9

Constructive Logics. Part II: Linear Logic and Proof Nets

Jean Gallier

May 1991

Publication Notes

This work was done while the author was on sabbatical leave from the University of Pennsylvania at Digital PRL.

Abstract

The purpose of this paper is to give an exposition of material dealing with constructive logics, typed λ-calculi, and linear logic. The first part of this paper gives an exposition of background material (with the exception of the Girard-translation of classical logic into intuitionistic logic, which is new). This second part is devoted to linear logic and proof nets. Particular attention is given to the algebraic semantics (in Girard's terminology, phase semantics) of linear logic. We show how phase spaces arise as an instance of a Galois connection. We also give a direct proof of the correctness of the Danos-Regnier criterion for proof nets. This proof is based on a purely graph-theoretic decomposition lemma. As a corollary, we give an $O(n^2)$-time algorithm for testing whether a proof net is correct. Although the existence of such an algorithm has been announced by Girard, our algorithm appears to be original.

Résumé

Le but de cet article est de donner une présentation d'éléments de logique constructive, de lambda calcul typé, et de logique linéaire. Dans la première partie de cet article nous présentons les bases (à l'exception de la traduction de Girard de la logique classique en logique intuitionniste, qui est nouvelle). Dans cette deuxième partie sont traités la logique linéaire et les réseaux de preuves. Une attention particulière est faite à la sémantique algébrique (appelée dans la terminologie de Girard, sémantique des phases) de la logique linéaire. Nous montrons comment la notion d'espace de phases apparait comme une instance d'une connection de Galois. Nous donnons aussi une preuve directe de la correction du critère de Danos et Regnier pour les réseaux de preuves. Cette preuve repose sur un lemme de décomposition de pure théorie des graphes. Comme corollaire, nous obtenons un algorithme en temps $O(n^2)$ pour tester si un réseaux de preuves est correct. Bien que l'existence d'un tel algorithme ait été annoncée par Girard, notre algorithme semble être original.

Keywords

Natural deduction, lambda calculus, sequent calculus, linear logic.

Acknowledgements

I wish to thank Hassan Aït-Kaci and Andreas Podelski for their comments. Special thanks to Kathleen Milsted, Jean-Christophe Patat, and Ascánder Súarez, for proofreading earlier versions very carefully.

Contents

1 Core Linear Logic and Propositional Linear Logic

In Girard's linear logic [7], the connectives $\wedge$ and $\vee$ are split into two versions: the *multiplicative* version of $\wedge$ and $\vee$, denoted as $\otimes$ and $\parr$, and the *additive* version of $\wedge$ and $\vee$, denoted as & and $\oplus$. The constants $\top$ (truth) and $\bot$ (falsity) are also split into their multiplicative version **1** and $\bot$, and their additive version $\top$ and **0**. We confess having some difficulties remembering Girard's notation for the connectives and constants, and we propose to use the following notation which we find reasonably motivated semantically, and thus easier to memorize. The *multiplicative* version of $\wedge$ and $\vee$ is denoted as $\otimes$ (called *tensor*) and $\parr$ (called *par*), and the *additive* version of $\wedge$ and $\vee$ is denoted as & and $\oplus$. The constants $\top$ (truth) and $\bot$ (falsity) have their multiplicative version **I** and $\bot$, and their additive version **1** and **0**. We also have *linear implication*, denoted as $\multimap$ (which is a multiplicative), and *linear negation*, denoted as $^\bot$. For pedagogical reasons, we feel that it is preferable to present the inference rules of linear logic in terms of two-sided sequents $\Gamma \vdash \Delta$, with explicit rules for linear negation ($^\bot$). One can then show that negation is an involution satisfying De Morgan-like properties, and that every proposition is equivalent to another proposition in "negation normal form", in which negation only applies to atoms. Thus, it is possibe to describe linear logic in terms of one-sided sequents $\vdash \Delta$, and this is the approach originally followed by Girard [7]. The presentation using one-sided sequents also has the technical advantage of cutting down in half the number of cases to be considered in proving properties of the logic, cut elimination for example. On the other hand, the presentation using two-sided sequents is better suited if one is interested in the "intuitionistic fragment" of linear logic in which the righthand side Δ of a sequent $\Gamma \vdash \Delta$ contains at most one proposition.

Definition 1 *The axioms and inference rules of the system $\mathcal{L}in_0$ for core linear logic are given below.*

Axioms:

$$A \vdash A$$

$$\vdash \mathbf{I} \qquad\qquad \bot \vdash$$

$$\Gamma \vdash \Delta, \mathbf{1} \qquad\qquad \mathbf{0}, \Gamma \vdash \Delta$$

Cut Rule:

$$\frac{\Gamma \vdash A, \Delta \quad A, \Lambda \vdash \Theta}{\Gamma, \Lambda \vdash \Delta, \Theta} \quad \textit{(cut)}$$

Multiplicative Rules:

$$\frac{A, B, \Gamma \vdash \Delta}{A \otimes B, \Gamma \vdash \Delta} \quad (\otimes\text{: } \textit{left}) \qquad \frac{\Gamma \vdash \Delta, A \quad \Lambda \vdash \Theta, B}{\Gamma, \Lambda \vdash \Delta, \Theta, A \otimes B} \quad (\otimes\text{: } \textit{right})$$

$$\frac{A, \Gamma \vdash \Delta \quad B, \Lambda \vdash \Theta}{A \parr B, \Gamma, \Lambda \vdash \Delta, \Theta} \quad (\parr\text{: } \textit{left}) \qquad \frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \parr B} \quad (\parr\text{: } \textit{right})$$

$$\frac{\Gamma \vdash \Delta, A \quad B, \Lambda \vdash \Theta}{A \multimap B, \Gamma, \Lambda \vdash \Delta, \Theta} \ (\multimap\text{: } \textit{left}) \qquad \frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \multimap B} \ (\multimap\text{: } \textit{right})$$

$$\frac{\Gamma \vdash \Delta, A}{A^{\perp}, \Gamma \vdash \Delta} \ (^{\perp}\text{: } \textit{left}) \qquad \frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, A^{\perp}} \ (^{\perp}\text{: } \textit{right})$$

$$\frac{\Gamma \vdash \Delta}{\mathbf{I}, \Gamma \vdash \Delta} \ (\mathbf{I}\text{: } \textit{left}) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \perp} \ (\perp\text{: } \textit{right})$$

Additive Rules:

$$\frac{A, \Gamma \vdash \Delta}{A \,\&\, B, \Gamma \vdash \Delta} \ (\&\text{: } \textit{left}) \qquad \frac{B, \Gamma \vdash \Delta}{A \,\&\, B, \Gamma \vdash \Delta} \ (\&\text{: } \textit{left})$$

$$\frac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \,\&\, B} \ (\&\text{: } \textit{right})$$

$$\frac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \oplus B, \Gamma \vdash \Delta} \ (\oplus\text{: } \textit{left})$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \oplus B} \ (\oplus\text{: } \textit{right}) \qquad \frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \oplus B} \ (\oplus\text{: } \textit{right})$$

The fragment of linear logic involving the formulae, axioms, and rules, containing only the multiplicative connectives $\otimes$, $\parr$, $^{\perp}$, $\mathbf{I}$, and $\perp$, is called *multiplicative linear logic.*

From the above rules, it is clear (as in classical logic) that linear negation is involutive, *i.e.*, both $A \vdash A^{\perp\perp}$ and $A^{\perp\perp} \vdash A$ are provable, and that both $(A \multimap B) \vdash (A^{\perp} \parr B)$ and $(A^{\perp} \parr B) \vdash (A \multimap B)$ are provable. We also have the following "De Morgan" properties of linear negation over $\otimes, \parr$ on the one hand, and $\&, \oplus$ on the other hand, namely that the following sequents are provable:

$$\begin{array}{ll} (A \otimes B)^{\perp} \vdash A^{\perp} \parr B^{\perp}, & A^{\perp} \parr B^{\perp} \vdash (A \otimes B)^{\perp}, \\ (A \parr B)^{\perp} \vdash A^{\perp} \otimes B^{\perp}, & A^{\perp} \otimes B^{\perp} \vdash (A \parr B)^{\perp}, \\ (A \,\&\, B)^{\perp} \vdash A^{\perp} \oplus B^{\perp}, & A^{\perp} \oplus B^{\perp} \vdash (A \,\&\, B)^{\perp}, \\ (A \oplus B)^{\perp} \vdash A^{\perp} \,\&\, B^{\perp}, & A^{\perp} \,\&\, B^{\perp} \vdash (A \oplus B)^{\perp}. \end{array}$$

It is very easy to show that linear negation exchanges on the one hand $\mathbf{I}$ and $\perp$, and on the other hand $\mathbf{1}$ and $\mathbf{0}$, formally expressed by the provability of the following sequents:

$$\begin{array}{ll} \mathbf{I}^{\perp} \vdash \perp, & \perp \vdash \mathbf{I}^{\perp}, \\ \mathbf{1}^{\perp} \vdash \mathbf{0}, & \mathbf{0} \vdash \mathbf{1}^{\perp}. \end{array}$$

It is also useful to note that in writing sequents, the meaning of the comma (,) is overloaded. In a sequent $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$, on the lefthand side, the comma is an "uncommitted" $\otimes$, but on the righthand side, the commma is an "uncommitted" $\parr$. The difference between $\otimes$ and & is illustrated by the fact that the sequents

$$(A \multimap B) \,\&\, (A \multimap C) \vdash \big(A \multimap (B \,\&\, C)\big) \quad \text{and} \quad A \multimap B, A \multimap C \vdash \big((A \otimes A) \multimap (B \otimes C)\big)$$

are provable, but that the sequent $A \multimap B, A \multimap C \vdash \big(A \multimap (B \otimes C)\big)$ is *not* provable. The additive connectives require resource sharing, but the multiplicative disallow it.

Since contraction and weakening have been eliminated, core linear logic is not very expressive. In order to regain expressiveness, new formulae involving the exponentials ! (of course) and ? (why not) are introduced. Then, weakening and contraction are reintroduced, but in a controlled manner. The inference rules for the exponentials are given in the next definition. If $\Gamma = A_1, \ldots, A_n$, then $!\Gamma = !A_1, \ldots, !A_n$, and $?\Gamma = ?A_1, \ldots, ?A_n$.

Definition 2 *The rules for the exponentials are given below.*

$$\frac{A, \Gamma \vdash \Delta}{!A, \Gamma \vdash \Delta} \;\textit{(dereliction: left)} \qquad \frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, ?A} \;\textit{(dereliction: right)}$$

$$\frac{\Gamma \vdash \Delta}{!A, \Gamma \vdash \Delta} \;\textit{(weakening: left)} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, ?A} \;\textit{(weakening: right)}$$

$$\frac{!\Gamma, A \vdash ?\Delta}{!\Gamma, ?A \vdash ?\Delta} \;\textit{(?: left)} \qquad \frac{!\Gamma \vdash A, ?\Delta}{!\Gamma \vdash !A, ?\Delta} \;\textit{(!: right)}$$

$$\frac{!A, !A, \Gamma \vdash \Delta}{!A, \Gamma \vdash \Delta} \;\textit{(contraction: left)} \qquad \frac{\Gamma \vdash \Delta, ?A, ?A}{\Gamma \vdash \Delta, ?A} \;\textit{(contraction: right)}$$

The system $\mathcal{L}in_0^{!,?}$ for *propositional linear logic* is obtained from the system $\mathcal{L}in_0$ by adding the inference rules of Definition 2. We can show easily that linear negation exchanges ! and ?, in the sense that the following sequents are provable:

$$(!A)^\perp \vdash ?A^\perp \qquad ?A^\perp \vdash (!A)^\perp,$$
$$(?A)^\perp \vdash !A^\perp \qquad !A^\perp \vdash (?A)^\perp.$$

Using (?: *left*), (!: *right*), (*dereliction*: *left*), and (*dereliction*: *right*), it is easy to show that ! and ? are idempotent, in the sense that the following sequents are provable:

$$!!A \vdash !A \qquad !A \vdash !!A,$$
$$??A \vdash ?A \qquad ?A \vdash ??A.$$

The best way to understand linear negation is to think in terms of *action* and *reaction*, or (*output*, *answer*) and (*input*, *question*). Thus, an action of type A (answer of type A) corresponds to a reaction of type $A^{\perp}$ (question of type $A^{\perp}$). We can adopt the convention that an occurrence of a formula A on the lefthand side of a sequent $\Gamma \vdash \Delta$ corresponds to a reaction, or input (or question), and an occurrence of A on the righthand side of a sequent corresponds to an action, or output (or answer). Intuitiveley, the action $!A$ has the meaning that an action of type A is *reusable*, or can be duplicated as many times as necessary. It also corresponds to the idea of *storage*. Dually, the action $?A$ has the meaning that the action of type A can be *consumed* as many times as necessary. It also corresponds to the idea of *reading* from memory. The intuitive meaning of the rule

$$\frac{!\Gamma \vdash A,\ ?\Delta}{!\Gamma \vdash\ !A,\ ?\Delta} \quad (!\text{: } \textit{right})$$

is more easily grasped if we consider its intuitionistic version

$$\frac{!\Gamma \vdash A}{!\Gamma \vdash\ !A} \quad (!\text{: } \textit{right})$$

where $\Delta = \varnothing$. This rule says that since all inputs in $!\Gamma$ are reusable, and A is an output consequence of $!\Gamma$, then in fact, as many copies as needed of the action A can be output from $!\Gamma$. Thus, this corresponds to *storing* the action A in memory. Similarly, the intuitive meaning of the rule

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, ?A} \quad (\textit{dereliction}\text{: } \textit{right})$$

is that the action of type $?A$ is *read* (*retrieved*) from memory, the intuitive meaning of

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, ?A} \quad (\textit{weakening}\text{: } \textit{right})$$

is that the action of type $?A$ is *erased*, and the intuitive meaning of

$$\frac{\Gamma \vdash \Delta, ?A, ?A}{\Gamma \vdash \Delta, ?A} \quad (\textit{contraction}\text{: } \textit{right})$$

is that the action of type $?A$ is *duplicated*.

It is possible to prove the following sequents, showing a form of distributivity of ! over & and $\otimes$, and of ? over $\oplus$ and $\parr$.

Lemma 1 *The following sequents are provable*

$$?(A \oplus B) \vdash ?A \parr ?B \qquad ?A \parr ?B \vdash ?(A \oplus B),$$
$$!(A \,\&\, B) \vdash\ !A \otimes\ !B \qquad !A \otimes\ !B \vdash\ !(A \,\&\, B).$$

Remark: We can introduce a new connective, *linear equivalence*, denoted by the symbol $\circ\!\!-\!\!\circ$, and write the obvious inference rules for it. Alternatively, we can take the formula $A \circ\!\!-\!\!\circ B$ as an abbreviation for $(A \multimap B)$ & $(B \multimap A)$. Then, for example, the provability of the two sequents $?(A \oplus B) \vdash ?A \parr ?B$ and $?A \parr ?B \vdash ?(A \oplus B)$ can be written as the provability of the formula $?(A \oplus B) \circ\!\!-\!\!\circ (?A \parr ?B)$.

In view of the fact that linear negation is an involution, it is possible to give a more concise description of linear logic if we restrict ourselves to right-sided sequents, that is, sequents of the form $\vdash \Delta$. This is possible because the sequent $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$ is provable iff the sequent $\vdash A_1^\perp, \ldots, A_m^\perp, B_1, \ldots, B_n$ is provable. We can go further by taking advantage of the De Morgan properties noted earlier. Thus, we can write formulae in negation normal form, where negation is pushed in all the way so that it applies only to atomic formulae. In this formulation, negation is no longer a connective. We have *positive literals* of the form A where A is atomic, and *negative literals* of the form $A^\perp$ where A is atomic. We construct formulae using the connectives $\otimes$, $\parr$, &, $\oplus$, !, and ?, and we only need the contants $\perp$ and $\mathbf{1}$. We define $A \multimap B$ as an abbrevation for $A^\perp \parr B$, and the negation of a formula is defined inductively as follows:

$$
\begin{aligned}
\mathbf{I}^\perp &= \perp, \\
\perp^\perp &= \mathbf{I}, \\
\mathbf{1}^\perp &= \mathbf{0}, \\
\mathbf{0}^\perp &= \mathbf{1}, \\
(A)^\perp &= A^\perp, \quad \text{for } A \text{ a positive literal,} \\
(A^\perp)^\perp &= A, \quad \text{for } A^\perp \text{ a negative literal,} \\
(A \otimes B)^\perp &= A^\perp \parr B^\perp, \\
(A \parr B)^\perp &= A^\perp \otimes B^\perp, \\
(A \mathbin{\&} B)^\perp &= A^\perp \oplus B^\perp, \\
(A \oplus B)^\perp &= A^\perp \mathbin{\&} B^\perp, \\
(!A)^\perp &= ?A^\perp, \\
(?A)^\perp &= !A^\perp.
\end{aligned}
$$

The inference rules are immediately rewritten for right-sided sequents. The only minor difference is that (!: *right*) is now written as

$$\frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A} \quad (!\text{: } \textit{right})$$

2 Representing Intuitionistic Logic into Linear Logic

It is possible to represent Intuitionistic Logic into Linear Logic via the following translation.

Definition 3 *Given a formula A of propositional logic, its translation A^i in linear logic is defined as follows:*

$$\begin{aligned} A^i &= A \quad \textit{when } A \textit{ is atomic}, \\ (A \wedge B)^i &= A^i \,\&\, B^i, \\ (A \vee B)^i &= !A^i \oplus !B^i, \\ (A \supset B)^i &= !A^i \multimap B^i, \\ (\neg A)^i &= !A^i \multimap \mathbf{0}, \\ \bot^i &= \mathbf{0}. \end{aligned}$$

Given an intuitionistic sequent $A_1, \ldots, A_m \vdash B$, its translation is defined as the sequent $!A_1^i, \ldots, !A_m^i \vdash B^i$. This translation preserves intuitionistic provability and is conservative, as shown in the following lemma.

Lemma 2 *Given a sequent $\Gamma \vdash C$ of intuitionistic logic, if $\Gamma \vdash C$ is provable in $\mathcal{G}_i^{\supset,\wedge,\vee,\bot}$, then its translation $!\Gamma^i \vdash C^i$ is provable in linear logic $\mathcal{L}in_0^!$. Conversely, if the translation $!\Gamma^i \vdash C^i$ of a sequent $\Gamma \vdash C$ is provable in linear logic $\mathcal{L}in_0^{!,?}$, then $\Gamma \vdash C$ is provable in $\mathcal{G}_i^{\supset,\wedge,\vee,\bot}$.*

Proof. One needs to show that the translated version of the axioms and the inference rules of $\mathcal{G}_i^{\supset,\wedge,\vee,\bot}$ are provable in $\mathcal{L}in_0^!$, which is indeed the case. The point is that ! is added by the translation when necessary to allow weakening or contraction on the left, and this allows the simulation of the rules of $\mathcal{G}_i^{\supset,\wedge,\vee,\bot}$. The provability of the sequent $!(A \multimap B) \vdash !A \multimap !B$ is also needed. For the converse, there is a difficulty with the constant $\mathbf{0}$. If we consider the fragment not involving $\mathbf{0}$, we need to know that the cut elimination theorem holds for $\mathcal{L}in_0^{!,?}$, which was proved by Girard [7] (see also Lincoln, Mitchell, Scedrov, and Shankar [8]), and we simply need to observe that a cut-free proof of an intuitionistic sequent over $\multimap$, &, $\oplus$, and !, only involves intuitionistic sequents. Thus, such a proof yields an intuitionistic proof if we erase ! and replace the additive connectives by the standard connectives $\supset$, $\wedge$, $\vee$. A more complex argument is needed in order to handle $\mathbf{0}$ (see Schellinx [11]). □

Classical logic can also be represented in linear logic.

3 Representing Classical Logic into Linear Logic

Given a classical sequent $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$, we will consider that the occurrences of $B_1, \ldots, B_n$ are positive, and that the occurrences of $A_1, \ldots, A_m$ are negative. Consequently, the translation makes use of signed formulae of the form pA and nA. Given $\Gamma = A_1, \ldots, A_m$, then $p\Gamma = pA_1, \ldots, pA_m$, and $n\Gamma = nA_1, \ldots, nA_m$.

Definition 4 *Given a formula A of propositional logic, its translations pA^c and nA^c in linear logic are defined as follows:*

$$
\begin{aligned}
pA^c = nA^c &= A \quad \textit{when } A \textit{ is atomic},\\
(p\neg A)^c &= (nA^c)^{\perp},\\
(n\neg A)^c &= (pA^c)^{\perp},\\
(pA \wedge B)^c &= ?pA^c \ \& \ ?pB^c,\\
(nA \wedge B)^c &= nA^c \ \& \ nB^c,\\
(pA \vee B)^c &= pA^c \oplus pB^c,\\
(nA \vee B)^c &= !nA^c \oplus !nB^c,\\
(pA \supset B)^c &= (nA^c)^{\perp} \oplus pB^c,\\
(nA \supset B)^c &= !(pA^c)^{\perp} \oplus !nB^c.
\end{aligned}
$$

Given a classical sequent $\Gamma \vdash \Delta$, its translation is defined as the sequent $!n\Gamma^c \vdash ?p\Delta^c$, where $n\Gamma^c = nA_1^c, \ldots, nA_m^c$ if $\Gamma = A_1, \ldots, A_m$, and similarly for $p\Delta^c$. This translation preserves classical provability and is conservative, as shown in the following lemma.

Lemma 3 *Given a sequent $\Gamma \vdash \Delta$ of classical logic, if $\Gamma \vdash \Delta$ is provable in $\mathcal{G}_c^{\supset,\wedge,\vee,\neg}$, then its translation $!n\Gamma^c \vdash ?p\Delta^c$ is provable in linear logic $\mathcal{L}in_0^{!,?}$. Conversely, if the translation $!n\Gamma^c \vdash ?p\Delta^c$ of a sequent $\Gamma \vdash \Delta$ is provable in linear logic $\mathcal{L}in_0^{!,?}$, then $\Gamma \vdash \Delta$ is provable in $\mathcal{G}_c^{\supset,\wedge,\vee,\neg}$.*

Proof. One needs to show that the translated version of the axioms and the inference rules of $\mathcal{G}_c^{\supset,\wedge,\vee,\neg}$ are provable in $\mathcal{L}in_0^{!}$, which is indeed the case. The point is that ! and ? are added by the translation when necessary to allow weakening or contraction, and this allows the simulation of the rules of $\mathcal{G}_c^{\supset,\wedge,\vee,\neg}$. We also use the equivalences $?(A \oplus B) \multimap\!\circ\, (?A \parr ?B)$ and $!(A \ \& \ B) \multimap\!\circ\, (!A \otimes !B)$.

For the converse, we need the fact that the cut elimination theorem holds for $\mathcal{L}in_0^{!,?}$, which was proved by Girard [7] (see also Lincoln, Mitchell, Scedrov, and Shankar [8]). Then, we simply observe that a cut-free proof of the translation of a classical sequent only involves translations of classical sequents. Thus, such a proof yields a classical proof if we erase the connectives ! and ?, and replace the additive connectives and $^{\perp}$ by the standard connectives $\supset$, $\wedge$, $\vee$, $\neg$ (it is also necessary to simulate ($\oplus$: *right*) and (&: *left*) with the rules of $\mathcal{G}_c^{\supset,\wedge,\vee,\neg}$, but this is standard). □

Remark: The above proof shows that the following translation for $pA \wedge B$, $nA \vee B$, and $nA \supset B$, also works:

$$
\begin{aligned}
(pA \wedge B)^c &= ?pA^c \otimes ?pB^c,\\
(nA \vee B)^c &= !nA^c \parr !nB^c,\\
(nA \supset B)^c &= ?pA^c \multimap !nB^c.
\end{aligned}
$$

We now consider one of the possible semantics for linear logic, "phase semantics".

4 Closure Operations, Galois Connections, Adjunctions

Phase semantics due to Girard [7] is an algebraic semantics for linear logic. Actually, this semantics turns out to be an instance of a well known concept of lattice theory (Galois connections). We believe that phase semantics can be understood better if it is presented explicitly in terms of a Galois connection. Thus, we will begin by reviewing some basic notions of lattice theory, the notion of *closure operation* and the notion of *Galois connection* (see Birkhoff [3]). The relationship between phase semantics and Galois connections has been noted by Avron [2].

Definition 5 *Let I be a set. A function $^\dagger: 2^I \to 2^I$ is a closure operation on 2^I iff the following properties hold: For all $X, Y \subseteq I$,*

(1) $X \subseteq X^\dagger$;

(2) $X^{\dagger\dagger} \subseteq X^\dagger$;

(3) $X \subseteq Y$ implies $X^\dagger \subseteq Y^\dagger$.

From (1) and (2), it is clear that $X^{\dagger\dagger} = X^\dagger$. A set X is called *closed* iff $X^\dagger = X$. It is clear that X is closed iff $X = Y^\dagger$ for some Y. The set of closed subsets of I is denoted as $I^\dagger$.

Observe that the set $I^\dagger$ of closed subsets of I is closed under arbitrary intersections. Given a family $(A_j)_{j \in J}$ of closed sets in $I^\dagger$, since $\bigcap_{j \in J}\{A_j\} \subseteq A_j$ for every $j \in J$, by monotonicity (property (3) in Definition 5), we have $(\bigcap_{j \in J}\{A_j\})^\dagger \subseteq A_j^\dagger$ for every $j \in J$, which is equivalent to $(\bigcap_{j \in J}\{A_j\})^\dagger \subseteq A_j$, since $A_j^\dagger = A_j$ for every $j \in J$ because the A_j are closed subsets. Thus, $(\bigcap_{j \in J}\{A_j\})^\dagger \subseteq \bigcap_{j \in J}\{A_j\}$. The inclusion $\bigcap_{j \in J}\{A_j\} \subseteq (\bigcap_{j \in J}\{A_j\})^\dagger$ follows from condition (1).

Remark: If we drop condition (3) of Definition 5 and add the two conditions:

(0) $\varnothing^\dagger = \varnothing$, and

(3′) $(A \cup B)^\dagger = A^\dagger \cup B^\dagger$,

then we obtain one of the possible definitions of a *topology* (the Kuratowski closure axioms). Indeed, we can define the family of open sets of the topology as the complements of the closed subsets of I. One can also verify easily that (3′) implies (3).

The set $I^\dagger$ of closed subsets of I can be naturally given the structure of a complete lattice. For the (easy) proof, see Birkhoff [3].

Theorem 1 *Given a set I and a closure operation † on 2^I, if we define the operations $\bigvee$ and $\bigwedge$ on the set $I^\dagger$ of closed subsets of I by*

$$\bigwedge_{j \in J} \{A_j\} = \bigcap_{j \in J} \{A_j\}, \qquad \bigvee_{j \in J} \{A_j\} = (\bigcup_{j \in J} \{A_j\})^\dagger,$$

then $I^\dagger$ is a complete lattice under inclusion.

If † is a closure operation which is injective on singleton sets (*i.e.*, $\{x\}^\dagger \neq \{y\}^\dagger$ whenever $x \neq y$), then the mapping $x \mapsto \{x\}^\dagger$ is a natural embedding of I into the complete lattice of closed subsets. If I is equiped with a binary operation, say $\bullet$, then we define $XY = \{x \bullet y \mid x \in X,\ y \in Y\}$, and we extend $\bullet$ to the complete lattice $I^\dagger$ by defining $X \bullet Y = (XY)^\dagger$.

A way to define closure operations is via Galois connections.

Definition 6 *Let I and J be two sets and R be a binary relation on $I \times J$. Given any two subsets $X \subseteq I$ and $Y \subseteq J$, we define (with a slight ambiguity of notation) the sets $X^* \subseteq J$ and $Y^+ \subseteq I$ as follows:*

$$X^* = \{y \in J \mid \forall x \in X,\ xRy\},$$
$$Y^+ = \{x \in I \mid \forall y \in Y,\ xRy\}.$$

We have the following lemma showing that $*+$ is a closure operation on 2^I, and that $+*$ is a closure operation on 2^J. The proof can be found in Birkhoff [3].

Lemma 4 *Given a binary relation R on $I \times J$, the following properties hold: For all $X, X' \subseteq I$ and $Y, Y' \subseteq J$,*

(1) $X \subseteq X'$ implies $X'^* \subseteq X^*$ and $Y \subseteq Y'$ implies $Y'^+ \subseteq Y^+$;

(2) $X \subseteq X^{*+}$, $Y \subseteq Y^{+*}$, $X^{*+*} = X^*$, $Y^{+*+} = Y^+$;

(3) $*+$ and $+*$ are closure operations on 2^I and 2^J respectively. Furthermore, the mappings $X \mapsto X^*$ and $Y \mapsto Y^+$ define a dual isomorphism[1] between the complete lattices of closed subsets of I and J.

The dual isomorphisms $X \mapsto X^*$ and $Y \mapsto Y^+$ are called *polarities*, and they are said to define a *Galois connection* between I and J.

In particular, if $\leq$ is a partial order on $I = J$, by taking $R = \leq$, then $\dagger = *+$ is a closure operation. Note that for $X \subseteq I$, X^* is the set of upper bounds of X, denoted as *upper*(X),

[1] A dual isomorphism h between posets is a bijection which is anti-monotonic, *i.e.*, $a \leq b$ implies $h(b) \leq h(a)$.

X^+ is the set of lower bounds of X, denoted as *lower*(X), X^{*+} = *lower*(*upper*(X)), and $\{x\}^\dagger = \{x\}^{*+} = \{y \mid y \leq x\}$ (the principal ideal generated by x). The natural mapping $x \mapsto \{x\}^{*+}$ is an embedding of $\langle I, \leq \rangle$ into the complete lattice of closed subsets of I, and this embedding preserves all existings least upper bounds and greatest lower bounds (in fact, I is dense in this lattice). It is also called the "Mac Neille completion", or "completion by cuts". Furthermore, if $\sim$ is an involution on I, that is, $x = \sim\sim x$, and $x \leq y$ implies $\sim y \leq \sim x$ for all $x, y \in I$, then we can extend $\sim$ to $I^\dagger$ by defining

$$\sim X = \{\sim y \mid y \in X^*\}.$$

It is easily verified that we get an involution.

A particularly interesting case arises when $I = J$ and R is symmetric. In this case, $* = +$, and the closure operation is $\dagger = **$. Also, the operation on the set $I^\dagger = I^{**}$ of closed subsets defined by $X \mapsto X^*$ is an involution with some nice properties. We define $\mathbf{1} = \emptyset^* = I$, and $\mathbf{0} = I^* = \emptyset^{**}$. It is immediately verified that $\mathbf{1}$ is the greatest element of I^{**}, and that $\mathbf{0}$ is its least element.

Lemma 5 *Given a symmetric relation R on a set I, for any family $(A_j)_{j \in J}$ of closed sets in $I^\dagger = I^{**}$, we have*

$$(\bigcup_{j \in J} \{A_j\})^* = \bigcap_{j \in J} \{A_j^*\},$$
$$(\bigcap_{j \in J} \{A_j\})^* = (\bigcup_{j \in J} \{A_j^*\})^{**},$$
$$(\bigwedge_{j \in J} \{A_j\})^* = \bigvee_{j \in J} \{A_j^*\},$$
$$(\bigvee_{j \in J} \{A_j\})^* = \bigwedge_{j \in J} \{A_j^*\}.$$

Proof. We have

$$a \in (\bigcup_{j \in J} \{A_j\})^* \quad \text{iff}$$
$$\forall b (b \in (\bigcup_{j \in J} \{A_j\}) \supset aRb), \quad \text{iff}$$
$$\forall b \big(\exists j \in J\, (b \in A_j) \supset aRb\big), \quad \text{iff}$$
$$\forall j \in J\, \forall b \big(b \in A_j \supset aRb\big), \quad \text{iff}$$
$$\forall j \in J\, (a \in A_j^*), \quad \text{iff}$$
$$a \in \bigcap_{j \in J} \{A_j^*\}.$$

Since the A_j are closed we have $A_j^{**} = A_j$, and the second identity follows from the first by applying $*$ to both sides, and replacing each A_j by A_j^*. Since by definition,

$$\bigwedge_{j \in J} \{A_j\} = \bigcap_{j \in J} \{A_j\}, \qquad \bigvee_{j \in J} \{A_j\} = (\bigcup_{j \in J} \{A_j\})^{**},$$

the last two identities follow from the first two and the fact that $X^{***} = X^*$. □

If R is irreflexive, that is, $\forall x \in I \neg(xRx)$, then $X \wedge X^* = \emptyset$ and $X \vee X^* = I$. Indeed, $a \in X \cap X^*$ implies aRa, which shows that $X \wedge X^* = \emptyset$. The other equality follows by duality. If R is symmetric and we also have a binary operation $\bullet$ on I, we can extend $\bullet$ to I^{**} by defining $X \bullet Y = (XY)^{**}$. We also define $\parallel$ by $X \parallel Y = (X^* \bullet Y^*)^* = (X^*Y^*)^*$. We can immediately verify that $X \bullet Y = (X^* \parallel Y^*)^*$. We have the following useful properties.

Lemma 6 *Given a symmetric relation R on a set I and a binary operation $\bullet$ on I, then for any family $(A_j)_{j \in J}$ of closed sets in $I^\dagger = I^{**}$ and any $B \in I^\dagger$, we have*

$$\bigvee_{j \in J} \{(A_j \bullet B)\} = \big((\bigcup_{j \in J} \{A_j\})B\big)^{**}, \qquad \big(\bigvee_{j \in J} \{A_j\}\big) \bullet B = \big((\bigcup_{j \in J} \{A_j\})^{**} B\big)^{**},$$
$$\bigwedge_{j \in J} \{(A_j \parallel B)\} = \big((\bigcup_{j \in J} \{A_j^*\})B^*\big)^*, \qquad \big(\bigwedge_{j \in J} \{A_j\}\big) \parallel B = \big((\bigcup_{j \in J} \{A_j^*\})^{**} B^*\big)^*.$$

Proof. Using the fact that $X \parallel Y = (X^*Y^*)^*$ and that $\bigwedge_{j \in J}\{A_j\} = \bigcap_{j \in J}\{A_j\}$, we have

$$\begin{aligned}
&a \in \bigwedge_{j \in J} \{(A_j \parallel B)\} \quad \text{iff} \\
&a \in \bigcap_{j \in J} \{(A_j \parallel B)\}, \quad \text{iff} \\
&a \in \bigcap_{j \in J} \{(A_j^* B^*)^*\}, \quad \text{iff} \\
&\forall j \in J \big(a \in (A_j^* B^*)^*\big), \quad \text{iff} \\
&\forall j \in J\, \forall b (b \in A_j^* B^* \supset aRb), \quad \text{iff} \\
&\forall b \big(\exists j \in J (b \in A_j^* B^*) \supset aRb\big), \quad \text{iff} \\
&\forall b \big(b \in (\bigcup_{j \in J} \{A_j^*\})B^* \supset aRb\big), \quad \text{iff} \\
&a \in \big((\bigcup_{j \in J} \{A_j^*\})B^*\big)^*.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&a \in \big(\bigwedge_{j \in J} \{A_j\}\big) \parallel B \quad \text{iff} \\
&a \in \big((\bigcap_{j \in J} \{A_j\})^* B^*\big)^*, \quad \text{iff} \\
&a \in \big((\bigcup_{j \in J} \{A_j^*\})^{**} B^*\big)^*.
\end{aligned}$$

Using the fact that $X \bullet Y = (X^* \parallel Y^*)^*$ and that $(\bigwedge_{j \in J}\{A_j\})^* = \bigvee_{j \in J}\{A_j^*\}$ by Lemma 5, the first equality follows from the third, and the second one follows by unwinding the definitions $X \bullet Y = (XY)^{**}$ and $\bigvee_{j \in J}\{A_j\} = (\bigcup_{j \in J}\{A_j\})^{**}$. □

In general, we only have the inclusions

$$\bigvee_{j\in J}\{(A_j \bullet B)\} \subseteq (\bigvee_{j\in J}\{A_j\}) \bullet B, \qquad (\bigwedge_{j\in J}\{A_j\}) \parallel B \subseteq \bigwedge_{j\in J}\{(A_j \parallel B)\}.$$

Equality holds when R has additional properties. For example, this is the case when $pRq \bullet r$ holds iff $p \bullet qRr$ holds. For this, we need the following lemma which will also be useful later.

Lemma 7 *If the relation R is symmetric and $pRq \bullet r$ holds iff $p \bullet qRr$ holds, then*

$$p \in (X \bullet Y^*)^* \quad \textit{iff} \quad \forall q(q \in X \supset p \bullet q \in Y).$$

Proof. By the definitions, $p \in (X \bullet Y^*)^*$ iff $p \in (XY^*)^*$ iff $\forall u(u \in XY^* \supset pRu)$, iff

$$\forall u\big(\exists q \exists r(q \in X \wedge r \in Y^* \wedge u = q \bullet r) \supset pRu\big),$$

iff

$$\forall u\Big(\exists q \exists r\big(q \in X \wedge \forall t(t \in Y \supset rRt) \wedge u = q \bullet r\big) \supset pRu\Big),$$

iff

$$\forall u \forall q \forall r\Big(\big(q \in X \wedge \forall t(t \in Y \supset rRt) \wedge u = q \bullet r)\big) \supset pRu\Big),$$

iff

$$\forall q \forall r\Big(\big(q \in X \wedge \forall t(t \in Y \supset rRt)\big) \supset pRq \bullet r\Big).$$

Now assume that there is some q such that $q \in X$ but $p \bullet q \notin Y$. Letting $t = p \bullet q$ in the above formula, $(t \in Y \supset rRt)$ is trivially false, and thus, we have

$$\forall r(pRq \bullet r).$$

However, by the hypothesis, $pRq \bullet r$ holds iff $p \bullet qRr$ holds, and so $\forall r(p \bullet qRr)$ holds, that is, $p \bullet q \in I^* = \mathbf{0}$. But we know that $\mathbf{0}$ is the smallest element of I^{**}, and so $\mathbf{0} \subseteq Y$, which implies that $p \bullet q \in Y$, contradicting the assumption $p \bullet q \notin Y$. Thus, we have shown that if $p \in (X \bullet Y^*)^*$ then $\forall q(q \in X \supset pRq \in Y)$. The converse it easier to show. For every q and r, if we assume that

$$(q \in X \supset p \bullet q \in Y) \quad \text{and} \quad \big(q \in X \wedge \forall t(t \in Y \supset rRt)\big),$$

then by letting $t = p \bullet q$, we get $rRp \bullet q$, which is equivalent to $pRq \bullet r$, by symmetry of R and the fact that $pRq \bullet r$ holds iff $p \bullet qRr$ holds. □

Note that $(X \bullet Y^*)^*$ can be taken as the semantic definition of $X \multimap Y$, since in linear logic, $X \multimap Y$ is equivalent to $X^\perp \parr Y$. Thus, the fact that $p \in (X \bullet Y^*)^*$ iff $\forall q(q \in X \supset p \bullet q \in Y)$ should not be a total surprise to those who know about Kripke semantics.

Lemma 8 *If the relation R is symmetric, $\bullet$ has an identity 1, and $pRq \bullet r$ holds iff $p \bullet qRr$ holds, then for any family $(A_j)_{j \in J}$ of closed sets in $I^\dagger = I^{**}$ and any $B \in I^\dagger$, we have*

$$B \parallel (\bigwedge_{j \in J} \{A_j\}) = \bigwedge_{j \in J} \{(B \parallel A_j)\}, \qquad B \bullet (\bigvee_{j \in J} \{A_j\}) = \bigvee_{j \in J} \{(B \bullet A_j)\},$$
$$B \parallel \mathbf{1} = \mathbf{1}, \qquad B \bullet \mathbf{0} = \mathbf{0}.$$

Proof. By Lemma 7, $p \in (XY^*)^*$ iff $\forall q(q \in X \supset p \bullet q \in Y)$. Since $X \parallel Y = (X^*Y^*)^*$,

$$\begin{aligned}
&p \in B \parallel (\bigwedge_{j \in J} \{A_j\}) \quad \text{iff} \\
&p \in B \parallel (\bigcap_{j \in J} \{A_j\}), \quad \text{iff} \\
&\forall q\Big(q \in B^* \supset p \bullet q \in (\bigcap_{j \in J} \{A_j\})\Big), \quad \text{iff} \\
&\forall q\big(q \in B^* \supset \forall j \in J(p \bullet q \in A_j)\big), \quad \text{iff} \\
&\forall j \in J\, \forall q\big(q \in B^* \supset p \bullet q \in A_j\big), \quad \text{iff} \\
&\forall j \in J\big(p \in (B^* A_j^*)^*\big), \quad \text{iff} \\
&\forall j \in J\big(p \in (B \parallel A_j)\big), \quad \text{iff} \\
&p \in \bigcap_{j \in J} \{(B \parallel A_j)\}, \quad \text{iff} \\
&p \in \bigwedge_{j \in J} \{(B \parallel A_j)\}.
\end{aligned}$$

The special case where $J = \varnothing$ is handled easily, and yields $B \parallel \mathbf{1} = \mathbf{1}$ and $B \bullet \mathbf{0} = \mathbf{0}$. The other equality follows from duality. □

One should note that an argument symmetric to the one used in Lemma 7 shows that $p \in (X^*Y)^*$ iff $\forall q(q \in Y \supset q \bullet p \in X)$. Therefore, under the hypotheses of Lemma 8, we also obtain the following identities, *without* appealing to the commutativity of $\bullet$:

$$(\bigwedge_{j \in J} \{A_j\}) \parallel B = \bigwedge_{j \in J} \{(A_j \parallel B)\}, \qquad (\bigvee_{j \in J} \{A_j\}) \bullet B = \bigvee_{j \in J} \{(A_j \bullet B)\}.$$

Another important concept is that of an *adjunction.* The concept of adjunction is central in category theory (see MacLane [9]), but for our purposes, we only need to define it for partially ordered sets.

Definition 7 *Given two partially ordered sets $\langle A, \leq \rangle$ and $\langle B, \leq \rangle$, for any two monotonic functions $f\colon A \to B$ and $g\colon B \to A$, f is a left adjoint to g (and g is a right adjoint to f) iff for all $x \in A, y \in B$,*

$$f(x) \leq y \quad \textit{iff} \quad x \leq g(y).$$

First, observe that if a function f has a right adjoint g, then it must be unique, even if f and g are not monotonic.

Lemma 9 *If f has a right adjoint g, then g is unique, even if f and g are not monotonic. Furthermore, $g(y)$ is the greatest element of the set $\{x \in A \mid f(x) \leq y\}$, and $f(x)$ is the least element of the set $\{y \in B \mid x \leq g(y)\}$.*

Proof. Since $f(x) \leq y$ iff $x \leq g(y)$, for $x = g(y)$, we get $f(g(y)) \leq y$ iff $g(y) \leq g(y)$. Since $\leq$ is reflexive, $g(y) \leq g(y)$ always holds, and thus $f(g(y)) \leq y$ for all $y \in B$. Now, assume that g_1 and g_2 are two right adjoints of f. Since g_2 is a right adjoint of f, $f(x) \leq y$ iff $x \leq g_2(y)$. In particular, for $x = g_1(y)$, $f(g_1(y)) \leq y$ iff $g_1(y) \leq g_2(y)$. But since g_1 is also a right adjoint of f, we know that $f(g_1(y)) \leq y$ for all $y \in B$, and thus $g_1(y) \leq g_2(y)$ for all $y \in B$. The argument being symmetric, we also have $g_2(y) \leq g_1(y)$ for all $y \in B$, and by antisymmetry of $\leq$, we have $g_1(y) = g_2(y)$ for all $y \in B$. Consider the set $\{x \in A \mid f(x) \leq y\}$. Since $f(g(y)) \leq y$ for all $y \in B$, we have $g(y) \in \{x \in A \mid f(x) \leq y\}$. If $f(x) \leq y$, since g is a right adjoint of f, then $x \leq g(y)$, and thus $g(y)$ is an upper bound for the set $\{x \in A \mid f(x) \leq y\}$. Since $g(y)$ also belongs to this set, it is its greatest element. The case of $f(x)$ is treated in a similar fashion. □

Other properties of adjoints are given in the next lemma.

Lemma 10 *(i) Two monotonic functions $f\colon A \to B$ and $g\colon B \to A$ are adjoints iff $f(g(y)) \leq y$ and $x \leq g(f(x))$ for all $y \in B$, $x \in A$. (ii) When f and g are adjoints, then $f = fgf$, $g = gfg$, and f and g restrict to bijections between $\{a \in A \mid a = g(f(a))\}$ and $\{b \in B \mid b = f(g(b))\}$.*

Proof. (i) We have already shown in Lemma 9 that if f and g are adjoints, then $f(g(y)) \leq y$ for all $y \in B$ and $x \leq g(f(x))$ for all $x \in A$. Conversely, if we assume that $f(x) \leq y$, by monotonicity of g, we have $g(f(x)) \leq g(y)$, and since $x \leq g(f(x))$ holds, we get $x \leq g(y)$. If we assume that $x \leq g(y)$, then by monotonicity of f, we have $f(x) \leq f(g(y))$, and since $f(g(y)) \leq y$ holds, we get $f(x) \leq y$. Thus, f and g are adjoints. (ii) Since $x \leq g(f(x))$ holds, by monotonicity of f, we have $f(x) \leq f(g(f(x)))$. Since $f(g(y)) \leq y$ holds for all y, then $f(g(f(x))) \leq f(x)$. By antisymmetry, we get $f(x) = f(g(f(x)))$ for all $x \in A$. The proof of the other identity is similar, and the last part of (ii) follows easily. □

Another crucial property of left adjoints is that they preserve all existing lubs of A.

Lemma 11 *If two monotonic functions $f\colon A \to B$ and $g\colon B \to A$ are adjoints, then f preserves all lubs existing in A, and g preserves all glbs existing in B.*

Proof. Assume that $S \subseteq A$ and that $\bigvee S$ exists. By monotonicity of f, we have $f(x) \leq f(\bigvee S)$ for all $x \in S$, and thus $\bigvee\{f(x) \mid x \in S\} \leq f(\bigvee S)$. On the other hand, if $f(x) \leq b$ for all $x \in S$, since f and g are adjoints, we have $x \leq g(b)$ for all $x \in S$, and thus $\bigvee S \leq g(b)$. Using once again the fact that f and g are adjoints, we have $f(\bigvee S) \leq b$, which shows that $f(\bigvee S) = \bigvee\{f(x) \mid x \in S\}$. The argument for g is symmetric. □

Lemma 11 gives a necessary condition for the existence of adjoints. By Lemma 9, the value of $g(y)$ is the greatest element of the set $\{x \in A \mid f(x) \leq y\}$. Thus, if all lubs exist in A and f preserves all lubs, it seems likely that its right adjoint g exists. This fundamental fact is indeed true. In the case of (nondegenerate) categories, this fundamental theorem due to Peter Freyd is known as the "Adjoint Functor Theorem". The proof of the general theorem involves a technical condition know as the "solution set condition", but fortunately, in the case of posets, this condition is always satisfied (see MacLane [9]).

Lemma 12 *(Adjoint Functor Theorem, after Freyd) Let $\langle A, \leq \rangle$ and $\langle B, \leq \rangle$ be two partially ordered sets, and $f: A \to B$ a monotonic function. If all lubs exist in A and f preserves all lubs, then f has a right adjoint $g: B \to A$ given by $g(y) = \bigvee\{z \in A \mid f(z) \leq y\}$.*

Proof. We know from Lemma 9 that $g(y) = \bigvee\{z \in A \mid f(z) \leq y\}$ is the only possible candidate. It is immediately verified that such a g is monotonic. Since f preserves existing lubs, we have

$$f(g(y)) = f(\bigvee\{z \in A \mid f(z) \leq y\}) = \bigvee\{f(z) \in A \mid f(z) \leq y\} \leq y.$$

By the definition of $g(y)$, we also have $g(f(x)) = \bigvee\{z \in A \mid f(z) \leq f(x)\} \geq x$. Thus, $f(g(y)) \leq y$ and $x \leq g(f(x))$ for all $y \in B$, $x \in A$, which by Lemma 10 shows that f and g are adjoints. □

The notion of adjunction yields an interesting generalization of the concept of Galois connection that we now describe. First, we consider the concept of a closure operation in an arbitrary partially ordered set.

Definition 8 *Let $\langle A, \leq \rangle$ be a partially ordered set. A function $^\dagger: A \to A$ is a closure operation on A iff the following properties hold: For all $X, Y \in A$,*

(1) $X \leq X^\dagger$;

(2) $X^{\dagger\dagger} \leq X^\dagger$;

(3) $X \leq Y$ implies $X^\dagger \leq Y^\dagger$.

Note that Definition 5 corresponds to the special case where the poset A is some power set 2^I and the partial order is inclusion. Recalling that a binary relation R on $I \times J$ induces two functions $*: 2^I \to 2^J$ and $+: 2^J \to 2^I$ satisfying the properties of Lemma 4, we can define a Galois connection between two posets $\langle A, \leq \rangle$ and $\langle B, \leq \rangle$ as a pair $\langle *, + \rangle$ of functions such that $*: A \to B$ and $+: B \to A$ are order-reversing and such that $X \leq X^{*+}$ and $Y \leq Y^{+*}$ for all $X \in A$ and $Y \in B$. But then, in view of Lemma 10, this is almost equivalent to saying that $*$ and $+$ are adjoints. The reason this is not exactly correct is that $*$ and $+$ are order-reversing rather than being order-preserving, and the inequality $Y \leq Y^{+*}$ is in the wrong direction. We

can fix this problem easily. Given any poset $\langle A, \leq \rangle$, we define the dual poset $\langle A^{op}, \leq^{op} \rangle$ such that $A^{op} = A$ and $x \leq^{op} y$ iff $y \leq x$. Then, $*: A \to B^{op}$ and $+: B^{op} \to A$ are monotonic and $X \leq X^{*+}$ and $Y \leq Y^{+*}$ express that they are adjoints. Thus, we are led to the following definition (see Birkhoff [3] and MacLane [9]).

Definition 9 *Given two posets $\langle A, \leq \rangle$ and $\langle B, \leq \rangle$, two monotonic functions $*: A \to B^{op}$ and $+: B^{op} \to A$ form a Galois connection between A and B iff $*$ is a left adjoint to $+$, that is, for all $X \in A, Y \in B$,*

$$X^* \geq Y \quad \textit{iff} \quad X \leq Y^+.$$

The following generalization of Lemma 4 is immediate.

Lemma 13 *Given a Galois connection $\langle *, + \rangle$ between two posets A and B, for all $X \in A$ and $Y \in B$, the following properties hold:*

(1) $X \leq X^{*+}$, $Y \leq Y^{+*}$, $X^{*+*} = X^*$, $Y^{+*+} = Y^+$;

(2) $*+$ and $+*$ are closure operations on A and B respectively.

We can now apply the above considerations to the definition of the phase semantics. We begin with core linear logic.

5 Phase Semantics

We first define core Girard structures. These structures consist of a carrier equipped with two overlapping algebraic structures: a (commutative) monoid structure to interpret the multiplicatives, and a lattice structure to interpret the additives. Similar structures have been considred by Avron [2],

Definition 10 *A core Girard structure is a quintuple $\mathbf{D} = \langle D, \leq, \bullet, 1, \sim \rangle$, satisfying the following conditions:*

(1) $\langle D, \leq \rangle$ is a complete lattice;

(2) $\sim$ is an involution on D;

(3) $\langle D, \bullet, 1 \rangle$ is a commutative monoid with identity 1;

(4) The monoid operation $\bullet$ is monotonic in each of its arguments, i.e., if $a \leq a'$ and $b \leq b'$, then $a \bullet b \leq a' \bullet b'$.

(5) Defining $\|$ *such that* $a \,\|\, b = \sim (\sim a \bullet \sim b)$, *we have*

$a \bullet b \leq c$ *iff* $a \leq \sim b \,\|\, c$.

We can prove easily that the condition $a \bullet b \leq c$ iff $a \leq \sim b \,\|\, c$, is equivalent to the condition $a \leq b$ iff $1 \leq \sim a \,\|\, b$. Indeed, assuming that $a \bullet b \leq c$ iff $a \leq \sim b \,\|\, c$ holds, using the fact that 1 is an identity for $\bullet$, setting $a = 1$, we obtain $b \leq c$ iff $1 \leq \sim b \,\|\, c$. Conversely, assuming that $a \leq b$ iff $1 \leq \sim a \,\|\, b$ holds, we have $a \bullet b \leq c$ iff $1 \leq \sim (a \bullet b) \,\|\, c$, that is $a \bullet b \leq c$ iff $1 \leq (\sim a \,\|\sim b) \,\|\, c$. Since $\|$ is associative, this is equivalent to $a \bullet b \leq c$ iff $1 \leq \sim a \,\|\, (\sim b \,\|\, c)$. But we also have $a \leq \sim b \,\|\, c$ iff $1 \leq \sim a \,\|\, (\sim b \,\|\, c)$, and thus $a \bullet b \leq c$ iff $a \leq \sim b \,\|\, c$.

Letting $0 = \sim 1$, the condition $a \bullet b \leq c$ iff $a \leq \sim b \,\|\, c$ is also equivalent to the condition $a \leq b$ iff $a \bullet \sim b \leq 0$. This follows immediately from the fact that $\sim$ is an involution.

A *core Girard prestructure* is a core Girard structure where D is a lattice (not necessarily complete) having a greatest element denoted as **1** and a least element denoted as **0**, where $\bullet$ is monotonic in each of its arguments.

In a core Girard structure, it is immediately verified that 0 is an identity for $\|$, and that

$$\sim (\bigwedge_{j \in J} \{a_j\}) = \bigvee_{j \in J} \{\sim a_j\},$$
$$\sim (\bigvee_{j \in J} \{a_j\}) = \bigwedge_{j \in J} \{\sim a_j\}.$$

What is more interesting is the fact that $\bullet$ preserves arbitrary least upper bounds. This follows from the fact that $a \mapsto a \bullet b$ is a left adjoint of $a \mapsto \sim b \,\|\, a$.

Lemma 14 *Given a Girard structure* $\mathbf{D} = \langle D, \leq, \bullet, 1, \sim \rangle$, *for every family* $(a_j)_{j \in J}$ *of elements of* D, *for every* $b \in D$, *we have*

$$(\bigvee_{j \in J} \{a_j\}) \bullet b = \bigvee_{j \in J} \{(a_j \bullet b)\}, \qquad b \bullet (\bigvee_{j \in J} \{a_j\}) = \bigvee_{j \in J} \{(b \bullet a_j)\};$$

In particular, corresponding to the case $J = \emptyset$, *we have* $\mathbf{0} \bullet b = b \bullet \mathbf{0} = \mathbf{0}$.

Proof. First, we note that $\mathbf{1} = \sim \mathbf{0} \,\|\, \mathbf{0}$, the greatest element of D. Since **0** is the least element of D, for every $a \in D$ we have $\mathbf{0} \leq \sim a \,\|\, \mathbf{0}$. But $\mathbf{0} \leq \sim a \,\|\, \mathbf{0}$ iff $\mathbf{0} \bullet a \leq \mathbf{0}$, iff $a \bullet \mathbf{0} \leq \mathbf{0}$ (since $\bullet$ is commutative), iff $a \leq \sim \mathbf{0} \,\|\, \mathbf{0}$. Thus, $\mathbf{1} = \sim \mathbf{0} \,\|\, \mathbf{0}$. As a consequence, $a \bullet \mathbf{0} = \mathbf{0}$, since $a \bullet \mathbf{0} \leq \mathbf{0}$ iff $a \leq \sim \mathbf{0} \,\|\, \mathbf{0} = \mathbf{1}$, and **0** is the least element of D. Note that conditions (2) and (4) imply that $a \mapsto a \bullet b$ and $a \mapsto \sim b \,\|\, a$ are monotonic (for any b), and condition (5) implies that they are adjoint. Thus, by Lemma 11, $a \mapsto a \bullet b$ preserves least upper bounds. The other identities follow by commutativity of $\bullet$. □

In fact, it is possible to define an intuitionistic version of Girard structures which is interesting in its own right. Such structures were investigated by Abrusci [1], Ono [10], and Troelstra [12].

Definition 11 *A core intuitionistic Girard structure is a tuple* $\mathbf{D} = \langle D, \leq, \bullet, 1, 0, \multimap, \sim \rangle$, *satisfying the following conditions:*

(1) $\langle D, \leq \rangle$ *is a complete lattice with least element* $\mathbf{0}$ *and greatest element* $\mathbf{1}$*;*

(2) $\sim a = a \multimap 0$, *for every* $a \in D$ *(where* 0 *is a distinguished element of* D*);*

(3) $\langle D, \bullet, 1 \rangle$ *is a commutative monoid with identity element* 1*;*

(4) if $a \leq a'$ *and* $b \leq b'$, *then* $a \bullet b \leq a' \bullet b'$ *and* $a' \multimap b \leq a \multimap b'$*;*

(5) $a \bullet b \leq c$ *iff* $a \leq b \multimap c$.

A core intuitionistic Girard structure is *classical* iff $a = \sim\sim a$ for all $a \in D$. It will be shown below that core Girard structures as defined in Definition 10 and classical core intuitionistic Girard structures are equivalent. We also have the following properties.

Lemma 15 *The following properties hold for core intuitionistic Girard structures.*

(i) $\mathbf{1} = \mathbf{0} \multimap \mathbf{0}$ *is the greatest element of* D*;*

(ii) For every family $(a_j)_{j \in J}$ *of elements of* D, *for every* $b \in D$, *we have*

$$(\bigvee_{j \in J} \{a_j\}) \bullet b = \bigvee_{j \in J} \{(a_j \bullet b)\}, \qquad b \bullet (\bigvee_{j \in J} \{a_j\}) = \bigvee_{j \in J} \{(b \bullet a_j)\};$$

In particular, corresponding to the case $J = \emptyset$, *we have* $\mathbf{0} \bullet b = b \bullet \mathbf{0} = \mathbf{0}$.

(iii) $a \multimap (b \multimap c) = (a \bullet b) \multimap c$*;*

(iv) For a classical structure, $a \multimap b = \sim (a \bullet \sim b)$, $0 = \sim 1$, *and* $a \vee b = \sim (\sim a \wedge \sim b)$.

Proof. (i) Since $a \bullet b \leq c$ iff $a \leq b \multimap c$ and $\mathbf{0}$ is the least element of D, we have for every $a \in D$, $\mathbf{0} \leq a \multimap \mathbf{0}$, iff $\mathbf{0} \bullet a \leq \mathbf{0}$, iff $a \bullet \mathbf{0} \leq \mathbf{0}$ (by commutativity of $\bullet$), iff $a \leq \mathbf{0} \multimap \mathbf{0}$. Thus, $\mathbf{1} = \mathbf{0} \multimap \mathbf{0}$. (ii) Note that condition (4) of Definition 11 expresses that $\bullet\colon D \times D \to D$ and $\multimap\colon D^{op} \times D \to D$ are monotonic (where D^{op} is equipped with the order $\leq^{op}$ such that $x \leq^{op} y$ iff $y \leq x$), and that (5) says that $x \mapsto x \bullet y$ is left adjoint to $x \mapsto y \multimap x$. By Lemma

11, $x \mapsto x \bullet y$ preserves least upper bounds. The other identities follow by commutativity of $\bullet$. (iii) $u \leq a \multimap (b \multimap c)$ iff $u \bullet a \leq b \multimap c$ iff $u \bullet a \bullet b \leq c$ iff $u \leq (a \bullet b) \multimap c$. (iv)

$$\begin{aligned} \sim (a \ \bullet\!\!\sim b) &= (a \ \bullet\!\!\sim b) \multimap 0 \\ &= a \multimap (\sim b \multimap 0) && \text{(by (iii))} \\ &= a \multimap (\sim\!\sim b) && \text{since } \sim x = x \multimap 0 \\ &= a \multimap b && \text{since } b = \sim\!\sim b. \end{aligned}$$

In particular, $\sim 1 = 1 \multimap 0 = \sim (1 \ \bullet\!\!\sim 0) = \sim\!\sim 0 = 0$, and thus $0 = \sim 1$. From condition (4) of Definition 11, $x \leq y$ implies that $\sim y \leq \sim x$. Since we also have $\sim\!\sim x = x$, $\sim$ is an involution, and $a \vee b = \sim (\sim a \wedge \sim b)$ follows. □

One can also show as an easy exercise that condition (4) of Definition 11 can be replaced by the identity

$$a \bullet (b \vee c) = (a \bullet b) \vee (a \bullet c).$$

We observed in the proof of Lemma 15 that $\bullet\colon D \times D \to D$ and $\multimap\colon D^{op} \times D \to D$ are monotonic, and that (5) says that $x \mapsto x \bullet y$ is left adjoint to $x \mapsto y \multimap x$. It is possible to develop categorical semantics for linear logic inspired by these observations. We now return to (classical) core linear logic.

We can interpret formulae of core linear logic as follows. Given any mapping v, called a *valuation*, assigning some element $v(P) \in D$ to every atomic symbol P, we extend v to formulae inductively as follows:

Definition 12 *Given a core Girard (pre)structure* **D**, *a valuation v is extended to formulae as follows:*

$$\begin{aligned} v(\mathbf{I}) &= 1, \\ v(\bot) &= 0, \\ v(\mathbf{1}) &= \mathbf{1}, \\ v(\mathbf{0}) &= \mathbf{0}, \\ v(A^{\bot}) &= \sim v(A), \\ v(A \otimes B) &= v(A) \bullet v(B), \\ v(A \parr B) &= v(A) \parallel v(B), \\ v(A \ \& \ B) &= v(A) \wedge v(B), \\ v(A \oplus B) &= v(A) \vee v(B), \end{aligned}$$

where $\wedge$ and $\vee$ are the lattice operations on D. Note that the fact that D is complete is not needed for this definition to make sense, just the existence of a least and a greatest element.

Given a sequent $\Gamma \vdash \Delta$ where $\Gamma = A_1, \ldots, A_m$ and $\Delta = B_1, \ldots, B_n$, we define

$$v(\Gamma \vdash \Delta) = \sim v(A_1) \parallel \cdots \parallel \sim v(A_m) \parallel v(B_1) \parallel \cdots \parallel v(B_n).$$

The set $T_{\mathbf{D}} = \{a \in D \mid 1 \leq a\}$ is called a *truth subset* of **D**. Given a sequent $\Gamma \vdash \Delta$, we say that v *satisfies* $\Gamma \vdash \Delta$ *in* **D** iff $v(\Gamma \vdash \Delta) \in T_{\mathbf{D}}$, *i.e.*, $1 \leq v(\Gamma \vdash \Delta)$. If $\Gamma = A_1, \ldots, A_m$ and $\Delta = B_1, \ldots, B_n$, then $1 \leq v(\Gamma \vdash \Delta)$ is equivalent to

$$v(A_1) \bullet \ldots \bullet v(A_m) \leq v(B_1) \parr \cdots \parr v(B_n),$$

or to

$$v(A_1) \bullet \ldots \bullet v(A_m) \ \bullet\!\!\sim v(B_1) \ \bullet \ldots \bullet\!\!\sim v(B_n) \leq 0.$$

In the special case $m = 0$, the condition $1 \leq v(\vdash \Delta)$ is equivalent to

$$1 \leq v(B_1) \parr \cdots \parr v(B_n),$$

and in the special case $n = 0$, the condition $1 \leq v(\Gamma \vdash)$ is equivalent to

$$v(A_1) \bullet \ldots \bullet v(A_m) \leq 0.$$

The condition $1 \leq v(\Gamma \vdash \Delta)$ is also denoted as $\mathbf{D} \models (\Gamma \vdash \Delta)[v]$. We say that $\Gamma \vdash \Delta$ *is valid in* **D**, denoted as $\mathbf{D} \models \Gamma \vdash \Delta$, iff $\mathbf{D} \models (\Gamma \vdash \Delta)[v]$ for every v, and finally we say that $\Gamma \vdash \Delta$ is *universally valid*, denoted as $\models \Gamma \vdash \Delta$, iff $\mathbf{D} \models \Gamma \vdash \Delta$ for all **D**. If we consider sequents of the special form $\vdash A$ where A is a formula, we obtain the notion of satisfaction, validity, and universal vality, for formulae. A universal formula is also called a *linear tautology*.

The soundness of the interpretation defined above is easily shown.

Lemma 16 *If $\Gamma \vdash \Delta$ is provable in linear logic, then for every core Girard (pre)structure* **D** *and every valuation v, $\mathbf{D} \models (\Gamma \vdash \Delta)[v]$. As a corollary, $\Gamma \vdash \Delta$ is valid.*

Proof. The verification proceeds by induction on proof trees. It amounts to checking the soundness of the axioms and of the proof rules. We check only a few cases, as the verification is straightforward. Consider the rule

$$\frac{\Gamma \vdash \Delta, A \quad \Lambda \vdash \Theta, B}{\Gamma, \Lambda \vdash \Delta, \Theta, A \otimes B} \quad (\otimes\text{: } \textit{right})$$

Thus, we can assume that $1 \leq v(\Gamma \vdash \Delta, A)$ and $1 \leq v(\Lambda \vdash \Theta, B)$. By (5) and Definition 12, this is equivalent to

$$v(\Gamma) \bullet v(\Delta^{\perp}) \leq v(A), \quad \text{and} \quad v(\Lambda) \bullet v(\Theta^{\perp}) \leq v(B),$$

where $v(\Gamma) = v(A_1) \bullet \ldots \bullet v(A_m)$ if $\Gamma = A_1, \ldots, A_m$, and $v(\Delta^{\perp}) = \sim v(B_1) \ \bullet \ldots \bullet\!\!\sim v(B_n)$ if $\Delta = B_1, \ldots, B_n$. By monotonicity of $\bullet$, we have

$$v(\Gamma) \bullet v(\Lambda) \bullet v(\Delta^{\perp}) \bullet v(\Theta^{\perp}) \leq v(A) \bullet v(B),$$

that is

$$v(\Gamma, \Lambda) \bullet v(\Delta^{\perp}, \Theta^{\perp}) \leq v(A \otimes B),$$

which means that

$$1 \leq v(\Gamma, \Lambda \vdash \Delta, \Theta, A \otimes B).$$

Consider the rule

$$\frac{A, B, \Gamma \vdash \Delta}{A \otimes B, \Gamma \vdash \Delta} \quad (\otimes\text{: } \textit{left})$$

By hypothesis, $1 \leq v(A, B, \Gamma \vdash \Delta)$. By (5), this is equivalent to

$$v(A) \bullet v(B) \bullet v(\Gamma) \bullet v(\Delta^{\perp}) \leq 0,$$

that is

$$v(A \otimes B) \bullet v(\Gamma) \bullet v(\Delta^{\perp}) \leq 0,$$

which means that

$$1 \leq v(A \otimes B, \Gamma \vdash \Delta).$$

Consider the cut rule

$$\frac{\Gamma \vdash A, \Delta \quad A, \Lambda \vdash \Theta}{\Gamma, \Lambda \vdash \Delta, \Theta} \quad (\textit{cut})$$

By assumption, we have $1 \leq v(\Gamma \vdash A, \Delta)$ and $1 \leq v(A, \Lambda \vdash \Theta)$. By (5) and Definition 12, this is equivalent to

$$v(\Gamma) \bullet v(\Delta^{\perp}) \leq v(A), \quad \text{and} \quad v(\Lambda) \bullet v(\Theta^{\perp}) \leq \sim v(A).$$

By monotonicity of $\bullet$, we have

$$v(\Gamma) \bullet v(\Lambda) \bullet v(\Delta^{\perp}) \bullet v(\Theta^{\perp}) \leq v(A) \ \bullet\!\sim v(A).$$

However, from $a \leq a$, we have $a \ \bullet\!\sim a \leq 0$, and so

$$v(\Gamma) \bullet v(\Lambda) \bullet v(\Delta^{\perp}) \bullet v(\Theta^{\perp}) \leq 0,$$

that is

$$v(\Gamma, \Lambda) \bullet v(\Lambda^{\perp}, \Theta^{\perp}) \leq 0,$$

which means that

$$1 \leq v(\Gamma, \Lambda \vdash \Delta, \Theta).$$

The case of the additives follows from the fact that $\wedge$ corresponds to greatest lower bound and $\vee$ corresponds to least upper bound. □

Note that the fact that D is complete is not used anywhere in the proof. We now turn to Girard's phase structures [7], and show their equivalence with core Girard structures.

Definition 13 *A phase structure* $\mathbf{P}$ *is a quadruple* $\langle P, \bullet, 1, \perp \rangle$*, where*

(1) $\langle P, \bullet, 1 \rangle$ *is a commutative monoid with identity* 1*;*

(2) $\perp$ *is a distinguished subset of* P*, the set of antiphases.*

The set P is called the set of *phases*.

Definition 14 *Given a phase structure* $\mathbf{P}$*, for any subset* X *of* P*, its dual* $X^{\perp}$ *is defined by*

$$X^{\perp} = \{p \in P \mid \forall q \in X,\ p \bullet q \in \perp\}.$$

A subset X *of* P *such that* $X = X^{\perp\perp}$ *is called a fact. Observe that* $\perp = \{1\}^{\perp}$*. We define* $\mathbf{I} = \perp^{\perp} = \{1\}^{\perp\perp}$, $\mathbf{1} = \emptyset^{\perp} = P$, *and* $\mathbf{0} = \mathbf{1}^{\perp}$.

We can now establish the connection with closure operations. Given a phase structure $\mathbf{P}$, if we define the binary relation R on P such that

$$xRy \quad \text{iff} \quad x \bullet y \in \perp,$$

then we have a Galois connection such that

$$X^{*} = X^{+} = \{p \in P \mid \forall q \in X,\ p \bullet q \in \perp\} = X^{\perp},$$

and by Lemma 4, $X \mapsto X^{\perp\perp}$ is a closure operation. By Theorem 1, the set of facts, *i.e.*, the set $P^{\dagger}$ of closed subsets of P, is a complete lattice. It is immediately verified that $\mathbf{1} = P$ is the greatest element of $P^{\dagger}$, and that $\mathbf{0}$ is its least element. The operation $\bullet$ can be extended to $P^{\dagger}$ and we can define an involution $\sim$ on $P^{\dagger}$ by setting

$$X \otimes Y = (XY)^{\perp\perp}, \qquad \sim X = X^{\perp}.$$

It should be noted that in order for $^{\perp}$ to be an involution, that is, to have $X^{*} = X^{+} = X^{\perp}$, it is not actually required that $\bullet$ be commutative. What we need is that R be symmetric, which holds iff $\perp$ satisfies the following property:

$$x \bullet y \in \perp \quad \text{iff} \quad y \bullet x \in \perp\ .$$

Abrusci [1] calls such a $\perp$ *cyclic*. Obviously, $\perp$ is cyclic when $\bullet$ is commutative. When $\perp$ is cyclic but $\bullet$ is not commutative, Abrusci calls the corresponding structure a *cyclic classical phase space* [1] (as opposed to a *commutative classical phase space*). We have not found yet situations where the more general condition of cyclicity of $\perp$ is preferable to the commutativity of $\bullet$. Thus, from now on, we assume $\bullet$ to be commutative. However, noncommutative phase spaces are interesting since they lead to noncommutative linear logic, investigated by Absrusci (among others).

When $\bullet$ is commutative, it is immediately verified that $\langle P^{\dagger}, \otimes, \mathbf{I}\rangle$ is a commutative monoid with $\mathbf{I}$ as its identity. If we define $X \parr Y = (X^{\perp} \otimes Y^{\perp})^{\perp} = (X^{\perp}Y^{\perp})^{\perp}$, then we also have a monoid structure $\langle P^{\dagger}, \parr, \perp\rangle$ with $\perp$ as its identity. The lattice operations on $P^{\dagger}$ are defined as in Theorem 1, but it will be convenient to regroup all these definitions:

$$X \otimes Y = (XY)^{\perp\perp}, \qquad X \parr Y = (X^{\perp}Y^{\perp})^{\perp},$$
$$X \wedge Y = X \cap Y, \qquad X \vee Y = (X \cup Y)^{\perp\perp}.$$

Thus, $P^{\dagger}$ is practically a core Girard structure. For this, we need a lemma.

Lemma 17 *Given a phase structure* **P**, *the following properties hold: (1) For any two facts* $X, Y \subseteq P$, *we have* $X \subseteq Y$ *iff* $X \otimes Y^{\perp} \subseteq \perp$. *(2) the operation* $\otimes$ *is monotonic in each argument (in fact,* $\otimes$ *preserves arbitrary least upper bounds).*

Proof. In order to prove (1), we first apply Lemma 7 to the relation R defined such that xRy iff $x \bullet y \in \perp$. Therefore, we have $p \in (X \otimes Y^{\perp})^{\perp}$ iff $\forall q(q \in X \supset p \bullet q \in Y)$.

In view of the above equivalence, $p \in X \otimes Y^{\perp}$ iff $p \in (X \otimes Y^{\perp})^{\perp\perp}$ iff

$$\forall q(q \in (X \otimes Y^{\perp})^{\perp} \supset p \bullet q \in \perp),$$

iff

$$\forall q\big(\forall r(r \in X \supset q \bullet r \in Y) \supset p \bullet q \in \perp\big).$$

This means that $X \otimes Y^{\perp} \subseteq \perp$ is equivalent to

$$\forall p\Big(\forall q\big(\forall r(r \in X \supset q \bullet r \in Y) \supset p \bullet q \in \perp\big) \supset p \in \perp\Big). \qquad (a)$$

Now, observe that if $\perp = P$, then $X^{\perp} = P$ for every $X \subseteq P$, and then all facts are equal to P. In this degenerated case, (1) holds trivially. Thus, we can assume that there is some $p \in P$ such that $p \notin \perp$. Assume that

$$\forall q\big(\forall r(r \in X \supset q \bullet r \in Y) \supset p \bullet q \in \perp\big)$$

holds. In particular, we can pick $q = 1$, and assume that

$$\forall r(r \in X \supset r \in Y) \supset p \in \perp$$

holds. Also assume that there is some r such that $r \in X$ but $r \notin Y$. Since $(r \in X \supset r \in Y)$ is false, the implication

$$\forall r(r \in X \supset r \in Y) \supset p \in \perp$$

holds trivially, and from (a), this implies that $p \in \perp$, contradicting the choice of p. Thus, $X \otimes Y^{\perp} \subseteq \perp$ implies that $X \subseteq Y$. Conversely, assume that $X \subseteq Y$ holds. For every p, if

$$\forall q\big(\forall r(r \in X \supset q \bullet r \in Y) \supset p \bullet q \in \perp\big)$$

holds, then this holds for $q = 1$, and since $\forall r(r \in X \supset r \in Y)$ also holds, we conclude than $p \in \perp$, establishing that $X \otimes Y^{\perp} \subseteq \perp$ holds. This concludes the proof of (1). Property (2) follows from Lemma 8. In fact, by Lemma 11, the preservation of least upper bounds is also a consequence of property (1) just proved above. □

Putting things together, we have the following lemma showing that every phase structures gives rise to a core Girard structure.

Lemma 18 *Given a phase structure* $\mathbf{P} = \langle P, \bullet, 1, \perp\rangle$, *if we define* $X \otimes Y = (XY)^{\perp\perp}$ *and* $\mathbf{I} = \perp^{\perp}$, *then* $\mathbf{D} = \langle P^{\perp\perp}, \subseteq, \otimes, \mathbf{I}, ^{\perp}\rangle$ *is a core Girard structure, the lattice operations being defined by* $X \wedge Y = X \cap Y$ *and* $X \vee Y = (X \cup Y)^{\perp\perp}$.

Proof. This follows from Lemma 17 and the fact that $^{\perp\perp}$ is a closure operation. □

Girard defines validity in a phase structure almost as we did in Definition 12, but in terms of valuations into the set of facts of P, and $\mathbf{P} \models A[v]$ holds iff $1 \in v(A)$ (see Girard [7]). Recall that $\mathbf{I} = \{1\}^{\perp\perp}$. Thus, given any fact X, if $1 \in X$ then $\{1\} \subseteq X$, which implies $\{1\}^{\perp\perp} \subseteq X^{\perp\perp}$, that is $\mathbf{I} \subseteq X$, since X is a fact ($X = X^{\perp\perp}$). Conversely, if $\mathbf{I} \subseteq X$, since $\mathbf{I} = \{1\}^{\perp\perp}$, then $1 \in X$. Thus, for a fact X, we have $1 \in X$ iff $\mathbf{I} \subseteq X$. This establishes the equivalence of Girard's notion of validity in terms of phase structures and the notion given in Definition 12.

Interestingly, every core Girard structure arises from a phase structure, as shown in the following lemma.

Lemma 19 *Given a core Girard structure* $\mathbf{D} = \langle D, \leq, \bullet, 1, \sim \rangle$, *if we define the set* $\perp$ *by* $\perp = \{x \in D \mid x \leq 0\}$, *then* $\mathbf{P} = \langle D, \bullet, 1, \perp \rangle$ *is a phase structure such that the core Girard structure* $\mathbf{D}' = \langle D^{\perp\perp}, \subseteq, \otimes, \mathbf{I}, ^{\perp} \rangle$ *defined in Lemma 18 is isomorphic to* $\mathbf{D}$.

Proof. Given any subset X of D, let *lower*(X) denote the set of lower bounds of X and *upper*(X) denote the set of upper bounds of X. Also, let $\sim X = \{\sim x \mid x \in X\}$. One easily verifies that $X^{\perp} =$ *lower*($\sim X$), *upper*(X) $= \sim$ *lower*($\sim X$), and $X^{\perp\perp} =$ *lower*(*upper*(X)). Thus, since D is a complete lattice, every fact $X^{\perp\perp} =$ *lower*(*upper*(X)) of $\mathbf{P}$ corresponds uniquely to the lower ideal *lower*($\bigvee X$), which itself corresponds uniquely to $\bigvee X$. This mapping establishes a bijection between $\mathbf{D}$ and $\mathbf{D}'$, and it is easily checked that it is an isomorphism. □

In Lemma 16, we have shown that the semantics given by core Girard structures (or equivalently phase structures) is sound with respect to the proof system. We can also show that the proof system is complete w.r.t. this semantics.

Lemma 20 *If a sequent* $\Gamma \vdash \Delta$ *is valid (in phase semantics), then it is provable in* $\mathcal{L}in_0$.

Proof. First of all, note that it is enough to prove completeness for sequents of the form $\vdash A$, *i.e.* propositions. At least two proofs can be given. The first one, suggested by Avron [2], consists in two steps. The first step is to prove completeness w.r.t. core Girard prestructures. For this, define an equivalence relation $\equiv$ on propositions as follows: $A \equiv B$ iff both sequents $A \vdash B$ and $B \vdash A$ are provable. Then, define an algebraic structure on the set D of equivalence classes modulo $\equiv$ by setting

$$\begin{aligned} \mathbf{1} &= [\mathbf{1}], \\ \mathbf{0} &= [\mathbf{0}], \\ 1 &= [\mathbf{I}], \\ 0 &= [\perp], \\ [A] \parallel [B] &= [A \nparallel B], \end{aligned}$$

$$[A] \bullet [B] = [A \otimes B],$$
$$[A] \vee [B] = [A \oplus B],$$
$$[A] \wedge [B] = [A \,\&\, B],$$
$$\sim [A] = [A^{\perp}],$$

and define $[A] \leq [B]$ iff $A \vdash B$ is provable. One can then check that $\mathbf{D} = \langle D, \leq, \bullet, 1, \sim \rangle$ is a core Girard prestructure. Note that $1 \leq [A]$ iff A is provable. If we pick the valuation v such that $v(P) = [P]$ for every atom P, then $v(A) = [A]$, and if A is valid, then in particular $\mathbf{D} \models A[v]$, that is $1 \leq [A]$, and thus A is provable. The second step is to show that every core Girard prestructure can be embedded into a core Girard structure, and this in preserving existing least upper bounds and greatest lower bounds. This is easily shown by using the Mac Neille completion and Theorem 1.

The second proof due to Girard consists in producing a particular phase structure and a particular valuation, such that validity amounts to provability (see Girard [7]). This construction appears to be another way of constructing the structure **D** defined in the first proof, in terms of a phase structure. Note that the set M of finite multisets of formulae is a commutative monoid under multiset union ($\Gamma \bullet \Delta = \Gamma, \Delta$), with identity $\emptyset$. If we let $\perp = \{\Gamma \mid \vdash \Gamma \quad \text{is provable}\}$, we can check that the sets of the form

$$Pr(A) = \{\Gamma \mid \vdash \Gamma, A \quad \text{is provable}\},$$

are facts, because $Pr(A) = Pr(A^{\perp})^{\perp}$. If we define the valuation v such that $v(P) = Pr(P)$ for every atom P, we can check that $v(A) = Pr(A)$. Since A is valid, $\mathbf{D} \models A[v]$, that is, $\emptyset \in Pr(A)$, and thus A is provable. □

We now extend the above semantics to (full) linear logic. For this, we need to add a unary operation □ to interpret the connective ! (*of course*).

Definition 15 *A Girard structure is a sextuple* $\mathbf{G} = \langle G, \leq, \bullet, 1, \sim, \Box \rangle$ *such that the quintuple* $\langle G, \leq, \bullet, 1, \sim \rangle$ *is a core Girard structure, and* $\Box : G \to G$ *is a unary operator satisfying the following properties: for all* $x, y \in G$,

(1) $\Box(1) = 1$;

(2) $\Box(x) \leq x$;

(3) $\Box(\Box(x)) = \Box(x)$;

(4) $\Box(x) \bullet \Box(y) = \Box(x \wedge y)$.

Definition 12 is extended to the exponentials as follows:

$$v(!A) = \Box(v(A)),$$
$$v(?A) = \sim \Box(\sim v(A)).$$

The following lemma is needed to show soundness of this semantics.

Lemma 21 *In every Girard structure, the following properties hold:*

(1) $\Box(x) \leq 1$*;*

(2) $\Box(x) \bullet y \leq y$*;*

(3) $\Box(x) \bullet \Box(x) = \Box(x)$*;*

(4) If $x \leq y$ *then* $\Box(x) \leq \Box(y)$*;*

(5) If $1 \leq x$ *then* $\Box(x) = 1$*;*

(6) If $\Box(x) \leq y$ *then* $\Box(x) \leq \Box(y)$*;*

(7) If $x_1 \bullet \ldots \bullet x_n \leq y$ *then* $\Box(x_1) \bullet \ldots \bullet \Box(x_n) \leq \Box(y)$.

Proof. These properties are easy to prove. Property (1) holds because

$$\Box(x) = \Box(x) \bullet 1 = \Box(x) \bullet \Box(1) = \Box(x \wedge 1) \leq x \wedge 1 \leq 1.$$

For (2), since by (1), $\Box(x) \leq 1$, by monotonicity of $\bullet$, we have $\Box(x) \bullet y \leq 1 \bullet y = y$. For (3), $\Box(x) \bullet \Box(x) = \Box(x \wedge x) = \Box(x)$. For (4), If $x \leq y$ then $x = x \wedge y$. Thus, $\Box(x) = \Box(x \wedge y) = \Box(x) \bullet \Box(y) \leq \Box(y)$, by (2). It is clear that (5) follows from (1) and (4). If $\Box(x) \leq y$, by (4), we have $\Box(\Box(x)) \leq \Box(y)$, and since $\Box(\Box(x)) = \Box(x)$, we have $\Box(x) \leq \Box(y)$. Since $\Box(x) \leq x$, if $x_1 \bullet \ldots \bullet x_n \leq y$ then $\Box(x_1) \bullet \ldots \bullet \Box(x_n) \leq y$. Since $\Box(x) \bullet \Box(y) = \Box(x \wedge y)$, we have $\Box(x_1) \bullet \ldots \bullet \Box(x_n) = \Box(x_1 \wedge \ldots \wedge x_n)$, and so $\Box(x_1 \wedge \ldots \wedge x_n) \leq y$. By (6), we get $\Box(x_1 \wedge \ldots \wedge x_n) \leq \Box(y)$, that is $\Box(x_1) \bullet \ldots \bullet \Box(x_n) \leq \Box(y)$. □

Lemma 22 *If* $\Gamma \vdash \Delta$ *is provable in linear logic, then for every Girard structure* **G** *and every valuation* v, $\mathbf{G} \models (\Gamma \vdash \Delta)[v]$. *As a corollary,* $\Gamma \vdash \Delta$ *is valid.*

Proof. Immediate by Lemma 21. □

We now give the following construction which shows how a Girard structure arises from a core Girard structure.

Theorem 2 *Let* $\mathbf{G} = \langle G, \leq, \bullet, 1, \sim, \Box \rangle$ *be a Girard structure. The set* F *defined by* $F = \{x \in G \mid x = \Box(x)\}$ *satisfies the following properties:*

(1) F *is closed under arbitrary least upper bounds. In particular,* $\mathbf{0} \in F$*;*

(2) F *is closed under* $\bullet$*;*

(3) $x \bullet x = x$ *for every* $x \in F$*;*

(4) The identity element 1 *is the greatest element of* F*.*

Furthermore, for every $a \in G$, $\Box(a) = \bigvee\{x \in F \mid x \leq a\}$.

Conversely, given a core Girard structure $\langle G, \leq, \bullet, 1, \sim\rangle$ *and a subset* F *of* G *satisfying the properties (1)–(4), then if we define* $\Box$ *by* $\Box(a) = \bigvee\{x \in F \mid x \leq a\}$*, the sextuple* $\mathbf{G} = \langle G, \leq, \bullet, 1, \sim, \Box\rangle$ *is a Girard structure.*

Proof. Let $\{x_j\}_{j \in J}$ be any family of elements from F, *i.e.*, such that $\Box(x_j) = x_j$ for all $i \in J$. Since $x_j \leq \bigvee_{j \in J}\{x_j\}$, by monotonicity of $\Box$ (proved in Lemma 21), $\Box(x_j) \leq \Box(\bigvee_{j \in J}\{x_j\})$, and since $\Box(x_j) = x_j$ for all $i \in J$, we have $x_j \leq \Box(\bigvee_{j \in J}\{x_j\})$, and thus

$$\bigvee_{j \in J}\{x_j\} \leq \Box(\bigvee_{j \in J}\{x_j\}).$$

Since $\Box(\bigvee_{j \in J}\{x_j\}) \leq \bigvee_{j \in J}\{x_j\}$ holds by property (2) of the definition of $\Box$ (Definition 15), we have

$$\Box(\bigvee_{j \in J}\{x_j\}) = \bigvee_{j \in J}\{x_j\},$$

showing that F is closed under nonempty least upper bounds. Since $\Box(x) \leq x$ for all $x \in G$, in particular $\Box(\mathbf{0}) \leq \mathbf{0}$, which implies that $\Box(\mathbf{0}) = \mathbf{0}$, since $\mathbf{0}$ is the least element of G. Therefore, F is closed under arbitrary least upper bounds.

For $x, y \in F$, we have $x \bullet y = \Box(x) \bullet \Box(y) = \Box(x \wedge y)$, by property (4) of the definition of $\Box$. Thus, $\Box(x \bullet y) = \Box(\Box(x \wedge y)) = \Box(x \wedge y)$, by property (3) of the definition of $\Box$. Therefore, $\Box(x \bullet y) = x \bullet y$.

For any $x \in F$, we have $x \bullet x = \Box(x) \bullet \Box(x) = \Box(x \wedge x) = \Box(x) = x$. Therefore, $x \bullet x = x$.

Since $\Box(x) \leq 1$ by property 1 of the definition of $\Box$, for any $x \in F$, we have $x = \Box(x) \leq 1$. Also, by Lemma 21, $\Box(1) = 1$. Therefore, 1 is the greatest element of F.

For every $x \in F$, by monotonicity of $\Box$, $x \leq a$ implies $\Box(x) \leq \Box(a)$, that is $x \leq \Box(a)$, since $\Box(x) = x$. But we also have $\Box(\Box(a)) = \Box(a)$, that is, $\Box(a) \in F$, and thus $\bigvee\{x \in F \mid x \leq a\} = \Box(a)$ for every $a \in G$. This concludes the proof of the first half of the theorem.

Conversely, assume that F has the properties (1)–(4), and define $\Box$ such that $\Box(a) = \bigvee\{x \in F \mid x \leq a\}$. First, note that since F is closed under arbitrary least upper bounds, $\Box(a) \in F$ for every $a \in G$, and obviously, $\Box(a) = a$ if $a \in F$.

Clearly, $\Box(a) \leq a$ for all $a \in G$, property (2) of the definition of $\Box$.

Since 1 is the greatest element of F, we also have $\Box(a) \leq 1$ for all $a \in G$, property (1) of the definition of $\Box$.

Since F is closed under arbitrary least upper bounds, $\Box(a) = \bigvee\{x \in F \mid x \leq a\} \in F$, and thus, $\Box(\Box(a)) = \bigvee\{y \in F \mid y \leq \Box(a)\} = \Box(a)$, property (3) of the definition of $\Box$.

Since $x \leq 1$ for every $x \in F$, for $x, y \in F$, we have $x \bullet y \leq x \bullet 1 = x$ and $x \bullet y \leq 1 \bullet y = y$, which implies that $x \bullet y \leq x \wedge y$. Thus, $a \bullet b \leq \bigvee\{x \in F \mid x \leq a \wedge b\}$, that is, $a \bullet b \leq \Box(a \wedge b)$, which implies $\Box(a) \bullet \Box(b) \leq \Box(a \wedge b)$, since $\Box(a) \leq a$, and $\Box(b) \leq b$. Also, since $\bullet$ distributes over $\bigvee$,

$$\begin{aligned}\Box(a) \bullet \Box(b) &= \left(\bigvee\{x \in F \mid x \leq a\}\right) \bullet \left(\bigvee\{y \in F \mid y \leq b\}\right) \\ &= \bigvee\{x \bullet y \mid x, y \in F,\ x \leq a,\ y \leq b\}.\end{aligned}$$

Since $\Box(a \wedge b) \leq a \wedge b \leq a$, $\Box(a \wedge b) \leq a \wedge b \leq b$, $\Box(a \wedge b) \in F$, and $z \bullet z = z$ for all $z \in F$, we have $\Box(a \wedge b) \leq \Box(a) \bullet \Box(b)$. Therefore, $\Box(a) \bullet \Box(b) = \Box(a \wedge b)$, property (4) of the definition of $\Box$. This concludes the proof of the second half of the theorem. $\Box$

One can show that in every core Girard structure **G**, the subset

$$F = \{x \in G \mid x \bullet x = x \text{ and } x \leq 1\}$$

satisfies the properties of Theorem 2. Thus, we obtain the following lemma, showing that every core Girard structure can be extended to a Girard structure.

Lemma 23 *Every core Girard structure* **G** *can be extended to a Girard structure by defining the operator* $\Box$ *such that* $\Box(a) = \bigvee\{x \leq a \wedge 1 \mid x \bullet x = x\}$.

Another interesting property of $\Box$ showing that it is the fixed point of some simple operators is given in the following lemma.

Lemma 24 *In every Girard structure* **G**, *for every* $a \in G$, *we have the following identities:*

(1) $\Box(a) = (a \wedge 1) \bullet \Box(a)$,

and

(2) $\Box(a) = (a \wedge 1) \wedge (\Box(a) \bullet \Box(a))$.

Proof. First, we prove (1). (i) Recall from Lemma 21 that $\Box(a) \bullet \Box(a) = \Box(a)$.
(ii) We have $\Box(a) = \Box(a) \bullet 1 = \Box(a) \bullet \Box(1) = \Box(a \wedge 1)$. (iii) If $x \leq 1$, then $x \bullet y \leq y$, since $x \bullet y \leq 1 \bullet y = y$. Since $a \wedge 1 \leq 1$, using (iii), we have $(a \wedge 1) \bullet \Box(a) \leq \Box(a)$. Using (ii) and the fact that $\Box(x) \leq x$ for every $x \in G$, we have $\Box(a) = \Box(a \wedge 1) \leq a \wedge 1$. Using (i) and the monotonicity of $\bullet$, we have $\Box(a) = \Box(a) \bullet \Box(a) \leq (a \wedge 1) \bullet \Box(a)$. Therefore,

$\Box(a) = (a \wedge 1) \bullet \Box(a)$, as desired. We now prove (2). Since $\Box(a) \bullet \Box(a) = \Box(a)$, we just have to prove that $\Box(a) = (a \wedge 1) \wedge \Box(a)$. Since $\Box(a) \leq a$ and $\Box(a) \leq 1$, we have $\Box(a) \leq a \wedge 1$, and thus $\Box(a) = (a \wedge 1) \wedge \Box(a)$. □

Lemma 24 shows that $\Box(a)$ is a fixed point of the operator $x \mapsto (a \wedge 1) \bullet x$, for every $a \in G$ (and also of the operator $x \mapsto (a \wedge 1) \wedge (x \bullet x)$). Since G is a complete lattice, and this operator is monotonic, by Tarski's fixed point theorem, the set of fixed points of this operator is a complete lattice. In particular, since $\bullet$ distributes over $\bigvee$, the least fixed point of this operator is given by the expression

$$\bigvee_{n \geq 1} \bigotimes_{n} (a \wedge 1).$$

This connection probably deserves further investigations. The interest in the identity $\Box(a) = (a \wedge 1) \wedge (\Box(a) \bullet \Box(a))$ stems from the fact that it implies the properties: (i) $\Box(a) \leq a$; (ii) $\Box(a) \leq 1$; and (iii) $\Box(a) \bullet \Box(a) = \Box(a)$ (due to Yves Lafont). In turn, these properties imply the soundness of the inference rules (*dereliction*: *left*), (*weakening*: *left*), and (*contraction*: *left*). Thus, we obtain an equivalent proof system for linear logic if we add the axiom $!A \multimap (A \,\&\, \mathbf{I}) \,\&\, (!A \otimes !A)$ and delete the above rules. By duality, we obtain an equivalent proof system for linear logic if we add the axiom $?A \multimap (A \oplus \bot) \oplus (?A \parr ?A)$ and delete the rules (*dereliction*: *right*), (*weakening*: *right*), and (*contraction*: *right*).

In order to interpret ! and ?, Girard defines an extension of the notion of phase structure that he calls a topolinear space (see Girard [7]). We give this definition and compare it with Definition 15.

Definition 16 *A topolinear space is a triple $\langle \mathbf{P}, \bot, F \rangle$, where $\mathbf{P}$ is a phase structure, and F is a subset of P, the set of closed facts, having the following properties:*

(1) F is closed under arbitrary &. In particular, $\mathbf{1} \in F$;

(2) F is closed under (finite) ⅋ (par);

(3) $x \parr x = x$ for every $x \in F$;

(4) The fact $\bot$ is the least element of F.

The linear negation of a closed fact is called an *open fact*.

Given a topolinear space, given a valuation v, the fact $v(!A)$ is defined as the greatest open fact included in $v(A)$, and $v(?A)$ is defined as the least closed fact containing $v(A)$. In other words:

$$v(!A) = \Big(\bigcup \{X^\bot \mid X \in F,\ X^\bot \subseteq v(A)\}\Big)^{\bot\bot}, \qquad v(?A) = \bigcap \{X \in F \mid X \supseteq v(A)\}.$$

Using the correspondence between core Girard structures and phase structures given by Lemma 18, it is clear that the subset F of Theorem 2 is the collection of open facts of Girard's topolinear space, and that the definition of $v(?A)$ corresponds exactly to the definition $\Box(a) = \bigvee\{x \in F \mid x \leq a\}$ (by the definition of the least upper bound of a fact).

As in the case of core Girard structures, not only do we have soundness, but also completeness.

Lemma 25 *If a sequent $\Gamma \vdash \Delta$ is valid (in Girard structures), then it is provable in $\mathcal{L}in_0^{!,?}$.*

Proof. As in Lemma 20, at least two proofs are possible. The first proof is an extension of Avron's proof [2]. It is necessary to extend the operation $\Box$ defined on $\mathbf{D}$ by $\Box([!A]) = ![A]$, to the completion by cuts $\mathbf{D}^\dagger$ of the core prestructure $\mathbf{D}$. For every $y \in \mathbf{D}^\dagger$, we define

$$\Box^\dagger(y) = \bigvee\{\{\Box(x)\}^\dagger \mid x \in \mathbf{D},\ \{x\}^\dagger \leq y\}.$$

Using the fact that $\bullet$ distributes over arbitrary least upper bounds, we can prove that $\Box^\dagger$ has the required properties (in particular, that $\Box^\dagger(a) \bullet \Box^\dagger(b) = \Box^\dagger(a \wedge b)$).

The other proof is due to Girard (see [7]). It is a generalization of the proof that we sketched in Lemma 20. We consider the phase structure consisting of the commutative monoid of multisets of formulae, and define F to be the family of arbitrary intersections of facts of the form $Pr(?A)$. One can then prove that a topolinear space is indeed obtained (this uses the fact that $\sharp$ distributes over arbitrary intersections). Then, it is easy to prove that $?Pr(A) = Pr(?A)$, and completeness follows immediately. $\Box$

Presently, $\Box$ has the property that $\Box(a) \bullet \Box(b) = \Box(a \wedge b)$, and it is also easy to verify that $\Box(a \wedge b) \leq \Box(a) \wedge \Box(b)$, but in general, we do not have $\Box(a \wedge b) = \Box(a) \wedge \Box(b)$. In the next section, we propose to modify the proof rules and the semantics so that $!A \otimes !B$ and $!A \,\&\, !B$ are equivalent.

6 A Variation On the Semantics of the Connective !

On the semantic side, we strengthen Definition 15 as follows.

Definition 17 *A Girard topostructure is a sextuple $\mathbf{G} = \langle G, \leq, \bullet, 1, \sim, \Box\rangle$ such that the quintuple $\langle G, \leq, \bullet, 1, \sim\rangle$ is a core Girard structure, and $\Box : G \to G$ is a unary operator satisfying the following properties: for all $x, y \in G$,*

(1) $\Box(1) = 1$*;*

(2) $\Box(x) \leq x$*;*

(3) $\Box(\Box(x)) = \Box(x)$*;*

(4) $\Box(x) \bullet \Box(y) = \Box(x \wedge y)$.

(5) $\Box(x \wedge y) = \Box(x) \wedge \Box(y)$.

From (4) and (5), we have that $\Box(x) \bullet \Box(y) = \Box(x) \wedge \Box(y)$. Definition 12 is extended to the exponentials as before:

$$v(!A) = \Box(v(A)),$$
$$v(?A) = \sim \Box(\sim v(A)).$$

We add the following rules to the definition of the rules for the exponentials

Definition 18

$$\frac{!A, !B, \Gamma \vdash \Delta}{!A \;\&\; !B, \Gamma \vdash \Delta} \quad (!\,\&\text{: } \textit{left})$$

$$\frac{\Gamma \vdash \Delta, ?A, ?B}{\Gamma \vdash \Delta, ?A \oplus ?B} \quad (?\oplus\text{: } \textit{right})$$

The system obtained by adding the rules of Definition 18 to the rules of the system $\mathcal{L}in_0^{!,?}$ is denoted as $\mathcal{L}in_0^{!,?,!\&,?\oplus}$. Soundness is easily obtained.

Lemma 26 *If* $\Gamma \vdash \Delta$ *is provable in the system of linear logic* $\mathcal{L}in_0^{!,?,!\&,?\oplus}$*, then for every Girard topostructure* $\mathbf{G}$ *and every valuation* v, $\mathbf{G} \models (\Gamma \vdash \Delta)[v]$. *As a corollary,* $\Gamma \vdash \Delta$ *is valid.*

Proof. Immediate by Lemma 21 and the fact that $\Box(x) \bullet \Box(y) = \Box(x) \wedge \Box(y)$. □

Theorem 2 is extended as follows.

Theorem 3 *Let* $\mathbf{G} = \langle G, \leq, \bullet, 1, \sim, \Box \rangle$ *be a Girard topostructure. The set* F *defined by* $F = \{x \in G \mid x = \Box(x)\}$ *satisfies the following properties:*

(1) F *is closed under arbitrary least upper bounds. In particular,* $\mathbf{0} \in F$*;*

(2) F *is closed under (finite) greatest lower bounds.*

(3) F *is closed under* $\bullet$*;*

(4) $x \bullet x = x$ *for every* $x \in F$*;*

(5) The identity element 1 *is the greatest element of* F.

Furthermore, for every $a \in G$, $\Box(a) = \bigvee\{x \in F \mid x \leq a\}$.

Conversely, given a core Girard structure $\langle G, \leq, \bullet, 1, \sim\rangle$ *and a subset* F *of* G *satisfying the properties (1)–(5), then if we define* $\Box$ *by* $\Box(a) = \bigvee\{x \in F \mid x \leq a\}$, *the sextuple* $\mathbf{G} = \langle G, \leq, \bullet, 1, \sim, \Box\rangle$ *is a Girard topostructure.*

Proof. Properties (1), (3)–(5) are verified as in the proof of Theorem 2. Since $\Box(a \wedge b) = \Box(a) \wedge \Box(b)$, if $a = \Box(a)$ and $b = \Box(b)$, then $a \wedge b = \Box(a) \wedge \Box(b) = \Box(a \wedge b)$, proving (2).

Conversely, since $\Box(x) \in F$ for every $x \in G$, by (2), $\Box(a) \wedge \Box(b) \in F$. Since $\Box(x) = x$ for $x \in F$, $\Box(\Box(a) \wedge \Box(b)) = \Box(a) \wedge \Box(b)$. On the other hand, as in the proof of Theorem 2, we have $\Box(x) \bullet \Box(y) = \Box(x \wedge y)$ and $\Box(\Box(x)) = \Box(x)$, and so,

$$\Box(\Box(a) \wedge \Box(b)) = \Box(\Box(a)) \bullet \Box(\Box(b)) = \Box(a) \bullet \Box(b) = \Box(a \wedge b).$$

Thus, $\Box(a \wedge b) = \Box(a) \wedge \Box(b)$, property (2) of Definition 17. $\Box$

We can also extend the completeness lemma (Lemma 25) to topostructures and $\mathcal{L}in_0^{!,?,!\&,?\oplus}$.

Lemma 27 *If a sequent* $\Gamma \vdash \Delta$ *is valid (in Girard topostructures), then it is provable in* $\mathcal{L}in_0^{!,?,!\&,?\oplus}$.

Proof. As in the proof of Lemma 25, it is necessary to extend the operation $\Box$ defined on $\mathbf{D}$ by $\Box([!A]) = ![A]$, to the completion by cuts $\mathbf{D}^\dagger$ of the core prestructure $\mathbf{D}$.[2] For every $y \in \mathbf{D}^\dagger$, we define

$$\Box^\dagger(y) = \bigvee\{\{\Box(x)\}^\dagger \mid x \in \mathbf{D},\ \{x\}^\dagger \leq y\}.$$

Using the fact that $\bullet$ distributes over arbitrary least upper bounds, we can prove that $\Box^\dagger$ has the required properties, in particular, that $\Box^\dagger(a) \bullet \Box^\dagger(b) = \Box^\dagger(a \wedge b)$. We can also prove that $\Box^\dagger(a \wedge b) = \Box^\dagger(a) \wedge \Box^\dagger(b)$, using the fact that $(!A \,\&\, !B) \multimap !(A \,\&\, B)$ is provable, and that in the completion by cuts, $X^\dagger \wedge Y^\dagger = X^\dagger \cap Y^\dagger$. $\Box$

We now turn to proof nets.

7 Proof Nets for Multiplicative Linear Logic

The same linear sequent can have different proofs differring for bureaucratic reasons, namely, that inferences are applied in a different order. For example, the sequent

$$\vdash (A \otimes B) \otimes C, A^\perp \parr B^\perp, C^\perp$$

[2]Recall that in the completion by cuts, for every subset $X \subseteq D$, we have $X^\dagger = \mathit{lower}(\mathit{upper}(X))$, and in particular, when $X = \{x\}$, we have $\{x\}^\dagger = \mathit{lower}(x)$.

has the following two proofs

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

and

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

Clearly, these two proofs differ in an inessential way, and it should be possible to come up with a notation akin to natural deduction so that these two proofs are identified. This is possible for the fragment of *multiplicative linear logic* involving only $\otimes$, $\parr$, and $^{\perp}$, using the notion of proof net due to Girard (see Girard [7], and Girard, Lafont, and Taylor [6]). First, we recall a definition.

Definition 19 *A literal is either a propositional letter P or the negation $P^{\perp}$ of a propositional letter.*

Proofs nets are certain unoriented connected graphs whose nodes are labeled with propositions. In order to define these graphs, we consider that labeled nodes have *entry and exit points* defined as follows: a literal has a single entry and a single exit, and both a tensor and a par have two entry points and a single exit point.

Definition 20 *A proof net (of multiplicative linear logic) is a finite unoriented connected node-labeled graph with the following properties:*

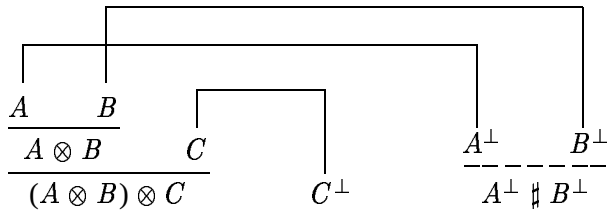
(1) For every node labeled with a literal, there is a single arc from the entry point of that literal to the entry point of a literal with the same name and the opposite sign;

(2) For every node labeled with a tensor $A \otimes B$ or a par $A \parr B$, there are two distinct nodes labeled with A and B respectively, such that the exit of A is connected to one of the two entry points of $A \otimes B$ (resp. $A \parr B$) and the exit of B is connected to the other entry point of $A \otimes B$ (resp. $A \parr B$), each by a single arc;

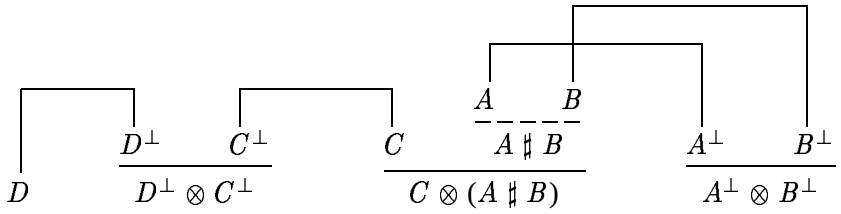
(3) The exit point of every node is connected to at most one other node.

Nodes whose exit points are not connected to any node will be called terminal nodes, or leaves.

For reasons that will become clear when we discuss the criterion for checking that a proof net corresponds to a sequential proof, we draw ($\nparallel$: *right*) inferences using a broken line, and ($\otimes$: *right*) inferences using a solid line. The following is an example of a proof net:



Another example of a proof net is the following:



As we shall see shortly, there is an algorithm for converting any sequential proof (for the multiplicative fragment of linear logic considered here) into a proof net. However, the definition of a proof net is a bit too liberal, due the local nature of the conditions involved, and some proof nets are unsound, in the sense that they do not correspond to any sequential proof. For technical reasons, we will need a slightly more liberal notion of a proof net. In fact, it turns out that this notion corresponds precisely to the notion of a sequential deduction, a sequential deduction being similar to a sequential proof, except that leaf nodes can also be labeled with arbitrary sequents $\vdash A$, where A is a proposition, rather than only axioms.

Definition 21 *A deduction net (of multiplicative linear logic) is a finite unoriented connected node-labeled graph satisfying properties (1) and (3) of Definition 20, and such that if property (2) does not hold for some node, then both entry points of such a node are not connected to any other node.*

Thus, a proof net is a deduction net that also satisfies property (2) of Definition 20. Contrary to a proof net, a deduction net may have nodes whose entry points are not connected to any other node. Such a node is called an *initial node*, or *root*. The following lemma is easily shown.

Lemma 28 *Let* Π *be a deduction net such that* k *of its terminal nodes are labeled with some propositions* $A_1, \ldots, A_k$*, and let* Π' *be some other deduction net having* k *of its entry nodes labeled with* $A_1, \ldots, A_k$*. The graph obtained by grafting* Π' *onto* Π *by identifying each selected terminal node of* Π *labeled with* A_i *with the corresponding entry node of* Π' *labeled with* A_i *is a deduction net.*

One can define a transformation that produces a deduction net from a sequential deduction, but not all deduction nets come from a sequential deduction. In order to single out which deduction nets really correspond to sequential deductions, one needs a global criterion. In his seminal paper, Girard gave such a criterion for proof nets, the "long trip condition" [7]. Later, Danos and Regnier proposed a different criterion [5].

We now present the Danos-Regnier criterion for soundness of a deduction net. This criterion is equivalent to Girard's original "trip conditions" criterion, but it is somewhat more manageable. It is convenient to consider that there are two kinds of edges:

(1) Edges connecting the exit of A and B to the entries of a tensor $A \otimes B$ and edges connecting the entry of some A to the entry of some $A^{\perp}$, considered as *solid*;

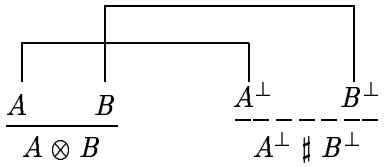
(2) Edges connecting the exit of A and B to the entries of a par $A \parr B$, considered as *soft*.

Definition 22 *Given a deduction net* Π*, a switch graph associated with* Π *is any subgraph of* Π *obtained by deleting exactly one of the two soft edges associated with every par node in* Π *(and keeping the other soft edge).*

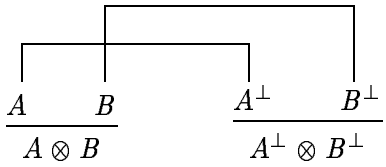
The Danos-Regnier criterion for soundness of a deduction net is stated as follows (see Danos and Regnier [5], and Danos [4]).

Definition 23 *A deduction net* Π *satisfies the Danos-Regnier criterion, or is sound, iff every switch graph associated with* Π *is a tree.*

For example, the following is a sound proof net, since both switch graphs are trees:



On the other hand, the following proof net is unsound, because the (only) switch graph has a cycle.



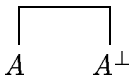
We now give an algorithm for transforming a sequential deduction into a deduction net, and show that the resulting proof net satisfies the Danos-Regnier criterion.

Lemma 29 *There is algorithm $\mathcal{N}$ which, given a deduction Π of a multiplicative sequent $\vdash A_1, \ldots, A_n$, produces a deduction net $\mathcal{N}(\Pi)$ whose terminal nodes are in one-to-one correspondence with the occurrences of formulae $A_1, \ldots, A_n$. Furthermore, $\mathcal{N}(\Pi)$ satisfies the Danos-Regnier criterion.*

Proof. The algorithm $\mathcal{N}$ is defined by induction on the structure of the deduction Π.

Case 1: Π consists of a single formula $\vdash A$. Then $\mathcal{N}(\Pi)$ is the deduction net consisting of the single node A. Obviously, $\mathcal{N}(\Pi)$ satisfies the Danos-Regnier criterion.

• Π consists of an axiom $\vdash A, A^{\perp}$. Then $\mathcal{N}(\Pi)$ is the proof net



Obviously, $\mathcal{N}(\Pi)$ satisfies the Danos-Regnier criterion.

Case 2: Π is of the form

$$\dfrac{\begin{array}{c}\Pi_1\\ \vdash \Gamma, A, B\end{array}}{\vdash \Gamma, A \parr B} \quad (\parr\text{: } \textit{right})$$

Then $\mathcal{N}(\Pi)$ is the proof net

$$\dfrac{\begin{array}{c}\mathcal{N}(\Pi_1)\\ A \quad\quad B\end{array}}{A \parr B}$$

obtained by grafting the exit nodes A and B of $\mathcal{N}(\Pi_1)$ respectively to the entry nodes A and B of the elementary proof net corresponding to the ($\parr$: *right*) inference. If $\mathcal{N}(\Pi_1)$ satisfies the Danos-Regnier criterion, then it is easy to verify that $\mathcal{N}(\Pi)$ also satisfies the Danos-Regnier criterion.

Case 3: Π is of the form

$$\dfrac{\begin{array}{cc}\Pi_1 & \Pi_2\\ \vdash \Gamma, A & \vdash \Delta, B\end{array}}{\vdash \Gamma, \Delta, A \otimes B} \quad (\otimes\text{: } \textit{right})$$

Then $\mathcal{N}(\Pi)$ is the proof net

$$\dfrac{\begin{array}{cc}\mathcal{N}(\Pi_1) & \mathcal{N}(\Pi_2)\\ A & B\end{array}}{A \otimes B}$$

obtained by grafting the exit node A of $\mathcal{N}(\Pi_1)$ and the exit node B of $\mathcal{N}(\Pi_2)$ respectively to the entry nodes A and B of the elementary proof net corresponding to the ($\otimes$: *right*) inference. If $\mathcal{N}(\Pi_1)$ and $\mathcal{N}(\Pi_2)$ satisfy the Danos-Regnier criterion, then it is easy to verify that $\mathcal{N}(\Pi)$ also satisfies the Danos-Regnier criterion. □

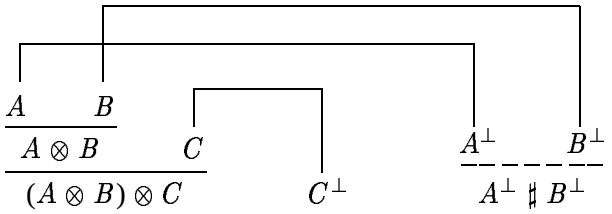
The transformation $\mathcal{N}$ identifies sequential deductions that differ only for inessential reasons, like the order of inferences. For example, the two sequential proofs

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

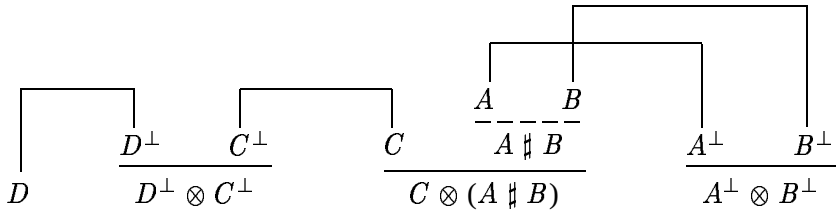
and

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

are mapped to the same proof net:



We now wish to show that the Danos-Regnier criterion insures that every proof net that satisfies the criterion is of the form $\mathcal{N}(\Pi)$ for some sequential deduction Π. This is proved by induction on the number of nodes in the deduction net. The proof is quite easy when the proof net has some terminal node labeled with a par, but the case when all terminal nodes are labeled with tensors is tricky and requires a detailed analysis of the structure of deduction nets. The problem is that splitting a proof net by chosing any arbitrary terminal node labeled with a $\otimes$ and deleting the two arcs incoming to this node may not yield sound proof nets. For example, splitting the proof net below at the node $A^{\perp} \otimes B^{\perp}$ does *not* yield proof nets. On the other hand, splitting either at node $D^{\perp} \otimes C^{\perp}$ or at node $C \otimes (A \parr B)$ yields sound proof nets.



The key observation is contained in the following lemma.

Lemma 30 *Let Π be a deduction net whose terminal nodes are all labeled with tensors, let $A \otimes B$ be one of these tensors, and let Π' be the subgraph obtained from Π by deleting this terminal node and the two edges from A to $A \otimes B$ and from B to $A \otimes B$. If the criterion holds for Π and A and B are connected in Π', then there is a set $\{C_1 \parr D_1, \ldots, C_k \parr D_k\}$ of par nodes such that the graph Π'' obtained from Π' by deleting all edges from C_i to $C_i \parr D_i$ and from D_i to $C_i \parr D_i$, $i = 1, \ldots, k$, consists of three disjoint maximal connected components which are deduction nets satisfying the criterion. Furthermore, without any loss of generality, it can be assumed that one component Π_1 contains both A and the C_i, another component Π_2 contains both B and the D_i, and the third Π_3 contains the $C_i \parr D_i$, $i = 1, \ldots, k$.*

Proof. Let us examine closely what happens when there is a terminal node labeled $A \otimes B$ such that A and B are connected in the subgraph Π' defined above.

- If A and B are connected in Π', then Π' itself is connected. Otherwise, Π' would consist of at least two disjoint maximal connected components, one of which does *not* contain both A and B, in which case, Π would not be connected, a contradiction.

- Π' contains some par node $C \parr D$. Otherwise, the only switch graph of Π' would be Π' itself, and similarly for Π, and both Π and Π' would be trees. But then, A and B would be connected in Π', and this would imply the existence of a cycle in Π, a contradiction.

- For every path p in Π' from A to B, there is some par node $C \parr D$ such that the path p contains both edges from C to $C \parr D$ and from D to $C \parr D$. Otherwise, there is in Π' a path p from A to B which uses at most one of the two incoming edges into each par node. Then, it is possible to pick a choice of the soft edges in Π' (and thus in Π) involving the edges used by the path p, so that this is a path from A to B in some switch graph of Π'. However, in Π, this path yields a cycle together with the edges from A to $A \otimes$B and from B to $A \otimes$B.

- From the previous item, there is a set $\{C_1 \parr D_1, \ldots, C_k \parr D_k\}$ of par nodes such that every path in Π' from A to B contains both edges from C_i to $C_i \parr D_i$ and from D_i to $C_i \parr D_i$, for some i, $1 \leq i \leq k$. The graph Π'' obtained from Π' by deleting all edges from C_i to $C_i \parr D_i$ and from D_i to $C_i \parr D_i$, $i = 1, \ldots, k$, consists of three disjoint maximal connected components. Furthermore, without any loss of generality, it can be assumed that one of the components contains both A and the C_i, another component contains both B and the D_i, and the third contains the $C_i \parr D_i$, $i = 1, \ldots, k$.

  Let us first delete the edges from C_i to $C_i \parr D_i$ in Π', $i = 1, \ldots, k$. We must obtain two disjoint maximal connected components. Indeed, since every path in Π' from A to B must contain for some i ($1 \leq i \leq k$) both edges from C_i to $C_i \parr D_i$ and from D_i to $C_i \parr D_i$, the resulting graph is not connected, and the maximal connected components containing A and B must be disjoint. On the other hand, if we had at least three disjoint components, Π' would not be connected. Thus, we have two disjoint connected components, Π_1 containing the C_i and A (or symmetrically B), and Π''' containing the D_i, the $C_i \parr D_i$, and B (or symmetrically A). Let us now delete the edges from D_i to $C_i \parr D_i$ in Π''', $i = 1, \ldots, k$. The

component Π''' must split into two disjoint connected components. Indeed, if the resulting graph were still connected, then it would be possible to connect A and B in Π' without passing through some edge from D_i to $C_i \parr D_i$ for some i ($1 \leq i \leq k$), a contradiction. But we also cannot have more than two disjoint components arising from Π''', since otherwise Π''' would not be connected. Finally, note that B and the $C_i \parr D_i$ ($1 \leq i \leq k$) are not in the same component. Otherwise, by chosing a switch graph of Π in which the edge from C_i to $C_i \parr D_i$ ($1 \leq i \leq k$) is selected, we would obtain a cycle. Thus, we have three disjoint maximal components, Π_1 containing the C_i and A, Π_2 containing the D_i and B, and Π_3 containing the $C_i \parr D_i$, $i = 1, \ldots, k$.

- It is easily checked that Π_1, Π_2, and Π_3, are deduction nets satisfying the criterion, and that Π_3 has nodes labeled with $C_1 \parr D_1, \ldots, C_k \parr D_k$ among its entry points. □

We can now prove the correctness of the Danos-Regnier criterion [5] (see also Danos [4]).

Theorem 4 *A deduction net Π can be obtained from some sequential deduction (i.e., is of the form $\mathcal{N}(\Pi_0)$ for some sequential deduction Π_0) iff every switch graph associated with Π is a tree.*

Proof. The necessity of the criterion has already been checked in Lemma 29. Thus, we turn to the sufficiency of the criterion. The proof proceeds by induction on the number of nodes in the deduction net. The case where the deduction net has a single node is clear. Otherwise, there are two cases:

Case 1. Some terminal node is labeled with a par, say $A \parr B$. Consider the subgraph Π' obtained from Π by deleting the terminal node in question and the two edges from A to $A \parr B$ and from B to $A \parr B$. We claim that Π' is a deduction net satisfying the correctness criterion. Indeed, if any switch graph obtained from Π' is not a tree, we also obtain a bad switch graph for Π by putting back the node $A \parr B$ and connecting it to either A or B (but not both).

Case 2. Every terminal node is labeled with a tensor.

This case is more delicate, as deleting any terminal node $A \otimes B$ and the edges from A to $A \otimes B$ and from B to $A \otimes B$ does not necessarily yield a deduction net satisfying the correctness criterion. However, we have the following claim:

Claim: There is a least some terminal node labeled $A \otimes B$ such that the subgraph Π' obtained from Π by deleting this terminal node and the two edges from A to $A \otimes B$ and from B to $A \otimes B$ is composed of two disjoint deduction nets Π'_1 (having A as a terminal node) and Π'_2 (having B as a terminal node) which both satisfy the criterion.

If there is a terminal node labeled with a tensor $A \otimes B$ and the claim fails, since Π is connected and has at least two nodes, nodes labeled A and B connected to the node $A \otimes B$ must exist in Π, and A and B must be connected in Π', since otherwise, there would be at

least three maximal connected components, contradicting the fact that Π is connected. Thus, we can apply Lemma 30, and there is a set $\{C_1 \parr D_1, \ldots, C_k \parr D_k\}$ of par nodes such that the graph Π'' obtained from Π' by deleting all edges from C_i to $C_i \parr D_i$ and from D_i to $C_i \parr D_i$, $i = 1, \ldots, k$, consists of three disjoint maximal connected components which are deduction nets satisfying the criterion. Furthermore, without any loss of generality, it can be assumed that one component Π_1 contains both A and the C_i, another component Π_2 contains both B and the D_i, and the third Π_3 contains the $C_i \parr D_i$, $i = 1, \ldots, k$. Since Π_3 is strictly smaller than Π, we conclude that the claim holds for Π_3 by applying the induction hypothesis. Thus, Π_3 is composed of two disjoint deduction nets Π_3' and Π_3'' and of a tensor node $A' \otimes B'$ connected to A' in Π_3' and to B' in Π_3''. Also observe that the graph $\Pi - \Pi_3$ obtained from Π_1, Π_2 by reconnecting the node $A \otimes B$ to A in Π_1 and to B in Π_2, and by reconnecting every node $C_i \parr D_i$ to both C_i in Π_1 and to D_i in Π_2, $i = 1, \ldots, k$, is a deduction net satisfying the criterion. The nodes $C_1 \parr D_1, \ldots, C_k \parr D_k$ must be either all in Π_3' or all in Π_3'', since otherwise, $\Pi - \Pi_3$ being a deduction net, it would be possible to create a cycle between A' and B' in some switch graph of Π. But then, $A' \otimes B'$ is a terminal node of Π satisfying the condition of the claim.

This concludes the proof of the claim, and thus the proof of the theorem. □

If we observe that the cut rule

$$\frac{\vdash \Gamma, A \qquad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} \quad (\textit{cut})$$

behaves just like the following special case of the ($\otimes$: *right*) rule

$$\frac{\vdash \Gamma, A \qquad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta, A \otimes A^\perp} \quad (\otimes\text{: } \textit{right}),$$

we can extend the above treatment of proof nets, including Lemma 29 and Theorem 4, to proof nets including *cut links*, which are links of the form

$$\frac{A \qquad A^\perp}{\text{CUT}} \quad .$$

Every node labeled with CUT is necessarily a terminal node.

The proof of Theorem 4 yields an $O(n^2)$-time algorithm for testing whether a deduction net comes from a sequential deduction. This is not a trivial result, since the naive method yields an exponential-time algorithm. Girard has announced the existence of an $O(n^2)$ algorithm, but as far as we know, no such algorithm has been published. The algorithm presented below works recursively. If the deduction net only has axiom links, the algorithm succeeds iff the deduction net consists of a single axiom link between A and $A^\perp$ or of a single node A (for some proposition A). If the deduction net has some terminal node labeled with a par node $A \parr B$, test recursively the subnets obtained by deleting the edges from $A \parr B$ to A and to B. If the deduction net has terminal nodes only labeled with tensor nodes, try to find a splitting

tensor node as follows. First, for each terminal node $A \otimes B$, delete the edges from $A \otimes B$ to A and to B. Then, find the maximally connected components of this graph. If the resulting graph is connected, the algorithm stops with failure. Otherwise, some terminal node labeled with a tensor $A \otimes B$ has been found such that A and B belong to two disjoint deduction nets Π_1 and Π_2 after the edges from $A \otimes B$ to A and to B have been removed from the original deduction net (there may be several choices, just consider the terminal nodes in some fixed order and pick the first one). Then, test recursively the subnets Π_1 and Π_2.

Since maximally connected components can be found in linear time, the cost of finding a splitting tensor is $O(n)$. It is then clear that the algorithm runs in $O(n^2)$.

Since a proof net is a special deduction net, we also obtain an $O(n^2)$-time algorithm for testing whether a proof net comes from a sequential proof.

8 Conclusion

We have provided an introduction to linear logic, focusing on its propositional fragment. In particular, we describe an algebraic semantics for linear logic, phase semantics. Contrary to Girard's original presentation [7] in which the notions of closure operation and Galois connection are implicit, we present phase semantics explicitly as a specific instance of a Galois connection. We hope that such an approach helps to understand better the motivations for this semantics, and also the reason why linear logic is sound and complete for this semantics. We also define proof nets for multiplicative linear logic and give a direct proof of the correctness of the Danos/Regnier criterion. This proof relies on a purely graph-theoretic decomposition lemma which appears to be new. As a corollary, we obtain an $O(n^2)$-time algorithm for testing the correctness of a proof net. The existence of such an algorithm was conjectured before, but our algorithm appears to be original. In a forthcoming paper, we intend to cover the quantifiers, proof nets for full linear logic, cut elimination, and the semantics of coherent spaces.

9 Appendix: Summary of Notation

The logical constants, logical connectives, and semantic symbols of linear logic are listed below.

I	multiplicative **true**
$\bot$	multiplicative **false**
1	additive **true**
0	additive **false**
$\otimes$	multiplicative **and** (*tensor*)
$\parr$	multiplicative **or** (*par*)
&	addittive **and**
$\oplus$	addittive **or**
$\multimap$	linear (multiplicative) implication
$\multimap\!\!\multimap$	linear (multiplicative) equivalence
$^\bot$	linear (multiplicative) negation
!	of course
?	why not
$\sim$	interpretation of $^\bot$
$\bullet$	interpretation of $\otimes$
$\|$	interpretation of $\parr$
$\square$	interpretation of !

Other symbols are listed below.

$\cup$	binary union
$\cap$	binary intersection
$\bigcup$	union of a family
$\bigcap$	intersection of a family
$\wedge$	binary greatest lower bound
$\vee$	binary least upper bound
$\bigwedge$	greatest lower bound of a family
$\bigvee$	least upper bound of a family
$\in$	set membership
$\subseteq$	set inclusion
$\varnothing$	empty set
$\mapsto$	functional mapping
$\leq$	partial order
†	closure operation
$\equiv$	equivalence relation

References

1. V. M. Abrusci. Sequent calculus for intuitionistic linear propositional logic. In Petio Petrov Petkov, editor, *Mathematical Logic*, pages 223–242. Plenum Press (1990).

2. A. Avron. The semantics and proof theory of linear logic. *Theoretical Computer Science*, 57:161–184 (1988).

3. G. Birkhoff. *Lattice Theory*. Colloquium Publications, Vol. 25. American Mathematical Society, Providence, Rhode Island, third edition (1979).

4. V. Danos. *La Logique Linéaire appliquée à l'étude de divers processus de normalisation (principalement du λ-calcul)*. Thèse de Doctorat, Université de Paris VII (June 1990).

5. V. Danos and L. Regnier. The structure of multiplicatives. *Archive for Mathematical Logic*, 28:181–203 (1989).

6. J.-Y. Girard, Y. Lafont, and P. Taylor. *Proofs and Types*, volume 7 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press (1989).

7. J.-Y. Girard. Linear logic. *Theoretical Computer Science*, 50:1–102 (1987).

8. P. Lincoln, J. Mitchell, A. Scedrov, and N. Shankar. Decision problems for propositional linear logic. Technical Report SRI-CSL-90-08, SRI International (1990).

9. S. MacLane. *Categories for the Working Mathematician*. Springer-Verlag, Berlin (1971).

10. H. Ono. Phase structures and quantales – a semantical study of logics without structural rules. In *Logics with restricted logical rules*, University of Tübingen (October 1990).

11. H. Schellinx. Some syntactical observations on linear logic. *Logic and Computation* (1990). to appear.

12. A. Troelstra. Lectures on linear logic. Technical Report, University of Amsterdam, 1018TV Amsterdam (December 1990).

PRL Research Reports

The following documents may be ordered by regular mail from:

Librarian – Research Reports
Digital Equipment Corporation
Paris Research Laboratory
85, avenue Victor Hugo
92563 Rueil-Malmaison Cedex
France.

It is also possible to obtain them by electronic mail. For more information, send a message whose subject line is `help` to `doc-server@prl.dec.com` or, from within Digital, to `decprl::doc-server`.

Research Report 1: *Incremental Computation of Planar Maps*. Michel Gangnet, Jean-Claude Hervé, Thierry Pudet, and Jean-Manuel Van Thong. May 1989.

Research Report 2: *BigNum: A Portable and Efficient Package for Arbitrary-Precision Arithmetic*. Bernard Serpette, Jean Vuillemin, and Jean-Claude Hervé. May 1989.

Research Report 3: *Introduction to Programmable Active Memories*. Patrice Bertin, Didier Roncin, and Jean Vuillemin. June 1989.

Research Report 4: *Compiling Pattern Matching by Term Decomposition*. Laurence Puel and Ascánder Suárez. January 1990.

Research Report 5: *The WAM: A (Real) Tutorial*. Hassan Aït-Kaci. January 1990.

Research Report 6: *Binary Periodic Synchronizing Sequences*. Marcin Skubiszewski. May 1991.

Research Report 7: *The Siphon: Managing Distant Replicated Repositories*. Francis J. Prusker and Edward P. Wobber. May 1991.

Research Report 8: *Constructive Logics. Part I: A Tutorial on Proof Systems and Typed λ-Calculi*. Jean Gallier. May 1991.

Research Report 9: *Constructive Logics. Part II: Linear Logic and Proof Nets*. Jean Gallier. May 1991.

Research Report 10: *Pattern Matching in Order-Sorted Languages*. Delia Kesner. May 1991.

Research Report 11: *Towards a Meaning of LIFE*. Hassan Aït-Kaci and Andreas Podelski. June 1991.

Research Report 12: *Residuation and Guarded Rules for Constraint Logic Programming*. Gert Smolka. June 1991.

Research Report 13: *Functions as Passive Constraints in LIFE*. Hassan Aït-Kaci and Andreas Podelski. June 1991.

Research Report 14: *Automatic Motion Planning for Complex Articulated Bodies*. Jérôme Barraquand. June 1991.