Subnets of Proof-nets in $\mathbf{MLL}^-$

G. Bellin * J. van de Wiele

December 21, 1994

Abstract

The paper studies the properties of the subnets of proof-nets. Very simple proofs are obtained of known results on proof-nets for $\mathbf{MLL}^-$, Multiplicative Linear Logic without propositional constants.

Contents

1 Preface

The theory of proof-nets for $\mathbf{MLL}^-$, multiplicative linear logic without the propositional constants $\mathbf{1}$ and $\bot$, has been extensively studied since Girard's

*Research supported by EC Individual Fellowship Human Capital and Mobility, contract n. 930142

fundamental paper [5]. The improved presentation of the subject given by Danos and Regnier [3] for propositional $\mathbf{MLL}^-$ and by Girard [7] for the first-order case has become canonical: the notions are defined of an arbitrary proof-structure and of a 'contex-forgetting' map $(\, . \,)^-$ from sequent derivations to proof-structures which preserves cut-elimination; correctness conditions are given that characterize proof-nets, the proof-structures $\mathcal{R}$ such that $\mathcal{R} = (\mathcal{D})^-$, for some sequent calculus derivation $\mathcal{D}$. Although Girard's original correctness condition is of an exponential computational complexity over the size of the proof-structure, other correctness conditions are known of quadratic computational complexity.

A further simplification of the canonical theory of proof-nets has been obtained by a more general classification of the subnet of a proof-net. Given a proof-net $\mathcal{R}$ and a formula A in $\mathcal{R}$, consider the set of subnets that have A among their conclusions, in particular the *largest* and the *smallest* subnet in this set, called the *empire* and the *kingdom* of A, respectively. One must give a construction proving that such a set is not empty: in Girard's fundamental paper a construction of the empires is given which is linear in the size of the proof-net. When the notion of kingdom is introduced, the essential properties of proof-nets – including the existence of a sequent derivation $\mathcal{D}$ such that $\mathcal{R} = (\mathcal{D})^-$ (Theorem 1, *sequentialization theorem*) – can be easily proved using simple properties of the kingdoms and empires, in particular the fact that the relation X *is in the kingdom of* Y is a strict ordering. [1]

Moreover the map $(\, . \,)^-$ identifies equivalence classes of sequent derivations, where $\mathcal{D}_i$ and $\mathcal{D}_j$ are equivalent if they differ only for permutations of inferences. Now consider the set of derivations $\mathcal{B}$ which have A as a conclusion, and that are subderivations of some derivation $\mathcal{D}_i$ in an equivalence class. The kingdom and the empire of a formula A in the proof-net $(\mathcal{D}_i)^-$ yield the notions of the minimum and the maximum, respectively, in such a set of subderivations (Theorem 2). This fact gives evidence that the notions is question do not depend on accidental features of the representation; therefore satisfactory generalizations of our results to larger fragments or to other logics should include Theorem 2.

Such a generalization is impossible in any logic with any form of Weakening, e.g., in the fragment $\mathbf{MLL}$ of multiplicative linear logic with the rule for the constant $\bot$. Indeed a minimal subderivation in which a formula A may be introduced by Weakening is an axiom; but the process of permuting Weakening

[1]The notion of kingdom and the discovery of its properties originated in the Équipe de Logique in the winter 1991-92 and appeared in discussions through electronic mail involving Danos, Girard, Gonthier, Joinet, Regnier, (Paris VII), Gallier and de Groote (University of Pennsylvania) and the author (University of Edinburgh).

upwards in a derivation is non-deterministic and does not always identify a unique axiom as the minimum in our set of subderivations; hence in such a logic we cannot have a meaningful notion of *kingdom*.

2 Proof Nets for Propositional $\mathbf{MLL}^\perp$

We give a simple presentation of the well-known basic theory of proof nets for Multiplicative Linear Logic without propositional constants ($\mathbf{MLL}^-$). The main novelty is the use of the structural properties of subnets of a proof-net, in particular the tight relations between *kingdoms* and *empires*. A pay-off is a simple and elegant proof of the following theorems:[2]

Theorem 1. *There exists a* "context-forgetting" *map* $(\ .\ )^-$ *from sequent derivations in* $\boldsymbol{MLL}^-$ *to proof nets for* $\boldsymbol{MLL}^-$ *with the following properties:*
(a) *Let* $\mathcal{D}$ *be a derivation of* Γ *in the sequent calculus for* $\boldsymbol{MLL}^-$*; then* $(\mathcal{D})^-$ *is a proof net with conclusions* Γ.
(b) (Sequentialization) *If* $\mathcal{R}$ *is a proof net with conclusions* Γ *for* $\boldsymbol{MLL}^-$*, then there is a sequent calculus derivation* $\mathcal{D}$ *of* Γ *such that* $\mathcal{R} = (\mathcal{D})^-$.
(c) *If* $\mathcal{D}$ *reduces to* $\mathcal{D}'$*, then* $\mathcal{D}^-$ *reduces to* $(\mathcal{D}')^-$.
(d) *If* $\mathcal{D}^-$ *reduces to* $\mathcal{R}'$ *then there is a* $\mathcal{D}'$ *such that* $\mathcal{D}$ *reduces to* $\mathcal{D}'$ *and* $\mathcal{R}' = (\mathcal{D}')^-$.

Theorem 2. (Permutability of Inferences) (i) *Let* $\mathcal{D}$ *and* $\mathcal{D}'$ *be a pair of derivation of the same sequent* $\vdash \Gamma$ *in propositional* $\boldsymbol{MLL}^-$*. Then* $(\mathcal{D})^- = (\mathcal{D}')^-$ *if and only if there exists a sequence of derivations* $\mathcal{D} = \mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n = \mathcal{D}'$ *such that* $\mathcal{D}_i$ *and* $\mathcal{D}_{i+1}$ *differ only for a permutation of two consecutive inferences.*

(ii) *Let* $\mathcal{R}$ *be a proof-net and let* A *be a formula occurrence in* $\mathcal{R}$*. Then there exists a derivation* $\mathcal{D}$ *with* $(\mathcal{D})^- = \mathcal{R}$ *and a subderivation* $\mathcal{B}$ *of* $\mathcal{D}$ *such that* $(\mathcal{B})^- = eA$*. A similar statement holds for* kA.

2.1 Propositional Proof Structures and Proof Nets

A *link* is an $m+n$-ary relation between formula occurrences, for some $m, n \geq 0$, $m + n \neq 0$. Suppose $X_1, \ldots, X_{m+n}$ are in a link: if $m > 0$, then $X_1, \ldots, X_m$ are called the *premises* of the link; if $n > 0$, then $X_{m+1}, \ldots, X_{m+n}$ are called the *conclusions* of the link. If $m = 0$, the link is called an *axiom* link.

[2] Here we prove part (a) and (b) of Theorem 1; the proof of parts (c) and (d) are clear from [5, 7].

Links are graphically represented as

$$\frac{X_1, \ldots, X_m}{X_{m+1}, \ldots, X_{m+n}}$$

We consider links of the following forms:

Identity Links:

$$\textit{axiom links:} \quad \overline{A \quad A^-} \qquad \textit{cut links:} \quad \frac{A \quad A^-}{cut}$$

Multiplicative Links:

$$\textit{times links:} \quad \frac{A \quad B}{A \otimes B} \qquad \textit{par links:} \quad \frac{A \quad B}{A \wp B}$$

Convention. We assume that the logical axioms and cut links are *symmetric* relations. Other links are *not* regarded as symmetric. The word "*cut*" in a cut link is not a formula, but a place-holder; following common practice, we may sometimes omit it.

Definitions 1. (i) A *proof structure* $\mathcal{S}$ for propositional $\mathbf{MLL}^-$ consists of (i) a nonempty set of *formula-occurrences* together with (ii) a set of identity links, multiplicative links satisfying the properties:

1. Every formula-occurrence in $\mathcal{S}$ is the conclusion of one and only one link;

2. Every formula-occurrence in $\mathcal{S}$ is the premise of at most one link.

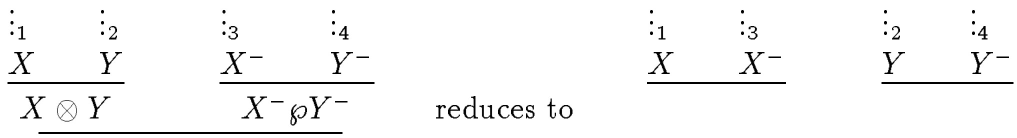
We write $X \prec Y$ if X is a *hereditary premise* of Y; in this case we also say that 'X is above Y'. We shall draw proof structures in the familiar way as non-empty, not necessarily planar, graphs.

(ii) We define the following reductions on propositional $\mathbf{MLL}^-$ proof structures:

Axiom Reductions

$$\begin{array}{ccccc} \vdots & & & & \vdots \\ \underline{X \quad \overline{X^-}} & \overline{\quad\ } X & & \text{reduces to} & X \\ & & \vdots & & \vdots \end{array}$$

Symmetric Reductions



Definitions 2. Let $\mathcal{R}$ be a propositional proof structure for $\mathbf{MLL}^-$.

(i) A *Danos-Regnier switching* s for $\mathcal{R}$ consists in the choice for each *par* link $\mathcal{L}$ in $\mathcal{R}$ of one of the premises of $\mathcal{L}$.

(ii) Given a switching s for $\mathcal{R}$, we define the undirected *Danos-Regnier graph* $s(\mathcal{R})$ as follows:

- the vertices of $s(\mathcal{R})$ are the formulas of $\mathcal{R}$;
- there is an edge between vertices X and Y exactly when:

1. X and Y are the conclusions of a logical axioms or the premises of a cut link; or
2. X is a premise and Y the conclusion of a *times* link; or else
3. Y is the conclusion of a *par* and X is the occurrence selected by the switching s.

Definition 3. Let $\mathcal{R}$ be a multiplicative proof-structure. $\mathcal{R}$ is a *proof-net* for propositional $\mathbf{MLL}^-$ if for every switching s of $\mathcal{R}$, the graph $s(\mathcal{R})$ is *acyclic* and *connected* (i.e., an undirected *tree*).

2.2 Subnets

Definitions 4. Let $m : \mathcal{S} \to \mathcal{R}$ be any injective map of $\mathbf{MLL}^-$ proof structures (regarded as sets of formula occurrences) such that X and $m(X)$ are occurrences of the same formula.

(i) We say that *m preserves the links* if for every $\mathcal{L}$ in $\mathcal{S}$ there is a link $\mathcal{L}'$ in $\mathcal{R}$ of the same kind such that

$$\mathcal{L} : \frac{X_1, \ldots, X_k}{X_{k+1}, \ldots X_{k+n}} \qquad \mapsto \qquad \mathcal{L}' : \frac{mX_1, \ldots, mX_k}{mX_{k+1}, \ldots mX_{k+n}}$$

(ii) A proof-structure $\mathcal{S}$ is a *substructure* of a proof-structure $\mathcal{R}$ if there is an injective map $\iota : \mathcal{S} \to \mathcal{R}$ preserving links. If $\mathcal{S}$ is a substructure of $\mathcal{R}$, then the lowermost formula occurrences of $\mathcal{S}$ are also called the *doors* of $\mathcal{S}$.

(iii) We write $st\Sigma$ for the *smallest substructure* of $\mathcal{R}$ containing Σ.

(iv) A *subnet* is a substructure which satisfies the condition of proof-nets.

Remark. In definition 4.(ii) let ι be the identity map. A subset $\mathcal{S}$ of $\mathcal{R}$ (with the links of $\mathcal{R}$ holding among the occurrences in $\mathcal{S}$) is a substructure if and only if

(1) $\mathcal{S}$ is closed under hereditary premises and
(2) if $\overline{X_0 \quad X_1}$ is an axiom and $X_i \in \mathcal{S}$ then $X_{1-i} \in \mathcal{S}$.

In particular, the set of formula occurrences in $st(\Sigma)$ consists of Σ, of all the hereditary premises of Σ and of the axioms above them:

$$st(\Sigma) = \bigcup_{Z \in \Sigma} \{X : X \preceq Z\} \cup \bigcup_{Z \in \Sigma} \{X \in \overline{X \quad Y} : Y \preceq \Sigma\}.$$

Lemma 1. *Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be subnets of the proof net $\mathcal{R}$. Then*
(i) $\mathcal{S} = \mathcal{R}_1 \cup \mathcal{R}_2$ *is a subnet if and only if* $\mathcal{R}_1 \cap \mathcal{R}_2 \neq \emptyset$.

(ii) *If* $\mathcal{R}_1 \cap \mathcal{R}_2 \neq \emptyset$ *then* $\mathcal{R}_0 = \mathcal{R}_1 \cap \mathcal{R}_2$ *is a subnet.*

Proof. Let $\mathcal{R}$ be a proof net and $\mathcal{R}'$ any substructure. Given a switching s' for $\mathcal{R}'$, extend s' to a switching s for $\mathcal{R}$; then $s'\mathcal{R}'$ is a subgraph of $s\mathcal{R}$, hence $s'\mathcal{R}'$ is acyclic, since $s\mathcal{R}$ is. Therefore we need only to consider the connectedness of $s\mathcal{S}$ and $s\mathcal{R}_0$.

To prove (i), assume $\mathcal{R}_1$ and $\mathcal{R}_2$ are subnets with nonempty intersection and fix a switching s for $\mathcal{S} = \mathcal{R}_1 \cup \mathcal{R}_2$. For $i = 1, 2$ let $s\mathcal{R}_i$ be the restriction of $s\mathcal{R}$ to $\mathcal{R}_i$; then $s\mathcal{R}_i$ is connected since $\mathcal{R}_i$ is a subnet. Let A be in $\mathcal{R}_1$ and B in $\mathcal{R}_2$; if $C \in \mathcal{R}_1 \cap \mathcal{R}_2$, then A is connected with C since $s\mathcal{R}_1$ is connected and B is connected with C since $s\mathcal{R}_2$ is connected, hence A is connected with B as required. The converse is immediate, namely, if $\mathcal{R}_1 \cap \mathcal{R}_2 = \emptyset$, then any Danos-Regnier graph on $\mathcal{R}_1 \cup \mathcal{R}_2$ is disconnected.

To prove (ii), let s_0 be a switching for $\mathcal{R}_0 = \mathcal{R}_1 \cap \mathcal{R}_2$; let s_1, s_2 be extensions of s_0 to $\mathcal{R}_1$, $\mathcal{R}_2$, respectively; then $s = s_1 \cup s_2$ is a switching of $\mathcal{R}_1 \cup \mathcal{R}_2$. If A and B occur in $\mathcal{R}_0$, then they are connected by a path π_1 in $s_1\mathcal{R}_1$ and by a path π_2 in $s_2\mathcal{R}_2$; if $\pi_1 \neq \pi_2$, then there is a cycle in $s\mathcal{S}$, which is impossible. But $\pi_1 = \pi_2$ means that A and B are connected in $s_0\mathcal{R}_0$. ∎

Proposition 1: (i) *Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be proof nets and let*

$$\mathcal{S} = \mathit{Times}\,(\mathcal{R}_1, \mathcal{R}_2) = \dfrac{\begin{matrix}\mathcal{R}_1 & \mathcal{R}_2 \\ A & B\end{matrix}}{A \otimes B} \quad \text{or} \quad \mathcal{S} = \mathit{Cut}\,(\mathcal{R}_1, \mathcal{R}_2) = \dfrac{\begin{matrix}\mathcal{R}_1 & \mathcal{R}_2 \\ A & A^-\end{matrix}}{\mathit{cut}}$$

Then $\mathcal{S}$ is a proof net if and only if $\mathcal{R}_1 \cap \mathcal{R}_2 = \emptyset$.

(ii) *Let $\mathcal{R}_0$ be a substructure of the proof net $\mathcal{R}$ and let*

$$\mathcal{S} = Par\,(\mathcal{R}_0) = \frac{\begin{array}{c}\mathcal{R}_0\\ A_1 \quad A_2\end{array}}{A \wp B}$$

Then $\mathcal{S}$ is a subnet if and only if $\mathcal{R}_0$ is a subnet.

Proof. (i) Let s be a switching of $\mathcal{S} = Times\,(\mathcal{R}_1, \mathcal{R}_2)$; since $\mathcal{R}_1$ and $\mathcal{R}_2$ are proof nets, each of the graphs $s\mathcal{R}_1$ and $s\mathcal{R}_2$ are acyclic and connected; in addition to $s\mathcal{R}_1 \cup s\mathcal{R}_2$, $s\mathcal{S}$ has the vertex $A \otimes B$ and two edges $(A, A \otimes B)$ and $(B, A \otimes B)$, which establish a connection between $s\mathcal{R}_1$ and $s\mathcal{R}_2$; this is the only connection since $\mathcal{R}_1$ and $\mathcal{R}_1$ are disjoint.
Conversely, if $\mathcal{R}_1 \cap \mathcal{R}_2 \neq \emptyset$, then by lemma 1.(i) $\mathcal{R}_1 \cup \mathcal{R}_2$ is a subnet. Therefore given any switching s of $\mathcal{S}$, the nodes A and B in are connected already in $s(\mathcal{R}_1 \cup \mathcal{R}_2)$; also the edges along link $\frac{A \quad B}{A \otimes B}$ yield another connection between the vertices A and B, hence there is a cycle in $s\mathcal{S}$. ∎
Part (ii) is immediate: for any switching s of $\mathcal{R}$, $s\mathcal{S}$ comes from $s\mathcal{R}_0$ by introducing an additional edge $(A_i, A_1 \wp A_2)$ to a leaf A_i, where $A \wp B$ is a new leaf. ∎

By induction on the definition of a sequent derivation in $\mathbf{MLL}^{-}$ we define the map $(\ .\ )^{-}$ from sequent derivations to proof structures ("forgetting the context").

Theorem 1.(a) *Let $\mathcal{D}$ be a derivation in the sequent calculus for $\mathbf{MLL}^{-}$; then $(\mathcal{D})^{-}$ is a proof net.*

Proof. Axioms are proof nets, and the property of being a net is preserved under the *times*, *cut* and *par* rules by Proposition 1. ∎

Definitions 5. Let Σ be a set of formula-occurrences in a proof-net $\mathcal{R}$.
(i) The *territory* $t\Sigma$ of is the smallest subnet of $\mathcal{R}$ including Σ (*not necessarily as doors*).
(ii) The *kingdom* kA [the *empire* eA] of a formula-occurrence A in a proof-net $\mathcal{R}$ is the smallest [the largest] subnet of $\mathcal{R}$ having A as a door.
(iii) Let $X \ll Y =_{df} X \in kY$.

Remarks. (i) Given a proof-net $\mathcal{R}$ and formula occurrences Σ in $\mathcal{R}$, the subnet $t\Sigma$ always exists by Lemma 1.
(ii) Suppose for no X, Y in Σ we have that X is a hereditary premise of Y $(X \prec Y)$. Then $st\Sigma$, the smallest substructure containing Σ, has all the occurrences in Σ among its doors. On the other hand, there may not be a *subnet* having all of Σ among its doors.
(iii) The existence of kA and eA is immediate by Lemma 1 once we prove there

exists a subnet having A as a door. This can be done by giving an explicit construction of eA as in [5, 7] and in the following section.

2.3 Empires and Kingdoms: Existence and Properties

Among the results in this section, for the proof of the Sequentialization theorem we need only the fact that for each formula occurrence A in a proof-net $\mathcal{R}$ there exists a subnet having A as a door.

Definition 6. Let A be a formula occurrence in the proof net $\mathcal{R}$. For a given D-R-switching s, let $s(\mathcal{R}, A)$ be (the set of formula occurrences and of links occurring in) the connected component of the graph $s\mathcal{R}$ which is obtained as follows:

- if A is a premise of a link in $\mathcal{R}$ with conclusion Z and there is an edge (A, Z) in the D-R-graph $s\mathcal{R}$, then remove (A, Z) and let $s(\mathcal{R}, A)$ be the component containing the vertex A.
- otherwise, let $s(\mathcal{R}, A)$ be $s\mathcal{R}$.

We write $\overline{s(\mathcal{R}, A)}$ for the connected component not containing A after the removal of the edge (A, Z) from $s\mathcal{R}$, if such an edge exists; $\overline{s(\mathcal{R}, A)}$ is empty otherwise.

Definition 7. Let $\mathcal{R}$ be a proof-net and let Σ be a set of formula-occurrences in $\mathcal{R}$. We write $path_s(\Sigma)$ for the smallest subgraph of $s\mathcal{R}$ connecting all formula-occurrences in Σ. Clearly $path_s(A, B)$ is a path of $s\mathcal{R}$, for every A, B in $\mathcal{R}$ and every switching s for $\mathcal{R}$.

Proposition 2. (Characterizartions of empires; cf. [3, 5, 7]) *Let $\mathcal{R}$ be a proof net. Then $e(A)$ (the largest subnet of $\mathcal{R}$ containing A as a conclusion) exists and is characterized by the following equivalent conditions:*

(a) $\bigcap_s s(\mathcal{R}, A)$, *where s varies over all possible switchings;*

(b) *the smallest set of formula occurrences in $\mathcal{R}$ closed under the following conditions:*

(i) $A \in e(A)$;

(ii) if $\frac{X_1 \quad X_2}{Y}$ is a link in $\mathcal{S}$ and $Y \in e(A)$, then $X_1, X_2 \in e(A)$, ($\uparrow$-*step*);

(iii) if $\overline{X_0 \quad X_1}$ is an axiom in $\mathcal{S}$ and $X_i \in e(A)$, then $X_{1-i} \in e(A)$ ($\rightarrow$-*step*);

(iv) if $\frac{X_1 \quad X_2}{X_1 \otimes X_2}$ is a link in $\mathcal{S}$, and for $i = 1$ or 2 $X_i \neq A$ and $X_i \in e(A)$, then $X_1 \otimes X_2 \in e(A)$ ($\downarrow$-*step*);

(v) if $\frac{X_1 \quad X_2}{X_1 \wp X_2}$ is a link in $\mathcal{S}$, $X_1 \neq A \neq X_2$ and $\{X_1, X_2\} \subset e(A)$, then $X_1 \wp X_2 \in e(A)$ ($\Downarrow$-*step*).

(According to our conventions, $X_i \neq A$ means that X_i and A are different formula *occurrences*.)

Proof. The following proof of $(a) = (b)$ follows the argument in [7]. To show that $(b) \subseteq (a)$ we show that the set (a) is closed under the conditions $(i) \perp (v)$ defining (b). This is easy for clauses (i), (iii), (iv) and (v) of (b), and also for clause (ii), if the link in question is a *times* link. Now suppose that for some *par* link $\mathcal{L}$ the conclusion $X_1 \wp X_2 \in \bigcap_s s(\mathcal{R}, A)$, but, say, for the premise X_2 we have $X_2 \notin \bigcap_s s(\mathcal{R}, A)$. Then for some s we have that $X_1 \wp X_2$ belongs to $s(\mathcal{R}, A)$ and X_2 does not. Therefore A is premise of a link with conclusion Z and X_2 belongs to the same connected component as Z, i.e., to $\overline{s(\mathcal{R}, A)}$; let π be $path_s(X_2, Z)$, the path connecting X_2 and Z in $\overline{s(\mathcal{R}, A)}$. Since the switching s in $\mathcal{L}$ is Left and the edge $(X_1, X_1 \wp X_2)$ belongs to $s(\mathcal{R}, A)$, it plays no role in the connections π between X_2 and Z. Therefore if s' is like s, except that the switch on $\mathcal{L}$ is changed from Left to Right, then we still have a connection π between X_2 and Z; since $X_1 \wp X_2 \in \bigcap_s s(\mathcal{R}, A)$, π can be extended to a connection $path_{s'}(A, Z)$, between A and Z in $s'(\mathcal{R}, A)$; but then in $s'A$ we have a cycle, and this is a contradiction. Therefore $\{X_1, X_2\} \subset eA$.

To show that $(a) \subseteq (b)$ we consider a *principal switching* s for A: this is a switching such that for every *par* link $\mathcal{L}$, if a premise X_i of $\mathcal{L}$ is in (b), but the conclusion $X_0 \wp X_1$ is not, then s chooses X_{1-i}. We claim that if s is a principal switching, then $s(\mathcal{R}, A)$ is precisely (b).

Notice that any set $\mathcal{S}$ closed under clauses $(i) \perp (v)$ has the property that if $\mathcal{S}$ contains X, then it contains also every formula occurrence Z such that X and Z are in a link $\mathcal{L}$, in all cases *except perhaps the following*:

(1) X is A and a premise of $\mathcal{L}$, while Z is the conclusion of $\mathcal{L}$;

(2) $\mathcal{L}$ is a *par* link, X is a premise and Z the conclusion of $\mathcal{L}$, and the other premise Y is not it $\mathcal{S}$.

It follows that the set (b) is a substructure of $\mathcal{R}$ whose doors can only be conclusions of $\mathcal{R}$, or cuts, or occurrences X as in (1) or (2).

Now suppose a formula-occurrence W is in (a) but not in (b); choose a switching s principal for A. Since $s(\mathcal{R}, A)$ is connected and (b) is a substructure, the path π connecting A with W in $s(\mathcal{R}, A)$ must exit (b) from a door X as in cases (1) or (2). But this is impossible by the definition of principal switching and of $s(\mathcal{R}, A)$. Hence $(a) \subseteq (b)$ as claimed.

We must show that A is a door of the substructure equivalently defined by (a) and (b). Let $Z \in \bigcap_s s(\mathcal{R}, A)$ and suppose $A \prec Z$. Choose a switching s

such that if $\dfrac{X_0 \quad X_1}{X_0 \wp X_1}$ is a link such that $A \preceq X_i \prec Z$, then s chooses X_{1-i}.

We claim that there must be a *times* link $\dfrac{B \quad C}{B \otimes C}$ in $s(\mathcal{R}, A)$ such that, say, $A \preceq C \prec Z$: otherwise, $Z \notin s(\mathcal{R}, A)$, by the choice of s and the definition of $s(\mathcal{R}, A)$. Thus let $\mathcal{L}$ be the uppermost such link: then the path π connecting A and B in $s(\mathcal{R}, A)$ does not pass through C; but then in $s\mathcal{R}$ we have two distinct paths connecting A and B, and this contradicts the acyclicity of $s\mathcal{R}$.

Since (b) is a substructure satisfying the condition (a), for each s the restriction of $s(\mathcal{R}, A)$ to (b) is acyclic and connected, hence (b) is a subnet. We have proved that given a proof-net $\mathcal{R}$ and a formula-occurrence A in $\mathcal{R}$, a subnet with conclusion A always exists.

But (a) is also the largest among such subnets: let $\mathcal{S}$ be a substructure of $\mathcal{R}$ with A as a door and suppose $Z \in \mathcal{S} \setminus (a)$; then for some s, we have $Z \notin s(\mathcal{R}, A)$, from which it follows that no path connects A and Z in $s\mathcal{S}$; hence $\mathcal{S}$ is not a subnet. We conclude that $e(A) = (a) = (b)$. ∎

The construction of a principal switching was given first in Girard's *Trip Theorem* (cf. [5], 2.9.5.); using Girard's notion of a *trip* the principal switching constructed 'dynamically', by making the following choices during a trip.

Starting from A, the trip proceed upwards in $\mathcal{R}$, and at a branching point, i.e., at *times* link, we choose arbitrarily;

- if the trip reaches a *par* link for the first time from below, then we fix s arbitrarily and the trip continues to the chosen premise;
- if the trip reach a *par* link *for the first time* from a premise, then we let s choose the *other* premise.

The Trip Theorem shows that eA is exactly the set of occurrences visited between the first and the second visit to A. The algorithm is transfered to our setting using the correspondence between trips and D-R-graphs established by Danos and Regnier [3]. One advantage of such a formulation is that the following corollary becomes completely obvious.

Corollary. *The complexity of the computation of eA is linear on the size of the proof-net.* ∎

Proposition 3.(I) (properties of territories). *Let $\mathcal{R}$ be a proof-net and let Σ be a set of occurrences in $\mathcal{R}$. Then the territory $t\Sigma$ satisfies*

$$t\Sigma = t(path_s(\Sigma)) = \bigcup_{X \in path_s(\Sigma)} tX$$

for any switching s. ■

Proposition 3.(II) (characterizations of kingdoms).[3] *Let $\mathcal{R}$ be a proof net. Then the kingdom kA of A in $\mathcal{R}$ (the smallest subnet of $\mathcal{R}$ having A as a conclusion), exists and is characterized by the following equivalent conditions:*

(a) tA;

(b) *the smallest set satisfying the following conditions (Danos et al.):*

(o) $A \in kA$.

(i) Let $\overline{X \quad X^-}$ occur in $\mathcal{R}$. Then

$$\overline{X \quad X^-} = kX = t(X, X^-) = kX^-.$$

(ii) Let $\mathcal{L} : \dfrac{A \quad B}{A \otimes B}$ be a link in $\mathcal{R}$. Then

$$kX \otimes Y = kX \cup kY \cup \{X \otimes Y\}.$$

(iii) Let $\mathcal{L} : \dfrac{X \quad Y}{X \wp Y}$ be a link in $\mathcal{R}$. Then

$$kX \wp Y = \bigcup \{kC | C \in path_s(X, Y)\} \cup \{X \wp Y\}$$

for any switching s.

(c) *the smallest set of formula occurrences closed under the following conditions:*

(i) $A \in k(A)$;

(ii) if $\frac{X_1 \quad X_2}{Y}$ is a link in $\mathcal{S}$ and $Y \in k(A)$, then $X_1, X_2 \in k(A)$ [similarly, if $\frac{X[t/y]}{\exists y.X}$ is a link in $\mathcal{S}$ and $\exists y.X \in k(A)$, then $X[t/y] \in k(A)$] ($\uparrow$-*step*);

(iii) if $\overline{X_0 \quad X_1}$ is an axiom in $\mathcal{S}$ and $X_i \in k(A)$, then $X_{1-i} \in k(A)$ ($\rightarrow$-*step*);

(iv) if $\frac{\ldots X \ldots}{Y}$ is a link in $\mathcal{S}$ $X \neq A \neq Y$, $X \in k(A)$, then $Y \in kA$ iff $A \notin eX$ ($\downarrow$-*step*). ■

The proof is left to the reader; for case $(c)(iv)$, see the following Lemma 2.

[3] Characterization (b) is due to Danos and others, as specified in footnote 1. Characterization (c) was suggested to us by J-Y. Girard.

2.4 Sequentialization Theorem

Lemma 2. (Empire-Kingdom Nesting) *Let* $\mathcal{L}_1 : \frac{\dots A \dots}{C}$ *and* $\mathcal{L}_2 : \frac{\dots B \dots}{D}$ *be distinct links in a proof net* $\mathcal{R}$ *for* $\boldsymbol{MLL}^-$. *Suppose* $B \in eA$; *then* $D \notin eA$ *if and only if* $C \in kD$.

Proof. Clearly $B \in eA \cap kD$, hence $\mathcal{R}_0 = eA \cap kD$ and $\mathcal{S} = eA \cup kD$ are subnets of $\mathcal{R}$. If $C \notin kD$ and $D \notin eA$, then $\mathcal{S}$ is a subnet with conclusion A, which is larger than eA, since it contains D: this contradicts the definition of the empire of A. If $C \in kD$ and $D \in eA$, then $\mathcal{R}_0$ is a subnet with conclusion D, which is smaller than kD since it does not contain C: this contradicts the definition of the kingdom of D. ∎

Lemma 3. (Kingdom Ordering) (i) *Let* $\mathcal{R}$ *be a proof net and let* X, Y *occur in* $\mathcal{R}$. *If* $X \ll Y$ *and* $Y \ll X$ *then either* X *and* Y *are the same occurrence or they occur in an axiom* $\overline{X \quad Y}$ *of* $\mathcal{R}$. (ii) *Hence* $\ll$ *is an ordering* of the conclusions of non-axiom links.

Proof. For an axiom $\mathcal{A} = \overline{X\ X^-}$ we have $kX = \mathcal{A} = kX^-$. Otherwise, let $X \in kY$, with X and Y distinct; if also $Y \in kX$, then $kY \cap kX$ is a subnet, and necessarily $kX = kX \cap kY = kY$.

If X is $X_1 \wp X_2$ in a link $\mathcal{L}$: $\dfrac{X_1 \quad X_2}{X_1 \wp X_2}$ then the result of removing X and $\mathcal{L}$ from kY is still a subnet, and this contradicts the definition of kY.

If X is $X_1 \otimes X_2$ in a link $\dfrac{X_1 \quad X_2}{X_1 \otimes X_2}$ then clearly $kX = k(X_1) \cup k(X_2) \cup \{X\}$, hence for $i = 1$ or 2, $Y \in k(X_i)$; but by Lemma 2, Y is not even in $e(X_i)$. ∎

Theorem 1.(b) (Sequentialization) *If* $\mathcal{R}$ *is a proof net with conclusions* Γ, *then there is a sequent calculus derivation* $\mathcal{D}$ *of* Γ *such that* $\mathcal{R} = (\mathcal{D})^-$.

Proof. By induction on the size of $\mathcal{R}$. If $\mathcal{R}$ is an axiom, then $\mathcal{D}$ is an axiom sequent. If one of the lowermost links is a *par* or *for all* link, then we remove such a link, we apply the induction hypothesis to the resulting subnet and we conclude by applying a suitable *par* inference. Now suppose that all the conclusions of $\mathcal{R}$ are conclusions either of an axiom or of a *times* link: we choose a terminal *times* link $\mathcal{L}$ whose conclusion $X = A_i \otimes B_i$ is maximal w.r.t. $\ll$. In this case eA_i and eB_i split $\mathcal{R} \setminus \{A_i \otimes B_i\}$. Suppose not; then there is a link $\mathcal{L} : \frac{\dots D \dots}{C}$ such that, say, $D \in eB_i$ and $C \notin eB_i$. But C occurs at or above another conclusion $Y = A_j \otimes B_j$. By the lemma 2 $X = A_i \otimes B_i \in kC$; also $C \in kY$ hence $kC \subset kY$; thus we obtain $X \in kY$, contradicting the choice of X. ∎

Remark. The computational complexity of Girard's *no-short-trip* condition and of Danos-Regnier's requirement that all D-R-graphs be acyclic and connected is clearly exponential on the size of the given proof-structure. It is known (see, e.g., [3, 4, 1]) that there are procedures to decide whether or not a proof-structure $\mathcal{R}$ for $\mathbf{MLL}^-$ is a proof-net in time quadratic over the cardinality of $\mathcal{R}$.

2.5 Permutability of Inferences in the Sequent Calculus

Given a derivation $\mathcal{D}$ and two formula-occurrences X_1 and X_2 in some sequents of $\mathcal{D}$, if X_1 is an ancestor of X_2 then certainly the inference introducing X_1 must occur above the inference introducing X_2. We are concerned with occurrences X_1 and X_2 in $\mathcal{D}$ such that neither one is an ancestor of the other. Suppose X_1 is introduced above X_2 in $\mathcal{D}$, we ask whether there is a derivation $\mathcal{D}'$ which is obtained from $\mathcal{D}$ by successive permutation of the inferences and such that X_1 is introduced below X_2 in $\mathcal{D}'$.

Counterexample. The following is a derivation in $\mathbf{MLL}^-$ in which the applications of the $\otimes$-rule and of the $\wp$-rule cannot be permuted.

$$\dfrac{\dfrac{\dfrac{\vdash P^-, P \qquad \vdash Q, Q^-}{\vdash P^-, P\otimes Q, Q^-}\otimes}{\vdash Q^-, P^-, P\otimes Q}\, exchange}{\vdash Q^-\wp P^-, P\otimes Q}\wp$$

Remark. In the sequent calculus for propositinal $\mathbf{MLL}^-$ $\otimes/\wp$, $cut/\wp$ and $\exists/\forall$ are the only exceptions to the permutability of inferences where neither one of the principal formulas is an ancestor of the other.

A full characterization of permutability of inference in $\mathbf{MLL}^-$ is obtained using the 'context-forgetting' map $(\,.\,)^-$ of derivations into proof-nets and the notions of empire and kingdom. Such a map uniquely associates each inference $\mathcal{I}$ in $\mathcal{D}$ other than Exchange with a link $\mathcal{L}$ in $(\mathcal{D})^-$ and the principal formula(s) of $\mathcal{I}$ with the conclusion(s) of $\mathcal{L}$.

Theorem 2. (i) *Let $\mathcal{D}$ and $\mathcal{D}'$ be a pair of derivation of the same sequent $\vdash \Gamma$ in propositional $\boldsymbol{MLL}^-$. Then $(\mathcal{D})^- = (\mathcal{D}')^-$ if and only if there exists a sequence of derivations $\mathcal{D} = \mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n = \mathcal{D}'$ such that $\mathcal{D}_i$ and $\mathcal{D}_{i+1}$ differ only for a permutation of two consecutive inferences.*

(ii) *Let $\mathcal{R}$ be a proof-net and let A be a formula occurrence in $\mathcal{R}$. Then there exists a derivation $\mathcal{D}$ with $(\mathcal{D})^- = \mathcal{R}$ and a subderivation $\mathcal{B}$ of $\mathcal{D}$ such that $(\mathcal{B})^- = eA$. A similar statement holds for kA.*

Proof. (i) The "if" part is clear. To prove the "only if" part, let $(\mathcal{D})^- =$

$\mathcal{R} = (\mathcal{D}')^-$; consider a branch of $\mathcal{D}$ and let $\mathcal{I}_0$ the last inference from bottom up where $\mathcal{D}$ agrees with $\mathcal{D}'$. If $\mathcal{I}_0$ is an axiom, then $\mathcal{D}$ and $\mathcal{D}'$ entirely agree in the order of inferences in this branch. Otherwise, let $\mathcal{I}_A$ be the inference immediately above $\mathcal{I}_0$ in the branch of $\mathcal{D}$ under consideration, and let $\mathcal{I}'_A$ be the inference of $\mathcal{D}'$ such that the principal formulas of $\mathcal{I}_A$ and $\mathcal{I}'_A$ are mapped to the same formula occurrence A of $\mathcal{R}$: such an $\mathcal{I}'_A$ exists, since $(\mathcal{D})^- = (\mathcal{D}')^-$.

Moreover, let $\mathcal{I}'_1, \ldots, \mathcal{I}'_k$ be the inferences which occur in $\mathcal{D}'$ between $\mathcal{I}'_A$ and $\mathcal{I}_0$ (proceeding downwards). Notice that if the principal formula of any $\mathcal{I}'_i$ for $i \leq k$ is mapped to a formula B of $\mathcal{R}$, then the inference $\mathcal{I}_B$ of $\mathcal{D}$ whose principal formula is mapped to B also occurs *above* the inference $\mathcal{I}_0$, by our assumption that $\mathcal{D}$ and $\mathcal{D}'$ agree in the given branch up to $\mathcal{I}_0$. It follows that no descendant of A is active in $\mathcal{I}'_1, \ldots, \mathcal{I}'_k$.

If the inference $\mathcal{I}'_A$ is an instance of the *par* rule, then clearly it can be permuted below $\mathcal{I}'_1, \ldots, \mathcal{I}'_k$. If $\mathcal{I}'_A$ is a *times* rule, say, A is $A_1 \otimes A_2$, then we have

$$\mathcal{I}_A : \frac{\begin{array}{cc} \mathcal{B}_1 & \mathcal{B}_2 \\ \vdots & \vdots \\ \vdash \Gamma_1, A_1 & \vdash \Gamma_2, A_2 \end{array}}{\vdash \Gamma_1, \Gamma_2, A_1 \otimes A_2} \qquad \mathcal{I}'_A : \frac{\begin{array}{cc} \mathcal{B}'_1 & \mathcal{B}'_2 \\ \vdots & \vdots \\ \vdash \Delta_1, A_1 & \vdash \Delta_2, A_2 \end{array}}{\vdash \Delta_1, \Delta_2, A_1 \otimes A_2}$$

If $\mathcal{I}'_1$ is another *times* rule, then clearly it can be permuted above $\mathcal{I}'_A$. If $\mathcal{I}'_1$ is a *par* rule, then consider the inference $\mathcal{I}_C$ of $\mathcal{D}$ such that the principal formulas of $\mathcal{I}'_1$ and $\mathcal{I}_C$ are mapped to the same formula occurrence $C = C_0 \wp C_1$ of $\mathcal{R}$. Now $(\mathcal{B}_j)^-$ is a subnet of $\mathcal{R}$ with A_j as a conclusion, hence $(\mathcal{B}_j)^- \subseteq e(A_j)$; similarly $(\mathcal{B}'_j)^- \subseteq e(A_j)$. Since $\mathcal{I}_C$ occurs above $\mathcal{I}_A$, the link $\dfrac{C_0 \quad C_1}{C_0 \wp C_1}$ occurs in $e(A_j)$; moreover, $e(A_j) \cap e(A_{1-j}) = \emptyset$, hence the active formulas C_0 and C_1 of $\mathcal{I}_1$ are both in the same branch $\mathcal{B}'_j$ of $\mathcal{D}'$. It follows that $\mathcal{I}_1$ can be permuted above $\mathcal{I}'_A$.

(ii) Let $(\mathcal{D})^- = \mathcal{R}$; let $\mathcal{I}_A$ be the inference in $\mathcal{D}$ whose principal formula is mapped to A in $\mathcal{R}$; let $\mathcal{B}_A$ be the subderivation of $\mathcal{D}$ ending with $\mathcal{I}_A$. To find a derivation $\mathcal{D}'$ and a subderivation $\mathcal{B}'$ such that $(\mathcal{B}') = eA$, let k be the number of formula-occurrences in $eA \setminus (\mathcal{B}_A)^-$: then there are also k inferences in $\mathcal{D}$ which must be successively permuted above $\mathcal{I}_A$. We proceed by induction on eA, as characterized by Proposition 2. We need to consider only the following cases:

$\downarrow$-step for *times*, clause (iv): $X \in eA$ and $X \neq A$ implies $X \otimes Y \in eA$. By induction hypothesis we may assume that X is introduced above $\mathcal{I}_A$. If $\mathcal{I}'$ introduces $X \otimes Y$ and occurs below $\mathcal{I}_A$, then X is a passive formula of every sequent between $\mathcal{I}_A$ and $\mathcal{I}'$. If we permute $\mathcal{I}'$ with the inference $\mathcal{I}''$ immediately above it, we do not increase the number of formulas in $eA \setminus (\mathcal{B})^-$, After a finite number of steps, the inference introducing $X \otimes Y$ is permuted above $\mathcal{I}_A$ and we have reduced k.

$\Downarrow$-step for *par* links, clause (v): $X \in eA, Y \in eA$ and $X \neq A \neq Y$ imply $X \wp Y \in eA$. By induction hypothesis we assume that both X and Y are introduced above $\mathcal{I}_A$, and let $\mathcal{I}'$ be the inference introducing $X \wp Y$ below $\mathcal{I}_A$. It follows that for each application of the $\otimes$-rule between $\mathcal{I}_A$ and $\mathcal{I}'$ the ancestors of $X \wp Y$ occur in one branch only, namely that containing $\mathcal{I}_A$. Therefore the inference $\mathcal{I}'$ can always be permuted with the inference $\mathcal{I}''$ immediately above it, even in the case when $\mathcal{I}''$ is a $\otimes$-rule. After a finite number of steps we reduce k.

Finally, to find a derivation $\mathcal{D}''$ and a subderivation $\mathcal{B}''$ such that $(\mathcal{B}'') = kA$, consider the doors of $k(A)$ which are premises of some link; let $X_1, \ldots, X_n$ be the conclusions of such links. Since $X_i \notin kA$ by Lemma 2, we have $A \in e(X_i)$ and by the above argument, the inference $\mathcal{I}_A$ can be permuted above the inference $\mathcal{I}_i$ introducing X_i in $\mathcal{D}$. The argument can be repeated for all $i \leq n$, without permuting $\mathcal{I}_A$ below a previously considered $\mathcal{I}_j$; the result follows. ■

3 Proof Nets for First Order $\mathbf{MLL}^{\perp}$

This section is essentially based on Girard [7].

3.1 First-Order Proof-Structures

We work with a *first-order* language for $\mathbf{MLL}^{-}$ and consider multiplicative proof-structures with the addition of the following links.

First-order links:

$$\textit{for all: } \frac{A}{\forall x.A} \qquad \textit{exists: } \frac{A[t/x]}{\exists x.A}$$

Definition 8. The variable x (possibly) occurring free in the premise of a *for all* link $\mathcal{L} : \dfrac{A}{\forall x.A}$ is called the *eigenvariable* associated with the link $\mathcal{L}$. Notice that the same variable x occurs free in the premise and bound in the conclusion of $\mathcal{L}$. We associate with each eigenvariable x a constant $\underline{x}$. Obviously, a link of the form $\dfrac{A[\underline{x}/x]}{\forall x.A}$ is *incorrect.*

Definitions 9. (i) A proof structure for *first order* $\mathbf{MLL}^{-}$ is defined as before with the addition of the following conditions:

3. (a) Each occurrence of a quantifier link uses a distinct bound variable.

   (b) If a variable occurs freely in some formula of the structure, then the variable is the eigenvariable of exactly one $\forall$-link.

   (c) The conclusions of the proof structure are closed formulas.

4. We say that in a first-order proof-structure $\mathcal{S}$ eigenvariables are used *strictly* if no substitution of any set of occurrences of an eigenvariable x with the constant $\underline{x}$ yields a correct proof structure with the same conclusions as $\mathcal{R}$. We require also that in first-order proof-structures eigenvariable are used strictly.[4]

(ii) Let $\mathcal{R}$ be a proof structure for $\mathbf{MLL}^-$ and let x be an eigenvariable in $\mathcal{R}$. The *free range of x in $\mathcal{S}$* is the set of all formula occurrences in which the eigenvariable x occurs freely. The *existential border* of x is the set of all the formula occurrences which are the conclusion of a link $\mathcal{L}$: $\dfrac{B[t/y]}{\exists y.B}$ where x occurs in the premise but not conclusion of $\mathcal{L}$. We say also that the link $\mathcal{L}$ is in the existential border of x.

(iii) We define the following additional reductions.

Symmetric Reductions

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ A[t/x]\end{matrix}}{\exists x.A} \qquad \dfrac{\begin{matrix}\mathcal{R}(x)\\ A^-\end{matrix}}{\forall x.A^-}}{cut} \quad \text{reduces to} \quad \dfrac{\begin{matrix}\vdots\\ A[t/x]\end{matrix} \qquad \begin{matrix}\mathcal{R}[t/x]\\ A^-[t/x]\end{matrix}}{cut}$$

where $\mathcal{R}(x)$ is the smallest substructure containing all occurrences of the eigenvariable x and $\mathcal{R}[t/x]$ results from $\mathcal{R}(x)$ by replacing t for x everywhere.

The definition of Danos-Regnier graph for first order proof structures is extended as follows.

Definitions 10. Let $\mathcal{R}$ be a proof structure for first order $\mathbf{MLL}^-$.

(i) A *Danos-Regnier switching s* in a first order proof structure $\mathcal{R}$ for $\mathbf{MLL}^-$ consists in a switch for each *par* and *for all* link of $\mathcal{R}$, where

- a switch for a *par* link is the choice of one of the premises of the link and

[4] We modify the setting of Girard [7] only with the condition of a strict use of the eigenvariables; this is enough to give a smooth tratment of kingdom and empires.

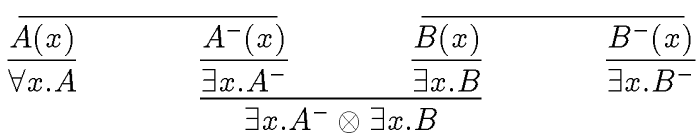
- a switch for a *for all* link with associate eigenvariable x is a choice of either (1) the premise of the link or of a formula occurrence in (2) the free range or in (3) the existential border of x (case (1) is needed if x does not occur free in $\mathcal{R}$).

(ii) Given a switching s for $\mathcal{R}$, we define the undirected *Danos-Regnier graph* $s(\mathcal{R})$ as follows:

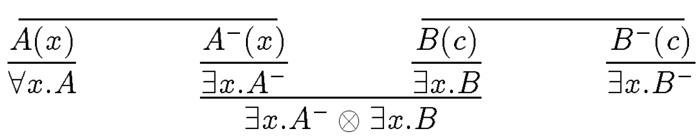
- the vertices of $s(\mathcal{R})$ are the formulas of $\mathcal{R}$;
- there is an edge between vertices X and Y exactly when:
  (a) X and Y are the conclusions of a logical axioms or the premises of a cut link;
  (b) X is a premise and Y the conclusion of a *times* or *exists* link;
  (c) Y is the conclusion of a *par* or *for all* link and X is the occurrence selected by the switching s.

(iii) $\mathcal{R}$ is a *proof net* for first order **DL** [$\mathbf{MLL}^-$] if for every switching s of $\mathcal{R}$, the graph $s(\mathcal{R})$ is acyclic [and connected].

The requirement that eigenvariable should be used strictly guarantees that the following structure is incorrect:



and must be rewritten as



where c is a new constant.

The following is an equivalent way of characterizing the same property.

Definition 11. An *x-tread* in a proof-structure $\mathcal{R}$ is a sequence $C_1, \ldots, C_n$ of formula occurrences which contain the free variable x and such that for each

$i < n$ there is a link $\mathcal{L}$ such that either (1) C_i is the premise and C_{i+1} is the conclusion of $\mathcal{L}$ or (2) C_i and C_{i+1} are conclusions of $\mathcal{L}$ (an axiom link) or (3) C_i is the conclusion and C_{i+1} is the premise of $\mathcal{L}$.

Fact 1. *In a proof structure eigenvariables are used strictly if and only if every occurrence of an eigenvariable x belongs to an x-thread ending with the $\forall$-link associated with x.* ■

3.2 Subnets

The definition of a *substructure* $\mathcal{S}_0$ of a proof-structure $\mathcal{S}$ must take into account the requirement that all conclusion of $\mathcal{S}_0$ should be closed formulas.

Definitions 12. (i) Let $\mathcal{S}$ be a proof structure for first order **MLL**. A set of formula occurrences and links $\mathcal{S}_0$ is a *substructure* of $\mathcal{S}$ if $\mathcal{S}_0$ is a proof structure and there is an injective map $\iota : \mathcal{S}_0 \to \mathcal{S}$ preserving links such that X and $\iota(X)$ are the same formula or X comes from $\iota(X)$ by a substitution of a free variable x with $\underline{x}$. (We will usually omit to mention the map ι.)
As before, a *subnet* is a substructure which satisfies the condition of proof-nets.

Fact 2. *If $\mathcal{S}$ is a substructure of a first order proof-structure $\mathcal{R}$ and a link $\mathcal{L} : \dfrac{A}{\forall x.A}$ occurs in $\mathcal{S}$, then the free range of x and its existential border are contained in $\mathcal{S}$.*

Proof. All eigenvariables are used strictly in $\mathcal{S}$ by definition. Suppose $\mathcal{L}$ occurs in $\mathcal{S}$ but x occurs outside $\mathcal{S}$; then there is an x-thread 'crossing the border of' $\mathcal{S}$, say at a door C. This means that any substitution of $\underline{x}$ for x in C spoils the link $\mathcal{L}$, i.e., $\mathcal{S}$ cannot be a substructure, a contradiction. ■

Lemma 1 (first order case) *In first order* $\mathbf{MLL}^-$, *the intersection and the union of subnets are subnets if and only if the intersection is nonempty.*

Proof. The argument for the propositional case applies here; we need only to make sure that if $\mathcal{R}_1$ and $\mathcal{R}_2$ are subnets of a proof-net $\mathcal{R}$ with $\mathcal{R}_1 \cap \mathcal{R}_2 \neq \emptyset$, then $\mathcal{S} = \mathcal{R}_1 \cup \mathcal{R}_2$ and $\mathcal{R}_0 = \mathcal{R}_1 \cap \mathcal{R}_2$ are *first-order substructures*, and in particular, the eigenvariables are used strictly and their conclusions are closed.
If a $\forall$-link of $\mathcal{R}$ does not occur in $\mathcal{S}$, then the associated eigenvariable z is replaced by $\underline{z}$ in the subnets $\mathcal{R}_1$ and in $\mathcal{R}_2$, hence in $\mathcal{S}$ too.
If a $\forall$-link with eigenvariable z occurs in $\mathcal{R}_0$, then (since eigenvariables are used strictly in $\mathcal{R}$) z also occurs inside $\mathcal{R}_0$ but not in any door of $\mathcal{R}_0$, by the Fact 2.
Finally, if a $\forall$ link with eigenvariable z occurs, say, in $\mathcal{R}_1 \setminus \mathcal{R}_2$, then any occurrence of z in the substructure $\mathcal{R}_0$ is replaced by $\underline{z}$. Moreover z does not

occur in the doors of $\mathcal{S}$: indeed by the same corollary, z does not occur in the doors of $\mathcal{R}_1$, hence it does not occur in $\mathcal{R}_2 \setminus \mathcal{R}_1$ either. ■

Proposition 1. (first order cases) *Let $\mathcal{R}_0$ be a substructure of the proof net $\mathcal{R}$. Then*
(iii)

$$\mathcal{S} = \mathit{For\ All}\,(\mathcal{R}_0) = \begin{array}{cc} & \mathcal{R}_0[x/\underline{x}] \\ \Gamma & \dfrac{A}{\forall x.A} \end{array}$$

is a subnet if only if $\mathcal{R}_0$ is a subnet and $\underline{x}$ does not occur in Γ.
(iv) *The substructure*

$$\mathcal{S} = \mathit{Exists}\,(\mathcal{R}_0) = \begin{array}{c} \mathcal{R}_0 \\ \dfrac{A[t/x]}{\exists x.A} \end{array}$$

is a subnet if $\mathcal{R}_0$ is one.

Proof. (iii) $\mathcal{S}$ is a substructure, since the substitution of x for $\underline{x}$ does not affect the conclusions of $\mathcal{S}$, which remain closed. Given a switching s for $\mathcal{S}$, $s\mathcal{S}$ differs from $s\mathcal{R}_0$ only for having a leaf $\forall x.A$ connected by an edge to some vertex of $\mathcal{R}_0$; thus $s\mathcal{S}$ is acyclic and connected, since $s\mathcal{R}_0$ is. (iv) is similar but easier. ■

Remark. It is not true that if $\mathcal{S} = \mathit{Exists}\ \mathcal{R}_0$ and $\mathcal{S}$ is a proof-net then $\mathcal{R}_0$ is a proof-net: for instance in $A[t/x]$ the term t may contain the eigenvariable of some *for all* link which occur in $\mathcal{R}_0$.

As before Theorem 1.(a) follows as a corollary. (Notice that if $\vdash \Gamma$ is the end sequent of $\mathcal{D}$ and a free variable x occurs in Γ, then $(\mathcal{D})^- = (\mathcal{D}[\underline{x}/x])^-$, a proof-structure with conclusions $\Gamma[\underline{x}/x]$.)

Theorem 1.(a) (first-order case) *Let $\mathcal{D}$ be a derivation in the sequent calculus for first order **MLL⁻**; then $(\mathcal{D})^-$ is a proof net.* ■

3.3 Empires and Kingdoms: Existence and Properties

As in the propositional case, we need to prove that given a proof-net $\mathcal{R}$ and a formula A in $\mathcal{R}$, *there always exists a subnet of $\mathcal{R}$ having A among its conclusions.*

Proposition 2. (Characterization of empires, first-order case; cf. [7]) *Let $\mathcal{R}$ be a proof net for first order* **MLL⁻** *and let A occur in $\mathcal{R}$. Then the empire eA of A in $\mathcal{R}$ exists and is characterized by the following equivalent conditions:*

(a) $\bigcap_s s(\mathcal{R}, A)$, *where s varies over all possible switchings;*

(b) *the smallest set of formula occurrences in* $\mathcal{R}$ *closed under conditions* (b)(i)-(v) *of Proposition 2 for propositional multiplicative links and moreover* (vi) if $\dfrac{X[t/y]}{\exists y.X}$ is a link in $\mathcal{S}$ and $X[t/y] \neq A$, then $\exists y.X \in e(A)$ if and only if $X[t/y] \in e(A)$, ($\uparrow$- and $\downarrow$-*steps*);

(vii) if $\dfrac{X}{\forall y.X}$ is a link in $\mathcal{S}$ and $X \neq A$, then $\forall y.X \in eA$ if and only if the free range of y and the occurrences in its existential border belong to eA ($\Uparrow$- and $\Downarrow$-*steps*).

Proof. We follow Girard [7]. (vii) Suppose $\forall y.X \in eA$, but for some C in the free range of y we have $C \notin eA$. Then A must be a premise of some link with conclusion Z, and for some s we have $\forall y.X \in s(\mathcal{R}, A)$ and $C \in \overline{s(\mathcal{R}, A)}$, where $\overline{s(\mathcal{R}, A)}$ is the connected component not containing A after removal of the edge (A, Z) from $s\mathcal{R}$. Therefore in $s(\mathcal{R}, A)$ there is a path connecting A and $\forall y.X$ and moreover in $\overline{s(\mathcal{R}, A)}$ there is a path connecting Z and C which obviously does not depend on the switch for $\forall y.X$. Now if we change the switch for $\forall y.X$ to choose C leaving all other choices unchanged, then we obtain a switch s' such that $s'\mathcal{R}$ is cyclic: indeed there still remains a connection between Z and C in $\overline{s'(\mathcal{R}, A)}$ (which lies outside eA) and there certainly is a distinct connection between A and $\forall y.X$ in $s'(\mathcal{R}, A)$ (since $\forall y.X \in eA$). But then $s'\mathcal{R}$ contains a cycle, a contradiction. ∎

The example at the beginning of the present section shows that an eigenvariable x can occur outside the kingdom of $\forall x.A$, unless a strict use of eigenvariables is required. We have the following *characterization of kingdoms in first order* **MLL**$^-$ (which is not true in in the setting of [7]).

Proposition 3. (Inductive definition of kingdoms, first-order cases) *Let* $\mathcal{R}$ *be a proof net for first order* ***MLL***$^-$*. Then kA, the kingdom of a in* $\mathcal{R}$ *exists and is characterized as the smallest set of formula occurrences closed under conditions* (i)-(iv) *of Proposition 3 for multiplicative propositional links and moreover*
(ii)' if $\dfrac{X[t/y]}{\exists y.X}$ is a link in $\mathcal{S}$ and $\exists y.X \in k(A)$, then $X[t/y] \in k(A)$, ($\uparrow$-*step*);

(v) if $\dfrac{X}{\forall y.X}$ is a link in $\mathcal{S}$ and $\forall y.X \in kA$, then the free range of y and the occurrences in its existential border belong to kA ($\Uparrow$-*step*). ∎

3.4 Sequentialization

The proof of Lemma 2 extends to the first-order case without modificatons.

Lemma 2. (Empire-Kingdom Nesting) *Let $\mathcal{L}_1 : \frac{\ldots A \ldots}{C}$ and $\mathcal{L}_2 : \frac{\ldots B \ldots}{D}$ be distinct links in a proof net $\mathcal{R}$. Suppose $B \in eA$; then $D \notin eA$ if and only if $C \in kD$.* ∎

Lemma 3. (Ordering of the kingdoms, first-order case) *In proof-nets for first order $\mathbf{MLL}^-$ the relation $\ll$ is a strict ordering of formula-occurrences that are not conclusions of axiom links.*

Proof. Suppose $X \in kY$, where X and Y not the conclusions of axioms links. Two cases are to be added to the propositional proof.

Let X be the conclusion of a link $\dfrac{A[t/x]}{\exists x.A}$. It follows from the definition of kingdom and proposition 1 that $kX = k(\exists x.A) = k(A[t/x]) \cup \{\exists x.A\}$. If X and Y are distinct and also $Y \in kX$, then $Y \in k(A[t/x])$ and this is absurd, since $Y \notin e(A[t/x])$ follows from $\exists x.A \in kY$ by lemma 2.

Finally, let X be the conclusion of a link $\dfrac{A}{\forall x.A}$. If follows from proposition 1 that $kX \setminus \{\forall x.A\} \subset eA$. If X and Y are distinct and also $Y \in kX$, then $Y \in eA$, and this contradicts lemma 2. ∎

Theorem 1.(b) *The Sequentialization Theorem holds in first order $\boldsymbol{MLL}^-$.*

Proof. We consider first the lowermost *par* and *for all* links, if such links exist. Otherwise, we choose a terminal link $\mathcal{L}$ whose conclusion is maximal w.r.t. $\ll$. If $\mathcal{L}$ is an *exists* link, then the result of removing it is still a proof-net. Suppose not; then $\mathcal{L}$: $\dfrac{A[t/x]}{\exists x.A}$ is in the existential border of y, where y is associated with $\dfrac{B}{\forall y.B}$ then $\exists x.A \in k(\forall y.B)$, by Fact 2, hence $\exists x.A$ it cannot be maximal w.r.t. $\ll$. The rest of the proof is as before. ∎

3.5 Permutability of Inferences in the Sequent Calculus

Counterexample. Let x occur free in P. The following is a derivation in MLL^- in which the applications of the $\exists$-rule and of the $\forall$-rule cannot be permuted.

$$\dfrac{\dfrac{\vdash P^-, P}{\vdash P^-, \exists x.P}\ \exists}{\vdash \forall x.P^-, \exists x.P}\ \forall$$

Theorem 2. (first order case) *The Theorem on permutability of inferences holds in first order* $\boldsymbol{MLL}^-$.

Proof. (i) Assuming the pure parameter property, the argument is similar to the propositional case, where *for all* rules behave like *par* rules and *exists* rules like *times* rules. The nontrivial case is the following: an inference $\mathcal{I}'_A$ of $\mathcal{D}'$ has the principal formula $A = \exists x.A_1$ and must be permuted below a *for all* rule $\mathcal{I}'_1$. As before we argue that in $\mathcal{D}$ we have an inference $\mathcal{I}_B$ such that $\mathcal{I}'_1$ and $\mathcal{I}_B$ are mapped to $B = \forall y.B_1$ and that such an inference must occur above the inference $\mathcal{I}_A$ whose active formula is $A_1[t/x]$; by the pure parameter property of $\mathcal{D}$, y does not occur in t, and the permutation is permissible.

(ii) As before, the argument is by induction on $eA \setminus (\mathcal{B}_A)^-$; to the propositional cases we add the following cases (the cases of existential links being unproblematic):

($\Uparrow$-step) *for all* link, clause (vii): By the pure parameter property the eigenvariables occur only above the associated $\forall$-inference, which already occurs above $\mathcal{I}_A$ by induction hypothesis.
($\Downarrow$-step) *for all* links, clause (vii): Let $\mathcal{I}'$ be the inference introducing $\forall y.X$ below $\mathcal{I}$, where $\forall y.X \in eA$. By induction hypothesis the eigenvariable y occurs only in sequents above $\mathcal{I}_A$, except for one occurrence of a formula $X(y)$ (an ancestor of $\forall y.X$) for each sequent between $\mathcal{I}_A$ and $\mathcal{I}'$. Hence we can always permute $\mathcal{I}'$ with the inference immediately above it. ∎

References

[1] G. Bellin. Mechanizing Proof Theory: Resource-Aware Logics and Proof-Transformations to Extract Implicit Information, Phd Thesis, Stanford University. Available as: Report CST-80-91, June 1990, Dept. of Computer Science, Univ. of Edinburgh.

[2] G. Bellin. Proof Nets for Multiplicative and Additive Linear Logic, Report LFCS-91-161, May 1991, Dept. of Computer Science, Univ. of Edinburgh.

[3] V. Danos and L. Regnier. The Structure of Multiplicatives, *Arch. Math. Logic* (1989) **28**, pp. 181-203.

[4] J. Gallier. Constructive Logics. Part II: Linear Logic and Proof Nets, preprint, Dept. of Computer and Information Science, University of Pennsylvania, 200 South 33rd St., Philadelphia, PA 19104, USA, Email: jean@saul.cis.upenn.edu

[5] J-Y. Girard. Linear Logic, *Theoretical Computer Science* **50**, 1987, pp. 1-102.

[6] J-Y. Girard. Quantifiers in Linear Logic, Proceedings of the SILFS conference held in Cesena, January 1987.

[7] J-Y. Girard. Quantifiers in linear logic II. Preprint, Équipe de Logique Mathématique, Université Paris VII, Tour 45-55. 5^e étage, 2, Place Jussieu, 75251 PARIS Cedex 05. France.

Gianluigi Bellin and Jacques van de Wiele
Équipe de Logique
Université de Paris VII
Tour 45-55, 5^e étage
2 Place Jussieu
75251 Paris Cedex 05
France