]. 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 [8, 10]. In contrast, when using our criterion, commutative correctness and non-commutativity are not checked independently.

In his thesis [10, 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. Ph. de Groote. Strong normalization in a non-deterministic typed lambda-calculus. In *Proceedings of the the 4th international symposium on Logical Foundations of Computer Science–Yaroslavl'97*, volume 1234 of *Lecture Notes in Computer Science*, pages 130–140. Springer Verlag, 1997.
4. J.-Y. Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.
5. J.-Y. Girard. Quantifiers in linear logic II. Technical Report 19, Equipe de Logique Mathématique, Université de Paris VII, 1991.
6. F. Lamarche. Proof nets for intuitionistic linear logic 1: Essential nets. Technical report, Imperial College, April 1994.
7. F. Lamarche. Games semantics for full propositional linear logic. In *Ninth Annual IEEE Symposium on Logic in Computer Science*. IEEE Press, 1995.
8. 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.
9. J. Lambek. The mathematics of sentence structure. *Amer. Math. Monthly*, 65:154–170, 1958.
10. D. Roorda. *Resource Logics: proof-theoretical investigations.* PhD thesis, University of Amsterdam, 1991.