A Lazy Logician's Guide to Linear Logic

Jennifer Davoren

July 1991

Department of Mathematics
Monash University
Clayton, Vic 3168
Australia

From August 1991:
Department of Mathematics
Cornell University
Ithaca, NY 14853
U.S.A.

A Lazy Logician's Guide to Linear Logic

0. Introduction

The purpose of these notes is to provide an accessible introduction to the main concepts of linear logic. The seminal work in this new area of research is the paper by Jean-Yves Girard, "Linear Logic", Theoretical Computer Science, 50 (1987), 1-102 (subsequently, Girard [1987]). This lengthy report is not recommended for light bed-time reading; its quite substantial content demands many hours in a quiet room and a good supply of pencils and paper. Over the last few years, the literature on linear logic has been growing at a rather more than linear rate. However, the bulk of these papers, including introductory expositions such as Lafont [1988a] and Seely [1989], are to be found in journals or conference proceedings whose intended audience consists of computer scientists and/or category theorists. We hope that these notes will be of use to logicians of other pursuasions. We will attempt to make perspicuous the rather elegant mathematics underlying linear logic.

Our basic reference is Girard [1987]. We work through much of that paper, filling out details, supplying proofs of lemmas, rearranging things etc. Section 5 also incorporates work from Girard, Lafont and Taylor [1989]. Departures from and modifications to the original are noted, as are references to other papers. One departure is our omission of propositional quantifiers, specifically the treatment of them in Chapters 3 and 4, on coherent spaces and proof nets respectively, of Girard [1987]. Readers keen to go higher order will need a good grip on ground level stuff; hopefully they'll get that here. In spite of justifiable complaints by a number of researchers (eg. Avron [1988], Seely [1989]) about Girard's choice of notation for his logical operators, we have stuck to the original. Appendix A consists of a translation table which may be helpful to readers of Seely [1989], Avron [1988] or anyone familiar with relevance logics.

To get a feel for what linear logic is on about, consider Hilbert-style axiomatic systems where the only rule of inference is Modus Ponens (MP), as in Avron [1988]. We restrict our attention to the implicational fragment of a language for propositional logic. We can characterize a <u>linear proof</u> as one in which every occurrence of a formula other than the last is used <u>exactly once</u> as a premise of MP. In contrast, the proofs appropriate to the system $\mathbf{R}_{\rightarrow}$ (the implicational subsystem of the relevance logic $\mathbf{R}$) are those in which every occurrence of a formula other than the last is used <u>at least once</u> as a premise of MP. In terms of Gentzen sequent calculi, systems for linear logic have neither contraction nor thinning among their structural rules; in the system for $\mathbf{R}$, thinning is dropped but contraction is retained. Thinning (also known as weakening) gives rise to spurious dependencies ('irrelevancies') such as $A \rightarrow (B \rightarrow A)$; in a proof of such a formula, the hypothesis B is not used, so we have wastage. Contraction allows an occurrence of a formula to be used over and over again; roughly, this means that the first time you get something, you pay for it, but after that you're getting stuff for free. In linear logic, nothing is wasted and nothing is gotten for free. (For more on the intuitive content of linear logic, see Section 4 below.)

Linear logic is attracting quite a lot of attention in the computer science community. Regrettably, the author is almost totally ignorant of computer science so is in no position to say anything about the significance of linear logic for this field. The reader is referred to Lafont [1988b], which is an extended version of Girard and Lafont [1987]. Lafont introduces the 'Linear Abstract Machine' as a technique of implementing functional programming languages based on *intuitionistic* linear logic, i.e. in the sequent calculus for this logic, the right sides of sequents contain at most one formula; see Appendix B for the two-sided sequent calculi for 'classical' and intuitionistic linear logic. The memory allocation in Lafont's implementation is such that there is no need for a *garbage collector*; very roughly, the sort of *waste* produced by thinning is what you would need a garbage collector for. In addition, the Linear Abstract Machine permits a synthesis of *strict* and *lazy* evaluation strategies: 'call by value' along side 'call by need'. (For those who have read ahead, the multiplicative $A \otimes B$ is a type of strict pairs while the additive $A \& B$ is a type of lazy pairs; we have no *need* to say any more about the matter here.) For more on the import of linear logic for the study of parallelism, see the introduction to Girard [1987] and the essay "Towards a Geometry of Interaction", Girard [1989]. The latter presents 'a program for proof theory inspired by its growing connections with computer science'.

These notes are based on material presented in a series of fifteen seminars held at the University of Melbourne, March – July 1991. The author wishes to thank, for invaluable comments and corrections, the regular participants: Jacinta Covington, Allen Hazen, David Odell (University of Melbourne) and Daniel Mahler (Monash University), and the irregular participants: Kevin Davey, John Collins, Lloyd Humberstone (Monash), David Kinnick and Harald Sondergaard (Melbourne).

1. Sequent calculi

1.0 Additives and multiplicatives

Suppose our lazy logician has a dim recollection of reading Schwichtenberg [1977], remembering only that a one-sided sequent calculus for classical logic means that there is only half as many rules to write out and deal with. Each two-sided sequent of the form

$$A_1, \ldots, A_n \vdash B_1, \ldots, B_m$$

is replaced by:

$$\vdash \sim A_1, \ldots, \sim A_n, B_1, \ldots, B_m .$$

Being a bit woolly on the details, our lazy logician hesitates between the following two possible rules for conjunction:

$$\frac{\vdash A, \Delta \qquad \vdash B, \Delta}{\vdash A \wedge B, \Delta} \qquad\qquad \frac{\vdash A, \Delta \qquad \vdash B, \Gamma}{\vdash A \wedge B, \Delta, \Gamma}$$

If we have the rules of thinning and contraction:

$$\frac{\vdash \Delta}{\vdash A, \Delta} \qquad \text{and} \qquad \frac{\vdash A, A, \Delta}{\vdash A, \Delta}$$

respectively, then with thinning we can derive the second of the conjunction rules from the first, and with contraction we can derive the first from the second.

Our lazy logician agrees to drop thinning and contraction: at the least, there will be a few less cases to worry about in the proof of Gentzen's Hauptsatz (Cut Elimination theorem). Moreover, contraction is responsible for the undecidability of predicate calculus. The sub-formula property (corollary of the Hauptsatz) yields a (theoretical) decision procedure for predicate calculus, provided a bound can be placed on the length of any sequent occurring in a cut-free proof. In the absence of contraction, all sequents occurring in a cut-free proof have length less than or equal to the length of the end sequent. (This is noted in Girard [1989], p.79, and elsewhere.)

In linear logic we have <u>two</u> quite different conjunctions:

- an <u>additive</u> conjunction & (called 'with'), characterized by the rule

$$\frac{\vdash A, \Delta \qquad \vdash B, \Delta}{\vdash A \& B, \Delta} \ (\&)$$

  i.e. two copies of the same parametric sequence are identified, giving a type of implicit contraction; and

- a <u>multiplicative</u> conjunction ⊗ (called 'times'), characterized by the rule

$$\frac{\vdash A, \Delta \qquad \vdash B, \Gamma}{\vdash A \otimes B, \Delta, \Gamma} \ (\otimes)$$

  i.e. parametric sequences are accumulated.

(The terms 'additive' and 'multiplicative', as well as the buzz word 'linear', have their origins in the coherent semantics for linear logic: see Section 5 below. With respect to the relevance logic tradition, 'additive' corresponds to 'extensional' and 'multiplicative' to 'intensional'.)

The absence of thinning and contraction also gives rise to two distinct verum-like constants:

- an additive one, $\top$, characterized by the axiom scheme:

  $$\vdash \top, \Delta$$

  where Δ is any sequence of formulae; and

- a multiplicative one, $\mathbb{1}$, characterized by the axiom:

  $$\vdash \mathbb{1}$$

A suprising feature of linear logic is that although it is constructive — propositional intuitionistic logic is faithfully translatable into modal linear logic — it retains an <u>involutive</u> negation, $(-)^\perp$. (We pronounce it 'perp'.) As a consequence, de Morgan-style duality is rife within linear logic:

- the additive disjunction $\oplus$ ('plus') is the de Morgan dual of $\&$;
- the multiplicative disjunction $⅋$ ('par') is the de Morgan dual of $\otimes$;
- the additive falsum-like constant $\mathbb{0}$ is the linear negation of $\top$; and
- the multiplicative falsum-like constant $\perp$ is the linear negation of $\mathbb{1}$.

(We pronounce $\perp$ as 'eet'.)

We get a rather sleek syntax and sequent calculus for linear logic if we take the symbols $\oplus, \wp, 0$ and $\perp$ as primitive, in addition to $\&, \otimes, \top$ and $\mathbb{1}$, and then introduce $(-)^\perp$ by <u>definition</u>. A symbol for linear implication, $\multimap$, ('entails'; we usually call it 'lollipop') will also be introduced by definition:

$$A \multimap B \overset{\text{df}}{=} A^\perp \wp B$$

i.e. the multiplicative analogue of material implication. Justification for this act of definitional fiat with respect to linear negation and linear implication will be found in the phase space semantics (Section 2).

Historically, Girard first worked with linear implication, by way of a 'decomposition' of intuitionistic implication (see sections 3.3 and 5.3 below) and then built the rest of the logic around it.

Some readers may be justifiably perplexed by the weird symmetries in Girard's notation:

	CONJUNCTION	VERUM-LIKE	DISJUNCTION	FALSUM-LIKE
ADDITIVE	$\&$	$\top$	$\oplus$	0
MULTIPLICATIVE	$\otimes$	$\mathbb{1}$	$\wp$	$\perp$

In particular, why doesn't the notation reflect the de Morgan dualities? Girard seems to want to stress that the multiplicative connectives distribute over their <u>notationally</u> similar additives (see section 1.3 below). One may also derive some consolation from the fact that it will turn out that the category of finite dimensional vector spaces over a field K, $\mathbf{Vect}_K$, whose morphisms are linear maps, is a model of linear logic. The multiplicative $\otimes$ is interpretted as the tensor product $\otimes$, the additive $\oplus$ is the direct sum $\oplus$ and linear negation $(-)^{\perp}$ is the duality operator $(-)^{*}$. (See section 5.4 below.) So linear logic has something to do with linear algebra.

1.1 The sequent calculi **LL** and **LLM**.

In later work we will need to refer to the pure multiplicative fragment, i.e. the symbols $\otimes$ and $⅋$ but not the constants $\mathbb{1}$ and $\perp$, so we allow for this in our definitions here.

Definition 1.1.0:
We have symbols of the following kinds:
- (i) connective symbols: $\otimes$, $⅋$, $\&$, $\oplus$;
- (ii) constants: $\mathbb{1}, \perp, \top, \mathbb{O}$;
- (iii) literals:
  - (a) propositional letters: $p, q, r, \ldots$
  - (b) the duals of propositional letters: $p^{\perp}, q^{\perp}, r^{\perp}, \ldots$

The language $\mathcal{L}$ of (propositional) linear logic is defined as follows:
- constants and literals are formulae in $\mathcal{L}$;
- if A and B are formulae in $\mathcal{L}$ then so are $A \otimes B$, $A ⅋ B$, $A \& B$ and $A \oplus B$.

The language $\mathcal{L}_m$ of the pure multiplicative fragment of linear logic is defined as follows:
- literals are formulae in $\mathcal{L}_m$;
- if A and B are formulae in $\mathcal{L}_m$ then so is $A \otimes B$ and $A ⅋ B$.

Constants and literals are atomic formulae of $\mathcal{L}$; literals are atomic formulae of $\mathcal{L}_m$.

Definition 1.1.1:
The expression $(A)^\perp$ where A is a formulae in $\mathcal{L}$ ($\mathcal{L}_m$) is defined as follows:

$$(\mathbb{1})^\perp \stackrel{df}{=} \perp \qquad (\perp)^\perp \stackrel{df}{=} \mathbb{1}$$

$$(\top)^\perp \stackrel{df}{=} \mathbb{0} \qquad (\mathbb{0})^\perp \stackrel{df}{=} \top$$

if p is a propositional letter, $(p^\perp)^\perp \stackrel{df}{=} p$;
if A and B are formulae in $\mathcal{L}$ ($\mathcal{L}_m$),

$$(A \otimes B)^\perp \stackrel{df}{=} (A)^\perp \parr (B)^\perp \qquad (A \parr B)^\perp \stackrel{df}{=} (A)^\perp \otimes (B)^\perp \, ;$$

if A and B are formulae in $\mathcal{L}$,

$$(A \& B)^\perp \stackrel{df}{=} (A)^\perp \oplus (B)^\perp \qquad (A \oplus B)^\perp \stackrel{df}{=} (A)^\perp \& (B)^\perp .$$

The expression $A \multimap B$, where A and B are formulae in $\mathcal{L}$, is defined as follows:

$$A \multimap B \stackrel{df}{=} (A)^\perp \parr B \, .$$

Parentheses may be omitted where appropriate.

Note that formulae in $\mathcal{L}$ are automatically in negation-normal form. Capital Roman letters A, B, C, D, E will be used solely as metalinguistic variables ranging over $\mathcal{L}$ (or $\mathcal{L}_m$). Metalinguistically, we have the identity

$$A^{\perp\perp} = A \, .$$

Definition 1·1·2:

An $\mathcal{L}$-sequent ($\mathcal{L}_m$-sequent) is an expression of the form

$$\vdash A_1, \ldots, A_n$$

where $A_1, \ldots, A_n$ are formulae in $\mathcal{L}$ ($\mathcal{L}_m$).
We use capital Greek letters $\Delta, \Gamma, \Sigma, \Theta$ to denote sequences of formulae.
If Δ is the empty sequence, then $\vdash \Delta$ has the same meaning as $\vdash \perp$.

The sequent calculus **LL** consists of the axiom schemes:

identity: $\vdash A, A^{\perp}$ where A is a propositional letter

additive: $\vdash \top, \Delta$

multiplicative: $\vdash \mathbb{1}$

and the following inference rules:

structural:
$$\frac{\vdash \Delta}{\vdash \sigma(\Delta)}\ (\text{EXCH}) \qquad \frac{\vdash A, \Delta \quad \vdash A^{\perp}, \Gamma}{\vdash \Delta, \Gamma}\ (\text{CUT})$$

where σ is any permutation of Δ

additive:
$$\frac{\vdash A, \Delta \quad \vdash B, \Delta}{\vdash A \& B, \Delta}\ (\&) \qquad \frac{\vdash A, \Delta}{\vdash A \oplus B, \Delta}\ (\text{FST}\oplus) \qquad \frac{\vdash B, \Delta}{\vdash A \oplus B, \Delta}\ (\text{SND}\oplus)$$

multiplicative:
$$\frac{\vdash A, \Delta \quad \vdash B, \Gamma}{\vdash A \otimes B, \Delta, \Gamma}\ (\otimes) \qquad \frac{\vdash A, B, \Delta}{\vdash A \parr B, \Delta}\ (\parr) \qquad \frac{\vdash \Delta}{\vdash \perp, \Delta}\ (\perp)$$

The sequent calculus **LLM** consists of the axiom scheme of identity and the inference rules (EXCH), (CUT), ($\otimes$) and ($\parr$).

The restriction of the identity axiom scheme to propositional letters is due to the following:

(i)
$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash A, A^{\perp}}{\vdash A^{\perp}, A}\,(\mathrm{EXCH})}{\vdash A^{\perp}\oplus B^{\perp}, A}\,(\mathrm{FST}\oplus)}{\vdash A, A^{\perp}\oplus B^{\perp}}\,(\mathrm{EXCH}) \qquad \dfrac{\dfrac{\dfrac{\vdash B, B^{\perp}}{\vdash B^{\perp}, B}\,(\mathrm{EXCH})}{\vdash A^{\perp}\oplus B^{\perp}, B}\,(\mathrm{SND}\oplus)}{\vdash B, A^{\perp}\oplus B^{\perp}}\,(\mathrm{EXCH})}{\vdash A\& B,\ A^{\perp}\oplus B^{\perp}}\,(\&)$$

(ii)
$$\vdash \top, 0$$

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

(iv)
$$\dfrac{\vdash \mathbb{1}}{\vdash \perp, \mathbb{1}}\,(\perp)$$

In view of the inference rule $(\parr)$, an $\mathcal{L}$-sequent or $\mathcal{L}_m$-sequent

$$\vdash A_1, \ldots, A_n$$

will be given the same semantic interpretation as the formula

$$A_1 \parr \ldots \parr A_n .$$

(Associativity is not going to be a problem).

In virtue of the structural rule (EXCH), we could work with multi-sets of formulae rather than sequences of formulae; we still have to distinguish <u>occurrences</u> of formulae.

Gentzen's proof of the Hauptsatz for the classical sequent calculus **LK** can be readily modified (working on cuts directly rather than on <u>mixes</u>, the latter requiring thinning) to give

<u>Proposition 1·1·3</u>: (Hauptsatz for **LL**)
If π is a proof of $\vdash \Delta$ in **LL**
then π can be transformed into a proof π' of $\vdash \Delta$
in which the inference rule (CUT) is not used. ■

Thistlewaite, McRobbie and Meyer [1988] have independently devised a one-sided sequent calculus strikingly similar to **LL**. Their system, for the relevance logic '**R** minus distribution', is the same as **LL** <u>plus</u> contraction. 'Distribution' in this context is an axiom scheme expressing the distributivity of additive conjunction over additive disjunction; it is conventionally adjoined to the relevance logic **R**. In the notation of linear logic, the axiom scheme is

$$A \,\&\, (B \oplus C) \multimap (A \,\&\, B) \oplus C .$$

With contraction, one readily derives

$$A \,\&\, (B \oplus C) \multimap (A \,\&\, B) \oplus (A \,\&\, C).$$

For more on the relation between linear logic and relevance logics, see Avron [1988].

In Appendix B, we set out the two-sided sequent calculus for standard, 'classical', linear logic and for intuitionistic linear logic.

1.2 Some theorems of **LL**

Definition 1.2.0:
A is a theorem of **LL** iff the sequent $\vdash A$ is provable in **LL**. A and B are provably equivalent in **LL**, written $A \equiv_{LL} B$, iff both $A \multimap B$ and $B \multimap A$ are theorems of **LL**.

Lemma 1.2.1:
The following are provable equivalences in **LL** (omitting the subscript **LL**):

(i) associativity and commutativity:

$$A \& (B \& C) \equiv (A \& B) \& C \qquad A \& B \equiv B \& A$$
$$A \oplus (B \oplus C) \equiv (A \oplus B) \oplus C \qquad A \oplus B \equiv B \oplus A$$
$$A \otimes (B \otimes C) \equiv (A \otimes B) \otimes C \qquad A \otimes B \equiv B \otimes A$$
$$A \invamp (B \invamp C) \equiv (A \invamp B) \invamp C \qquad A \invamp B \equiv B \invamp A$$

(ii) constants:

$$\top \& A \equiv A \qquad 0 \oplus A \equiv A$$
$$1 \otimes A \equiv A \qquad \bot \invamp A \equiv A$$
$$0 \otimes A \equiv 0 \qquad \top \invamp A \equiv \top$$
$$1 \multimap A \equiv A \qquad A \multimap \bot \equiv A^{\bot}$$
$$0 \multimap A \equiv \top \qquad A \multimap \top \equiv \top$$

(iii)

$$A \multimap B \equiv B^{\bot} \multimap A^{\bot}$$
$$(A \otimes B) \multimap C \equiv A \multimap (B \multimap C)$$
$$A \multimap (B \invamp C) \equiv (A \multimap B) \invamp C$$

(iv) distributivity of multiplicatives over 'opposite' additives:

$$A \otimes (B \oplus C) \equiv (A \otimes B) \oplus (A \otimes C)$$
$$A \parr (B \& C) \equiv (A \parr B) \& (A \parr C)$$

$$(A \oplus B) \multimap C \equiv (A \multimap C) \& (B \multimap C)$$
$$A \multimap (B \& C) \equiv (A \multimap B) \& (A \multimap C)$$

The following are theorem schemes for **LL**:

(vi) half-distributivity of multiplicatives over 'like' additives:

$$A \otimes (B \& C) \multimap (A \otimes B) \& (A \otimes C)$$
$$(A \parr B) \oplus (A \parr C) \multimap A \parr (B \oplus C)$$

$$(A \multimap C) \oplus (B \multimap C) \multimap ((A \& B) \multimap C)$$
$$(A \multimap B) \oplus (A \multimap C) \multimap (A \multimap (B \oplus C))$$

(vii) half-distributivity of additives:

$$(A \& B) \oplus (A \& C) \multimap A \& (B \oplus C)$$
$$A \oplus (B \& C) \multimap (A \oplus B) \& (A \oplus C)$$

(viii) weak distributivity of multiplicatives:

$$A \otimes (B \parr C) \multimap (A \otimes B) \parr C$$

Proof: We will only exhibit proofs for (vii) and (viii). The reader is invited to try one of the others for their own edification. The first equivalence in (iv) is 'borrowed' from linear algebra: the distributivity of the tensor product over direct sum. In (vii), read $\&$ as 'meet', $\oplus$ as 'join' and $\multimap$ as inclusion; such a translation yields general properties of lattices (see section 2.1 below).

We omit exchanges.

(vii)

$$
\dfrac{
\dfrac{
\dfrac{\vdash A, A^{\perp}}{\vdash A, A^{\perp}\oplus B^{\perp}}(\mathrm{FST}\oplus)
\quad
\dfrac{\dfrac{\vdash B, B^{\perp}}{\vdash B, A^{\perp}\oplus B^{\perp}}(\mathrm{SND}\oplus)}{\vdash B\oplus C, A^{\perp}\oplus B^{\perp}}(\mathrm{FST}\oplus)
}{\vdash A^{\perp}\oplus B^{\perp}, A\,\&\,(B\oplus C)}(\&)
\quad
\dfrac{
\dfrac{\vdash A, A^{\perp}}{\vdash A, A^{\perp}\oplus C^{\perp}}(\mathrm{FST}\oplus)
\quad
\dfrac{\dfrac{\vdash C, C^{\perp}}{\vdash C, A^{\perp}\oplus C^{\perp}}(\mathrm{SND}\oplus)}{\vdash B\oplus C, A^{\perp}\oplus C^{\perp}}(\mathrm{SND}\oplus)
}{\vdash A^{\perp}\oplus C^{\perp}, A\,\&\,(B\oplus C)}(\&)
}{
\dfrac{\vdash (A^{\perp}\oplus B^{\perp})\,\&\,(A^{\perp}\oplus C^{\perp}),\ A\,\&\,(B\oplus C)}{\vdash ((A^{\perp}\oplus B^{\perp})\,\&\,(A^{\perp}\oplus C^{\perp}))\mathbin{⅋}(A\,\&\,(B\oplus C))}(⅋)
}(\&)
$$

(viii)

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

∎

The restricted sequent calculus **LLM** is highly <u>conservative</u>.

<u>Observation 1.2.2:</u>
Let π be a cut-free proof of $\vdash \Delta$ in **LLM**, and let $\vdash A_1, A_1^{\perp}, \ldots, \vdash A_n, A_n^{\perp}$ be a list of all the instances of the identity axiom scheme which occur in π. Then the atomic subformulae (literals) of Δ are exactly $A_1, A_1^{\perp}, \ldots, A_n, A_n^{\perp}$.

This is established by a simple induction on the proof of $\vdash \Delta$.

Observation 1·2·3:

Let $\vdash \Delta$ be any provable sequent of **LLM**, and let $A_1, \ldots, A_n$ be a list of all occurrences (as atomic subformulae) of positive literals in Δ. Then the negative literals occurring in Δ are exactly $A_1^{\perp}, \ldots, A_n^{\perp}$. i.e. cuts destroy literals in dual pairs.

Observation 1·2·4:

(i) A formula of $\mathcal{L}_M$ of the form

$$A \multimap (A \otimes A)$$

is a theorem of **LLM** iff A is a theorem of **LLM**.

(ii) No formula of $\mathcal{L}_M$ of the form

$$(A \otimes B) \multimap A$$

where $B \neq A \parr A^{\perp}$ and $B \neq A^{\perp} \parr A$, is a theorem of **LLM**.

Formulae of type (i) are characteristic of contraction. Those of type (ii) are symptoms of thinning; $(A \otimes B) \multimap A$ is provably equivalent to $A \multimap (B \multimap A)$ by the associativity of $\parr$.

When we extend the sequent calculus from **LLM** to **LL**, we lose the balance of positive and negative literals (and hence have a more interesting logic). However, the analogue for $\mathcal{L}$ of 1·2·4 (i) still holds for **LL** and formulae of $\mathcal{L}$ of the form $(A \otimes B) \multimap A$ are not, in general, theorems of **LL** (but there are more cases to exclude).

Let us consider the axioms schemes and inference rules of **LL** a little more closely. The axiom scheme for $\top$ is generous, but harmlessly so. Observe that if an instance of the axiom scheme for $\top$ occurs in an **LL** proof, then there must be an occurrence of $\top$ in the end sequent (so $\top$'s can't be 'cut-out' completely). The rule ($\perp$) allows us to 'thin-in' as many copies of $\perp$ as we like. The rules (FST$\oplus$) and (SND$\oplus$) also involve a type of thinning, at the level of subformulae, but are still conservative with respect to parametric sequences. Otherwise put, these rules, like ($\otimes$) and ($\wp$), act <u>locally</u>, i.e. only on principal formulae. In contrast, the rule ($\&$), with its requirement that the two premise sequents contain the same parametric sequences, involves a <u>global</u> constraint. In our later work with an alternative proof procedure (the system of 'proof nets', in section 6) we will have trouble dealing with $\&$ because of this constraint. (The problem is familiar to relevance logicians: see Dunn [1986] or Avron [1988].)

2. Phase space semantics

In this section we give an algebraic semantics for linear logic and prove the soundness and completeness of **LL** with respect to this semantics. This is, as Girard puts it, a 'Tarskian-style' semantics and in virtue of completeness we get an 'official blessing' for the system **LL**. In Section **5** we present an alternative, 'disturbing' semantics in terms of coherent spaces, which Girard takes to be more in the tradition of Heyting. Coherent spaces emerge from a reworking of Dana Scott's theory of domains (models for intuitionistic logic / typed λ-calculus). Girard uses them to show how linear implication results from a 'decomposition' of intuitionistic implication. In the framework of coherent spaces, we can naturally associate a semantic object with each proof in **LL**.

But first we must bestow upon **LL** a nihil obstat.

2.0 Phase spaces and facts

Definition 2.0.0:

A phase space is a quadruple $\langle P, \cdot, 1, \perp_P \rangle$ consisting of

(i) a commutative monoid $\langle P, \cdot, 1 \rangle$,

i.e. satisfying (a) for all $p, q, r \in P$, $\quad p(qr) = (pq)r$

(b) for all $p \in P$, $\quad p1 = 1p = p$

and (c) for all $p, q \in P$, $\quad pq = qp$

and

(ii) a distinguished subset $\perp_P \subseteq P$.

The elements $p \in P$ are called <u>phases</u> and $\perp_P$ is the set of <u>orthogonal phases</u> of $\langle P, \cdot, 1, \perp_P \rangle$.

As the first of many abuses of notation, we shall refer to P as a phase space and drop the subscript on $\perp_P$ when the context makes it clear. We are going to interpret formulae in $\mathcal{L}$ by certain subsets of P; not suprisingly, $\perp_P$ will be the interpretation of the constant $\perp$. In what follows, we will re-use (and abuse) the connective symbols of $\mathcal{L}$ in giving definitions of the corresponding semantic operations.

<u>Definition 2.0.1</u>:
Let $G \subseteq P$ be any subset. We define the <u>dual</u> of G, written $G^\perp$, as follows:

$$G^\perp \overset{df}{=} \{ q \in P \mid \text{for all } p \in G \, (pq \in \perp) \}$$

So $G^\perp$ consists of those q which send all of G into $\perp$. Observe that for any $p \in P$,

$$\{p\}^\perp = \{ q \in P \mid pq \in \perp \}$$

and for any $G \subseteq P$,

$$G^\perp = \bigcap \{ \{p\}^\perp \mid p \in G \}$$

<u>Definition 2.0.2</u>:
Let $G \subseteq P$. G is a <u>fact</u> of P iff $G^{\perp\perp} = G$.
A fact G is <u>verified</u> in P iff $1 \in G$.

Girard thinks of the $p \in G$, where G is a fact of P, as phases 'between the fact and its verification', or tasks to be undertaken in order to verify G. When $1 \in G$, there are no tasks to do; G is verified in P. If we write '$p \models G$' instead of '$p \in G$' (as Girard does in his introductory discussion) the connection with Kripke-style semantics becomes clearer. (cf. Dunn [1986] on the semantics of relevance logics.)

<u>Lemma 2·0·3</u>: (Girard [1987])
Let $G, H \subseteq P$.

(i) $G \subseteq G^{\perp\perp}$;

(ii) $G^{\perp\perp\perp} = G^{\perp}$;

(iii) if $G \subseteq H$ then $H^{\perp} \subseteq G^{\perp}$;

(iv) G is a fact of P iff $G = H^{\perp}$ for some $H \subseteq P$.

(v) if H is a fact of P and $G \subseteq H$ then $G^{\perp\perp} \subseteq H$.

<u>Proof</u>:

(i) Let $p \in G$. Then for all $q \in G^{\perp}$, $pq \in \perp$. But

$$G^{\perp\perp} = \{p \in P \mid \text{for all } q \in G^{\perp} \, (pq \in \perp)\}.$$

Hence $p \in G^{\perp\perp}$.

(ii) By (i), $G^{\perp} \subseteq G^{\perp\perp\perp}$.
Let $q \in G^{\perp\perp\perp}$. Then for all $p \in G^{\perp\perp}$, $pq \in \perp$. Since $G \subseteq G^{\perp\perp}$, we have that for all $p \in G$, $pq \in \perp$.
Hence $q \in G^{\perp}$.

(iii) Similar argument to (ii).

(iv) Immediate consequence of (ii).

(v) Let $S = \bigcap \{H \subseteq P \mid G \subseteq H \text{ and } H = H^{\perp\perp}\}$.
Then $G \subseteq S \subseteq G^{\perp\perp}$. By (iii), $G^{\perp\perp} \subseteq S^{\perp\perp} \subseteq G^{\perp\perp\perp\perp}$.
By (ii), $G^{\perp\perp\perp\perp} = G^{\perp\perp}$, hence $G^{\perp\perp} = S^{\perp\perp}$.
To obtain $S = S^{\perp\perp}$, we need the following result.

Lemma 2.0.4: (Girard [1987])

If $\{G_i\}_{i\in I}$ is any family of facts of P then

$$\bigcap_{i\in I} G_i = \Big(\bigcup_{i\in I} G_i^{\perp}\Big)^{\perp}.$$

Hence the intersection of any family of facts is a fact.

Proof:

First observe that

$$\bigcup_{i\in I} G_i^{\perp} = \bigcup_{i\in I} \bigcap_{p\in G_i} \{q \mid pq \in \perp\}$$

Let $q \in \bigcup_{i\in I} G_i$. Then for some $i \in I$, and for all $p \in G_i$, $pq \in \perp$.
Thus if $p \in \bigcap_{i\in I} G_i$ then $pq \in \perp$, hence $p \in \big(\bigcup_{i\in I} G_i^{\perp}\big)^{\perp}$.
Conversely, let $p \in \big(\bigcup_{i\in I} G_i^{\perp}\big)^{\perp}$. Then for each $i \in I$, if $q \in G_i^{\perp}$ then $q \in \bigcup_{i\in I} G_i^{\perp}$ hence $pq \in \perp$. Hence $p \in \bigcap_{i\in I} G_i^{\perp\perp}$.
Since $G_i = G_i^{\perp\perp}$, we have $p \in \bigcap_{i\in I} G_i$. ∎

Corollary 2.0.5:

For any $G \subseteq P$,

$$\Big(\bigcup\{\{p\}^{\perp\perp} \mid p \in G\}\Big)^{\perp\perp} = G^{\perp\perp}.$$

∎

Definition 2.0.6:

$$\mathrm{Fact}(P) = \{ G \subseteq P \mid G = G^{\perp\perp} \}.$$

Fact(P) is partially ordered by inclusion. Note that $G \in \mathrm{Fact}(P)$ iff G is the intersection of some family of duals of singletons, i.e. $G = \bigcap \{ \{p\}^{\perp} \mid p \in H \}$ for some set $H \subseteq P$.

Lemma 2.0.3 (i)—(iii) implies that $(-)^{\perp\perp}$ is a closure operator on P. So by detouring via a standard result in lattice theory (eg. Burris and Sankappanavar [1981], I.5.2) we could have bypassed 2.0.4 and concluded that the poset $\langle \mathrm{Fact}(P), \subseteq \rangle$ is a complete lattice, with

$$\bigwedge_{i \in I} G_i = \bigcap_{i \in I} G_i \quad \text{and} \quad \bigvee_{i \in I} G_i = \Big(\bigcup_{i \in I} G_i \Big)^{\perp\perp}$$

where $\{G_i\}_{i \in I}$ is any family of facts of P.

Examples 2.0.7:

(i) $\perp \in \mathrm{Fact}(P)$ since $\perp = \{1\}^{\perp}$.

(ii) Define $\mathbb{1} \overset{\mathrm{df}}{=} \perp^{\perp}$ so $\mathbb{1} \in \mathrm{Fact}(P)$. Now

$$\mathbb{1} = \{ p \in P \mid \text{for all } q \in \perp \ (pq \in \perp) \}$$

Thus $1 \in \mathbb{1}$ and if $p \in \mathbb{1}$ and $r \in \mathbb{1}$ then $pr \in \mathbb{1}$. Hence $\mathbb{1}$ is a submonoid of P. Moreover, if $p \in \mathbb{1}$ and $q \in G$, for any subset $G \subseteq P$, then $pq \in G^{\perp\perp}$.

Observe that $G \in \mathrm{Fact}(P)$ is verified in P exactly when G contains $\mathbb{1}$:

$$1 \in G \text{ iff } G^{\perp} \subseteq \perp \text{ iff } \mathbb{1} \subseteq G, \text{ assuming } G = G^{\perp\perp}.$$

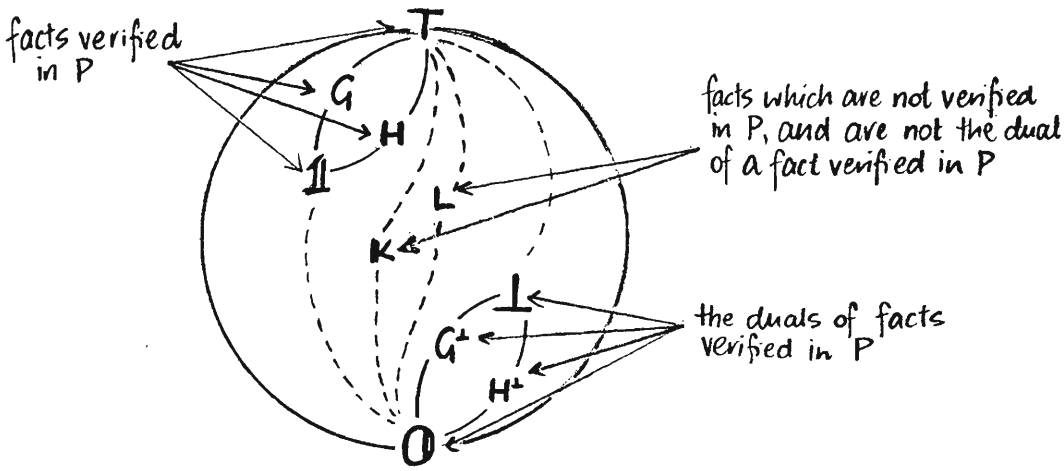
(iii) Define $\top \overset{df}{=} \emptyset^{\perp}$, hence $\top = P \in Fact(P)$.

(iv) Define $\mathbb{O} \overset{df}{=} \top^{\perp}$. Then $\mathbb{O} \in Fact(P)$, and since

$$\mathbb{O} = \{ p \in P \mid \text{for all } q \in P \, (pq \in \perp) \}$$

We have $\mathbb{O} \subseteq G$ for all $G \in Fact(P)$.
Trivially, $G \subseteq \top$ for all $G \in Fact(P)$,
hence $\langle Fact(P), \subseteq \rangle$ is a bounded lattice. (Henceforth, we'll use '$Fact(P)$' to refer to both the lattice and its underlying set.)

The general picture of $Fact(P)$ is as follows:



By construction, $(-)^{\perp}$ is an involution on $Fact(P)$, but it is well removed from classical negation. We certainly <u>don't</u> have, for all $G \in Fact(P)$, either $1 \in G$ or $1 \in G^{\perp}$. Moreover, there is nothing to rule out the possibility of <u>both</u> $1 \in G$ and $1 \in G^{\perp}$, for some $G \in Fact(P)$. However, we do have the following

<u>Lemma 2.0.8:</u>

There is a $G \in Fact(P)$ such that $1 \in G$ and $1 \in G^{\perp}$ iff $1 \in \perp_P$.

<u>Proof</u>:

Suppose $G \in Fact(P)$ is such that $1 \in G$ and $1 \in G^{\perp}$. Then $G^{\perp} \subseteq \perp$ and $\mathbb{1} \subseteq G^{\perp}$. Hence $\mathbb{1} \subseteq \perp$, so $1 \in \perp$.
Conversely, suppose $1 \in \perp$. But $1 \in \mathbb{1}$ always, so we are done.

■

Phase spaces $\langle P, \cdot, 1, \perp_P \rangle$ such that $1 \in \perp_P$ are a bit weird, if not outright pathalogical. Now as a Corollary to the Hauptsatz, we have that $\vdash \perp$ is not provable in **LL**. (Note that this only gives a weak consistency; the provability of the empty sequent is only <u>really</u> dangerous in the presence of weakening.) Once we have proved the completeness of **LL**, we'll have a guarrantee that not all phase spaces are pathalogical.

2.1 <u>The Additives</u>

Obviously, the additives are the lattice operations on $Fact(P)$.

<u>Definition 2.1.0</u>:
Let $G, H \in Fact(P)$.
Define

$$G \& H \stackrel{df}{=} G \cap H \quad \text{and} \quad G \oplus H \stackrel{df}{=} (G \cup H)^{\perp\perp}.$$

<u>Observation 2.1.1</u>:
Since $Fact(P)$ is a bounded lattice, the operations $\&$ and $\oplus$ are associative and commutative, and admit identity elements $\top$ and $\mathbb{0}$ respectively;

i.e. $\quad \top \& G = G \quad$ and $\quad \mathbb{0} \oplus G = G$.

Moreover, for all $G, H, K \in Fact(P)$,

$$(G \& H) \oplus (G \& K) \subseteq G \& (H \oplus K)$$
$$G \oplus (H \& K) \subseteq (G \oplus H) \& (G \oplus K).$$

Lemma 2.0.4 yields the de Morgan duality:

$$G \& H = (G^{\perp} \oplus H^{\perp})^{\perp} \quad \text{and} \quad G \oplus H = (G^{\perp} \& H^{\perp})^{\perp}$$

for all $G, H \in Fact(P)$.

Note the verification conditions for & and $\oplus$:

(i) $1 \in G \& H$ iff $1 \in G$ and $1 \in H$;

(ii) if $1 \in G$ or $1 \in H$ then $1 \in G \oplus H$, but the converse does not, in general, hold.

Lemma 2.1.2:

Fact(P) is not necessarily a distributive lattice.

Proof.

There is a plentiful supply of finite phase spaces which provide counter-examples. Among the simplest is the monoid $P = \langle \mathbb{Z}/6\mathbb{Z}, +, 0 \rangle$ with $\perp_P = \{2, 5\}$.

$$\perp = \{0\}^{\perp} = \{n \in \mathbb{Z}/6\mathbb{Z} \mid n + 0 \in \{2,5\} \, [\text{mod } 6]\} = \{2,5\} = \{3\}^{\perp}.$$
$$\{1\}^{\perp} = \{n \in \mathbb{Z}/6\mathbb{Z} \mid n + 1 \in \{2,5\} \, [\text{mod } 6]\} = \{1,4\} = \{4\}^{\perp}.$$
$$\{2\}^{\perp} = \{n \in \mathbb{Z}/6\mathbb{Z} \mid n + 2 \in \{2,5\} \, [\text{mod } 6]\} = \{0,3\} = \{5\}^{\perp}.$$

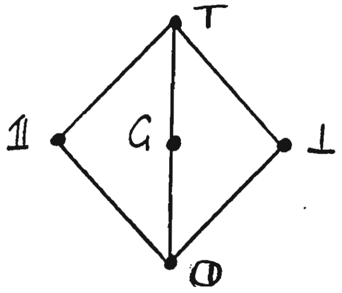
$\mathbb{1} = \{2\}^{\perp} \cap \{5\}^{\perp} = \{0, 3\}$. Let $G = \{1\}^{\perp} = \{4\}^{\perp}$.

** the pagination has gone askew; there are no pages 26, 27 and 28. **

We have examined all the duals of singletons, so $\mathrm{Fact}(P) = \{\mathbb{1}, \perp, G, \top, \mathbb{O}\}$ where $\top = \mathbb{Z}/6\mathbb{Z}$ and

$$\mathbb{O} = \top^{\perp} = \bigcap_{i<6} \{i\}^{\perp} = \emptyset.$$

The Hasse diagram for Fact(P) is as follows:



Hence $\quad G \& (\mathbb{1} \oplus \perp) = G \& \top = G$

While $\quad (G \& \mathbb{1}) \oplus (G \& \perp) = \mathbb{O} \oplus \mathbb{O} = \mathbb{O}$ $\blacksquare$

Lemma 2.1.3:

Fact(P) is not necessarily a modular lattice, i.e. it may fail to satisfy the modularity condition:

$$\text{if} \quad G \subseteq H \quad \text{then} \quad G \oplus (H \& K) = H \& (G \oplus K)$$

(Of course, non-modularity implies non-distributivity, but this time our example isn't quite so simple.)

Proof: Consider the monoid $P = \langle \mathbb{Z}/4\mathbb{Z}, +, 0 \rangle$ with $\perp_P = \{1, 2\}$

$$\begin{aligned}
\perp = \{0\}^{\perp} &= \{n \in \mathbb{Z}/4\mathbb{Z} \mid n+0 \in \{1,2\} \ [\text{mod } 4]\} = \{1,2\} \\
\{1\}^{\perp} &= \{n \in \mathbb{Z}/4\mathbb{Z} \mid n+1 \in \{1,2\} \ [\text{mod } 4]\} = \{0,1\} \\
\{2\}^{\perp} &= \{n \in \mathbb{Z}/4\mathbb{Z} \mid n+2 \in \{1,2\} \ [\text{mod } 4]\} = \{0,3\} \\
\{3\}^{\perp} &= \{n \in \mathbb{Z}/4\mathbb{Z} \mid n+3 \in \{1,2\} \ [\text{mod } 4]\} = \{2,3\}
\end{aligned}$$

Now $\mathbb{1} = \{1\}^{\perp} \cap \{2\}^{\perp} = \{0\}$, $\quad T = \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{0} = \emptyset$.

Set $G = \{0\}^{\perp} \cap \{1\}^{\perp} = \{1\}$,

$H = \{1\}^{\perp} = \{0,1\}$

$K = \{3\}^{\perp} = \{2,3\}$

and $L = \{2\}^{\perp} = \{0,3\}$

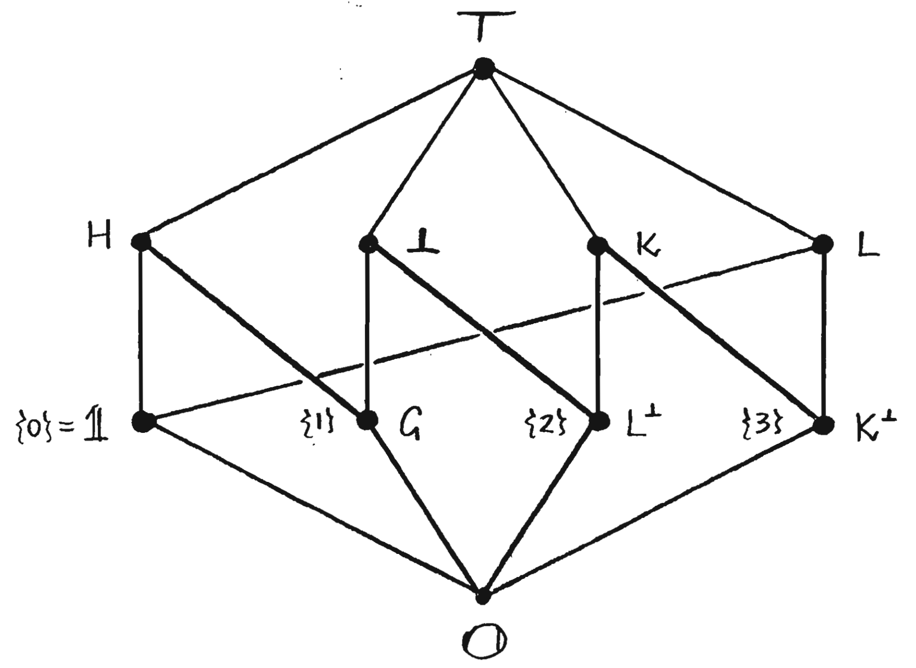
Then $H^{\perp} = G$,

$K^{\perp} = \{2\}^{\perp} \cap \{3\}^{\perp} = \{3\}$

and $L^{\perp} = \{0\}^{\perp} \cap \{3\}^{\perp} = \{2\}$.

No three of the $\{i\}^{\perp}$, $i<4$, have a non-empty intersection so $Fact(P) = \{T, H, \perp, K, L, \mathbb{1}, G, L^{\perp}, K^{\perp}, \mathbb{0}\}$.

The Hasse diagram should make things clearer.



Now $G \subseteq H$ but $G \oplus (H \& K) = G \oplus \mathbb{0} = G$

while $H \& (G \oplus K) = H \& T = H$. ∎

<u>Exercise 2·1·4:</u> Find a finite phase space such that $Fact(P)$ is non-modular and of smaller cardinality than the above.

Note 2.1.5:

Given that Fact(P) is a complete lattice, it is going to be fairly straightforeward to give semantic definitions of (first-order) quantifiers for linear logic — they'll just be infinite generalizations of the additives. If A is a formula in the language of predicate linear logic then its interpretation in P, say $s_P(A)$, will be a family of facts of P, and

$$s_P(\wedge x.A) = \wedge s_P(A) = \bigcap s_P(A)\ ;$$
$$s_P(\vee x.A) = \vee s_P(A) = \left(\bigcup s_P(A)\right)^{\perp\perp}.$$

The sequent calculus for predicate linear logic, call it **LL₁**, is obtained from **LL** by suitably modifying the underlying language and adjoining the familiar quantifier rules:

$$\frac{\vdash A, \Delta}{\vdash \wedge x.A, \Delta}\ (\wedge) \qquad\qquad \frac{\vdash A[t/x], \Delta}{\vdash \vee x.A, \Delta}\ (\vee)$$

provided x is not free in Δ

Soundness and completeness of **LL₁** with respect to phase space semantics will come from tacking on the extra cases to the proofs for **LL**. On this matter, we concur with Girard: the details are '... straightforeward and boring and left to the reader.' (Girard [1987], p.27)

2.2 The multiplicatives

Each of the multiplicative operations are definable in terms of the product operation (commonly used in work with monoids, semi-groups or groups):

if $G, H \subseteq P$ then $GH \stackrel{df}{=} \{pq \mid p \in G \text{ and } q \in H\}$.

Since we are assuming P is a commutative monoid, $GH = HG$. From the definition of $(-)^{\perp}$, we have that $G^{\perp}G \subseteq \perp$ for all $G \subseteq P$. Note, however, that even when G and H are both facts, GH is not necessarily a fact.

Definition 2.2.1:
Let $G, H \in Fact(P)$.
Define

$$G \otimes H \stackrel{df}{=} (GH)^{\perp\perp}, \qquad G \mathbin{⅋} H \stackrel{df}{=} (G^{\perp}H^{\perp})^{\perp}$$

and $$G \multimap H \stackrel{df}{=} (GH^{\perp})^{\perp}.$$

Lemma 2.2.2: (Girard [1987])
The following properties are immediate consequences of the definitions:
for all $G, H \in Fact(P)$,

$$G \otimes H = (G^{\perp} \mathbin{⅋} H^{\perp})^{\perp} \qquad G \otimes H = (G \multimap H^{\perp})^{\perp}$$

$$G \mathbin{⅋} H = (G^{\perp} \otimes H^{\perp})^{\perp} \qquad G \mathbin{⅋} H = G^{\perp} \multimap H$$

$$G \multimap H = G^{\perp} \mathbin{⅋} H \qquad G \multimap H = (G \otimes H^{\perp})^{\perp}$$

■

Lemma 2.2.3: (Girard [1987])

(i) The operations $\otimes$ and $⅋$ are commutative and associative on Fact(P), and admit identity elements $\mathbb{1}$ and $\perp$ respectively;

i.e. $\quad \mathbb{1} \otimes G = G \quad$ and $\quad \perp ⅋ G = G$.

(ii) the operation $\multimap$ has the following properties with respect to Fact(P):

(a) $\quad G \multimap H = H^{\perp} \multimap G^{\perp}$;

(b) $\quad (G \otimes H) \multimap K = G \multimap (H \multimap K)$ and
$\quad G \multimap (H ⅋ K) = (G \multimap H) ⅋ K$;

(c) $\quad \mathbb{1} \multimap G = G \quad$ and $\quad G \multimap \perp = G^{\perp}$.

Proof:

In virtue of the previous lemma, each part of (ii) is an immediate consequence of one of the parts of (i). The commutativity of $\otimes$ and $⅋$ is also immediate. We show that, for any $G \in$ Fact(P), $\mathbb{1} \otimes G = G$, as follows.

First, observe that for any $G, H \subseteq P$, if $1 \in H$ then $G \subseteq GH$. Hence $G \subseteq \mathbb{1}G \subseteq (\mathbb{1}G)^{\perp\perp} = \mathbb{1} \otimes G$.
Conversely, if $p \in \mathbb{1}$ and $q \in G$ then $pq \in G^{\perp\perp} = G$. Hence $\mathbb{1}G \subseteq G$. But then $(\mathbb{1}G)^{\perp\perp} \subseteq G$, and we are done.

As a consequence, $\perp ⅋ G = G$.

All we now need show is that $\otimes$ is associative. To do this we show that

$$(G \otimes H) \otimes K = ((GH)K)^{\perp\perp} = (G(HK))^{\perp\perp} = G \otimes (H \otimes K)$$

The middle identity comes from the associativity of the monoid operation, and the outer two are consequences of the following lemma.

Lemma 2.2.4: (Girard [1987])
Let $G, H \subseteq P$ be any subsets.
Then
$$G^{\perp\perp} H^{\perp\perp} \subseteq (GH)^{\perp\perp}.$$

Proof:
Let $p \in G^{\perp\perp}$, $q \in H^{\perp\perp}$ and $r \in (GH)^{\perp}$. We need to show that $pqr \in \perp$. First fix $g \in G$. Then since $r \in (GH)^{\perp}$ we have that for all $h \in H$, $rgh \in \perp$. Hence $rg \in H^{\perp} = H^{\perp\perp\perp}$. Since $q \in H^{\perp\perp}$, we have $rgq \in \perp$. Now $g \in G$ was arbitrary, so for all $g \in G$, $(qr)g \in \perp$. Hence $qr \in G^{\perp} = G^{\perp\perp\perp}$. Then since $p \in G^{\perp\perp}$, we get $pqr \in \perp$. ∎

Lemma 2.2.5: (Girard [1987])
The following distributivity properties hold for all $G, H, K \in Fact(P)$:

(i) $G \otimes (H \oplus K) = (G \otimes H) \oplus (G \otimes K)$, $\quad \mathbf{0} \otimes G = \mathbf{0}$,
$G \parr (H \& K) = (G \parr H) \& (G \parr K)$, $\quad \top \parr G = \top$,
$(G \oplus H) \multimap K = (G \multimap K) \& (H \multimap K)$, $\quad \mathbf{0} \multimap G = \top$,
$G \multimap (H \& K) = (G \multimap H) \& (G \multimap K)$, $\quad G \multimap \top = \top$;

(ii) $G \otimes (H \& K) \subseteq (G \otimes H) \& (G \otimes K)$,
$(G \parr H) \oplus (G \parr K) \subseteq G \parr (H \oplus K)$,
$(G \multimap K) \oplus (H \multimap K) \subseteq (G \& H) \multimap K$,
$(G \multimap H) \oplus (G \multimap K) \subseteq G \multimap (H \oplus K)$;

(iii) $G \otimes (H \parr K) \subseteq (G \otimes H) \parr K$.

Proof: We prove one from each of (i), (ii) and (iii); the rest then follow by Lemma 2.2.2.

(i) (a) $G \otimes (H \oplus K) \subseteq (G \otimes H) \oplus (G \otimes K)$,

i.e. $(G.(H \cup K)^{\perp\perp})^{\perp\perp} \subseteq ((GH)^{\perp\perp} \cup (GK)^{\perp\perp})^{\perp\perp}$.

Observe that $G.(H \cup K) \subseteq GH \cup GK$

$\subseteq (GH)^{\perp\perp} \cup (GK)^{\perp\perp}$.

By Lemma 2.2.4 $G.(H \cup K)^{\perp\perp} \subseteq (G.(H \cup K))^{\perp\perp}$, since $G = G^{\perp\perp}$.

Hence $G.(H \cup K)^{\perp\perp} \subseteq ((GH)^{\perp\perp} \cup (GK)^{\perp\perp})^{\perp\perp}$

By Lemma 2.0.3 (v), $(G.(H \cup K)^{\perp\perp})^{\perp\perp} \subseteq ((GH)^{\perp\perp} \cup (GK)^{\perp\perp})^{\perp\perp}$.

(b) $GH \subseteq G.(H \cup K) \subseteq G.(H \cup K)^{\perp\perp} \subseteq (G.(H \cup K)^{\perp\perp})^{\perp\perp}$.

By Lemma 2.0.3 (v), $(GH)^{\perp\perp} \subseteq (G.(H \cup K)^{\perp\perp})^{\perp\perp}$.

Likewise, $(GK)^{\perp\perp} \subseteq (G.(H \cup K)^{\perp\perp})^{\perp\perp}$.

Hence $(GH)^{\perp\perp} \cup (GK)^{\perp\perp} \subseteq (G.(H \cup K)^{\perp\perp})^{\perp\perp}$.

Again by Lemma 2.0.3 (v), we have

$$((GH)^{\perp\perp} \cup (GK)^{\perp\perp})^{\perp\perp} \subseteq (G.(H \cup K)^{\perp\perp})^{\perp\perp}.$$

(ii) $G \otimes (H \& K) \subseteq (G \otimes H) \& (G \otimes K)$

i.e. $(G.(H \cap K))^{\perp\perp} \subseteq (GH)^{\perp\perp} \cap (GK)^{\perp\perp}$

Observe that $G.(H \cap K) \subseteq GH \subseteq (GH)^{\perp\perp}$,

and $G.(H \cap K) \subseteq GK \subseteq (GK)^{\perp\perp}$.

Hence $G.(H \cap K) \subseteq (GH)^{\perp\perp} \cap (GK)^{\perp\perp}$.

By Lemma 2.0.3 (v), $(G.(H \cap K))^{\perp\perp} \subseteq (GH)^{\perp\perp} \cap (GK)^{\perp\perp}$.

Exercise 2.2.6: We've changed our mind: the proof of (iii) is left to the reader. (Write it out and you'll see why.)

∎

The following lemma gives an illuminating characterization of $G \multimap H$.

Lemma 2.2.7: (Girard [1987])
Let $G, H \in Fact(P)$.
Then

$$G \multimap H = \{ q \in P \mid \text{for all } p \in G \ (pq \in H) \}.$$

i.e. $G \multimap H$ consists of those q which send of all G into H.

Proof:
Recall that $\quad G \multimap H \overset{df}{=} (GH^{\perp})^{\perp}$

Let q be such that for all $p \in G$, $pq \in H$. Let $p \in G$ and $r \in H^{\perp}$, hence $pr \in GH^{\perp}$. Then $pq \in H = H^{\perp\perp}$, hence $(pq)r = q(pr) \in \perp$. Hence $q \in (GH^{\perp})^{\perp}$.

Conversely, suppose $q \in (GH^{\perp})^{\perp}$. Fix $p \in G$. Then for all $r \in H^{\perp}$, $q(pr) = (pq)r \in \perp$. Hence $pq \in H^{\perp\perp} = H$.

■

Corollary 2.2.8:
Let $G, H \in Fact(P)$.
Then $\quad 1 \in G \multimap H \quad$ iff $\quad G \subseteq H$. ■

One would expect the inclusion relation on $Fact(P)$ to represent implication, but it is nice to have one's expectations confirmed. This corollary is used repeatedly in the proof of the soundness theorem.

To give an overview of all the operations on Fact(P), we summarize the verification conditions:

Let $G, H \in$ Fact(P).

(i) $1 \in G^{\perp}$ iff $G \subseteq \perp$;

(ii) $1 \in G \& H$ iff $1 \in G$ and $1 \in H$;

(iii) $1 \in G \oplus H$ if $1 \in G$ or $1 \in H$;*

(iv) $1 \in G \otimes H$ if $1 \in G$ and $1 \in H$;*

(v) $1 \in G ⅋ H$ iff $G^{\perp} \subseteq H$;

(vi) $1 \in G \multimap H$ iff $G \subseteq H$.

* Of course, the converses of (iii) and (iv) need not hold. The best available necessary and sufficient conditions are in terms of the duals:

(iii)′ $1 \in G \oplus H$ iff $G^{\perp} \& H^{\perp} \subseteq \perp$

(iv)′ $1 \in G \otimes H$ iff $(GH)^{\perp} \subseteq \perp$

Clause (v) is an admission that the only sensible way to think of $G ⅋ H$ is as $G^{\perp} \multimap H$.

<u>Lemma 2.2.9:</u>

For all $G \in$ Fact(P),

(a) $1 \in G ⅋ G^{\perp}$;

(b) $1 \in \mathbb{1}$

(c) $1 \in \top ⅋ G$.

<u>Proof:</u>

(a) $1 \in G ⅋ G^{\perp}$ iff $G^{\perp} \subseteq G^{\perp}$. (b) has already been noted. For (c), recall that $\mathbb{0} \subseteq G$ for all $G \in$ Fact(P), hence $1 \in \top ⅋ G$. ∎

2.3 Soundness of LL

Definition 2.3.0:

Let Atom($\mathcal{L}$) denote the set of all atomic formulae in the language $\mathcal{L}$ of (propositional) linear logic.
A phase structure for $\mathcal{L}$ consists of a phase space $\langle P, \cdot, 1, \bot_P \rangle$ together with a function s_P: Atom($\mathcal{L}$) $\to$ Fact(P) satisfying

(i) $s_P(A^\perp) = s_P(A)^\perp$ for each propositional letter A of $\mathcal{L}$;
(ii) $s_P(\bot) = \bot_P$ and $s_P(\mathbb{1}) = \bot_P^\perp$;
(iii) $s_P(\top) = P$ and $s_P(\mathbb{0}) = P^\perp$.

Observation 2.3.1:

Let $\langle P, \cdot, 1, \bot, s_P \rangle$ be a phase structure for $\mathcal{L}$.
Then the function s_P has a unique extension $\hat{s}_P : \mathcal{L} \to$ Fact(P) satisfying

(i) for all $A \in$ Atom($\mathcal{L}$), $\hat{s}_P(A) = s_P(A)$; and
(ii) for all $A, B \in \mathcal{L}$,

$$\hat{s}_P(A \& B) = \hat{s}_P(A) \& \hat{s}_P(B),$$
$$\hat{s}_P(A \oplus B) = \hat{s}_P(A) \oplus \hat{s}_P(B),$$
$$\hat{s}_P(A \otimes B) = \hat{s}_P(A) \otimes \hat{s}_P(B),$$
$$\hat{s}_P(A \invamp B) = \hat{s}_P(A) \invamp \hat{s}_P(B).$$ ∎

(We trust the notational abuses are not too distressing.)

Definition 2.3.2:

A formula $A \in \mathcal{L}$ is valid in a phase structure $\langle P, \cdot, 1, \bot_P, s_P \rangle$ iff $\hat{s}_P(A)$ is verified in $\langle P, \cdot, 1, \bot_P \rangle$.
$A \in \mathcal{L}$ is a linear tautology iff A is valid in every phase structure $\langle P, \cdot, 1, \bot_P, s_P \rangle$.

A sequence Γ of formulae of $\mathcal{L}$, say $A_1, \ldots, A_n$, is valid in a phase structure $\langle P, \cdot, 1, \perp_P, s_P \rangle$ iff $\hat{s}_P(A_1 ⅋ \ldots ⅋ A_n)$ is verified in $\langle P, \cdot, 1, \perp_P \rangle$. (We write $\hat{s}_P(\Gamma)$ for short.)

<u>Theorem 2.3.3:</u> (Girard [1987]).
The sequent calculus **LL** is sound with respect to validity in phases structures.
ie. if $\vdash \Gamma$ is provable in **LL**
then Γ is valid in every phase structure for $\mathcal{L}$.

<u>Proof:</u> by induction on a proof π of $\vdash \Gamma$.
Let $\langle P, \cdot, 1, \perp_P, s_P \rangle$ be any phase structure for $\mathcal{L}$.
We use s as an abbreviation for $\hat{s}_P$.

(i) π is an instance of the identity axiom scheme, the $\mathbb{1}$ axiom or the $\top$ axiom scheme.
By Lemma 2.2.9, $1 \in s(\Gamma)$.

(ii) π is obtained from π_0 and π_1 by an application of (CUT):

$$\frac{\vdash A, \Delta_0 \qquad \vdash A^\perp, \Delta_1}{\vdash \Delta_0, \Delta_1} \text{(CUT)}$$

Let $s(A) = G$, $s(\Delta_0) = H$ and $s(\Delta_1) = K$.
Suppose $1 \in G ⅋ H$ and $1 \in G^\perp ⅋ K$. Then $G^\perp \subseteq H$, hence $H^\perp \subseteq G$, and $G \subseteq K$. Hence $H^\perp \subseteq K$, so $1 \in H ⅋ K$.

(iii) π is obtained from π_0 by an application of (EXCH):

$$\frac{\vdash \Delta}{\vdash \sigma(\Delta)} \text{(EXCH)}$$ for some permutation σ of Δ.

By the commutativity of ⅋, $s(\Delta) = s(\sigma(\Delta))$.

(iv) Π is obtained from Π_0 and Π_1 by an application of the rule ($\&$):

$$\frac{\vdash A, \Delta \qquad \vdash B, \Delta}{\vdash A \& B, \Delta}\ (\&)$$

Let $s(A) = G$, $s(B) = H$ and $s(\Delta) = K$.
Suppose $1 \in G \parr K$ and $1 \in H \parr K$.
Then $1 \in (G \parr K) \& (H \parr K) = (G \& H) \parr K$, by the distributivity of $\parr$ over $\&$.

(v) Π is obtained from Π_0 by an application of the rule (FST$\oplus$):

$$\frac{\vdash A, \Delta}{\vdash A \oplus B, \Delta}\ (\mathrm{FST}\oplus)$$

Let $s(A) = G$, $s(B) = H$ and $s(\Delta) = K$.
Suppose $1 \in G \parr K$. Then $G^\perp \subseteq K$. Since $G^\perp \cap H^\perp \subseteq G^\perp$,
we have $(G \oplus H)^\perp = G^\perp \cap H^\perp \subseteq K$.
Hence $1 \in (G \oplus H) \parr K$.

(vi) Π is obtained from Π_1 by an application of the rule (SND$\oplus$):
Symmetric with case (v).

(vii) Π is obtained from Π_0 and Π_1 by an application of the rule ($\otimes$):

$$\frac{\vdash A, \Delta_0 \qquad \vdash B, \Delta_1}{\vdash A \otimes B, \Delta_0, \Delta_1}\ (\otimes)$$

Let $s(A) = G$, $s(B) = H$, $s(\Delta_0) = K_0$ and $s(\Delta_1) = K_1$.
Suppose $1 \in G \parr K_0$ and $1 \in H \parr K_1$.
Hence $G^\perp \subseteq K_0$ and $H^\perp \subseteq K_1$, so $K_0^\perp \subseteq G$ and $K_1^\perp \subseteq H$.
Hence $K_0^\perp . K_1^\perp \subseteq G.H \subseteq (G.H)^{\perp\perp} = G \otimes H$.
By Lemma 2.0.3 (v), $(K_0^\perp . K_1^\perp)^{\perp\perp} \subseteq G \otimes H$,
i.e. $K_0^\perp \otimes K_1^\perp \subseteq G \otimes H$.
Hence $(G \otimes H)^\perp \subseteq K_0 \parr K_1$,
so $1 \in (G \otimes H) \parr K_0 \parr K_1$.

(viii) Π is obtained from Π_0 by an application of the rule ($⅋$):

$$\frac{\vdash A, B, \Delta}{\vdash A ⅋ B, \Delta}\ (⅋)$$

Immediate.

(ix) Π is obtained from Π_0 by an application of the rule ($\perp$):

$$\frac{\vdash \Delta}{\vdash \perp, \Delta}\ (\perp)$$

Since $\perp_P$ is the identity element for the operation $⅋$, $s(\Delta) = \perp_P ⅋ s(\Delta)$. ■

2.4 Completeness of **LL**

For the purposes of the proof, we will work with a variant sequent calculus **LL*** obtained from **LL** by omitting the exchange rule and adapting the axiom schemes and inference rules so as to be appropriate for multi-sets of formulae of $\mathcal{L}$, i.e. we distinguish occurrences of formulae but ignore the order. Clearly, if Δ is any multi-set of formulae of $\mathcal{L}$, and Δ' is any sequence of formulae of $\mathcal{L}$ whose components are exactly the elements of Δ, then $\vdash \Delta$ is provable in **LL*** iff $\vdash \Delta'$ is provable in **LL**.

Multi-sets of formulae of $\mathcal{L}$ form a commutative monoid: the operation is concatenation (denoted '$*$') and the empty multiset $\emptyset$ is the identity element. We denote this monoid by $\langle M, *, \emptyset \rangle$. We will build a canonical phase structure $\langle M, *, \emptyset, \perp_M, S_M \rangle$

which resembles the usual Lindenbaum algebra construction in the sense that formulae provably equivalent in LL will correspond to identical elements of Fact(M). This twist in this construction is the choice of $\perp_M$.

Theorem 2.4.0: (Girard [1987])
The sequent calculus **LL** is complete with respect to validity in phase structures.
i.e. for any formula A of $\mathcal{L}$,
if A is a linear tautology
then $\vdash A$ is provable in **LL**.

Proof.
Consider the monoid $\langle M, *, 1\rangle$; we use Δ, Γ, Σ to denote elements of M. For the duration of the proof, we use '$\vdash_* \Delta$' as an abbreviation for '$\vdash \Delta$ is provable in **LL***'.

Now we define $\perp_M = \{\Delta \in M \mid \vdash_* \Delta\}$,
i.e. the interpretation of the multiplicative falsum is the set of all provable multi-sets!

So $\langle M, *, \emptyset, \perp_M\rangle$ is a phase space; now we need a suitable interpretation function s_M.

For each formula A of $\mathcal{L}$, define
$Pr(A) = \{\Gamma \in M \mid \vdash_* A, \Gamma\}$

(Technically, we should write $\vdash_* [\![A]\!] * \Gamma$, where the square brackets $[\![\cdot]\!]$ are for multi-sets what curly brackets $\{\cdot\}$ are for sets; we will only do so when it is necessary for clarity.)

Lemma 2.4.1:

For any formulae $A \in \mathcal{L}$ and $B \in \mathcal{L}$,

$$\vdash_* A \multimap B \quad \text{iff} \quad Pr(A) \subseteq Pr(B).$$

Hence $\quad A \equiv_{LL} B \quad$ iff $\quad Pr(A) = Pr(B)$.

Proof:

Suppose $\vdash_* A \multimap B$. Then we must have $\vdash_* A^\perp, B$; i.e. in a cut-free proof, the last rule used must have been $(\otimes)$. Let $\Gamma \in Pr(A)$. Then $\vdash_* A, \Gamma$. But $\vdash_* A, \Gamma$ and $\vdash_* A^\perp, B$ together imply $\vdash_* B, \Gamma$ by (CUT). Hence $\Gamma \in Pr(B)$.

Conversely, suppose $Pr(A) \subseteq Pr(B)$. Now $A^\perp \in Pr(A)$ since $\vdash_* A, A^\perp$. Hence $A^\perp \in Pr(B)$, so $\vdash_* B, A^\perp$. Hence $\vdash_* A \multimap B$ by the rule $(\otimes)$. $\square$

We don't actually need this lemma at the moment — we do need it later in proving the completeness of the modal sequent calculus **LL!** (Section 3.2) — but it is of help in providing motivation for the construction.

Lemma 2.4.2:

For each formula $A \in \mathcal{L}$, $Pr(A) \in Fact(\mathbf{M})$.

Proof:

Consider the multi-set $[\![A]\!] \in M$. The singleton set $\{[\![A]\!]\}$ has as its dual

$$
\begin{aligned}
\{[\![A]\!]\}^{\perp} &= \{\Gamma \in M \mid [\![A]\!] * \Gamma \in \perp_M\} \\
&= \{\Gamma \in M \mid \vdash_* [\![A]\!] * \Gamma\} \\
&= Pr(A).
\end{aligned}
$$

Hence $Pr(A) \in Fact(M)$. □

Lemma 2.4.3: $Pr(\perp) = \perp_M$ and $Pr(\top) = M$.

Proof:
Let $\Delta \in Pr(\perp)$. Then $\vdash_* \perp, \Delta$. We have $\vdash_* \mathbb{1}$, so by (CUT), $\vdash_* \Delta$. Hence $\Delta \in \perp_M$.
Conversely, let $\Delta \in \perp_M$. Then $\vdash_* \Delta$, hence $\vdash_* \perp, \Delta$ by the rule $(\perp)$. Hence $\Delta \in Pr(\perp)$.

$Pr(\top) = \{\Delta \in M \mid \vdash_* \top, \Delta\} = M$, in virtue of the axiom scheme for $\top$. □

Lemma 2.4.4:
For each formula $A \in \mathcal{L}$, $Pr(A^{\perp}) = Pr(A)^{\perp}$.

Proof:
$Pr(A)^{\perp} = \{\Delta \in M \mid \text{for all } \Gamma \text{ (if } \vdash_* A, \Gamma \text{ then } \vdash_* \Delta, \Gamma)\}$

Let $\Delta \in Pr(A^{\perp})$. Then $\vdash_* A^{\perp}, \Delta$. Suppose $\vdash_* A, \Gamma$ for $\Gamma \in M$. Then by (CUT), $\vdash_* \Delta, \Gamma$. Hence $\Delta \in Pr(A)^{\perp}$.

Conversely, suppose $\Delta \in Pr(A)^{\perp}$. Now $\vdash_* A, A^{\perp}$ hence $\vdash_* \Delta, A^{\perp}$. So $\Delta \in Pr(A^{\perp})$. □

Now set $s_M = Pr \upharpoonright Atom(\mathcal{L})$. The previous two lemmas together imply that the function $s_M : Atom(\mathcal{L}) \to Fact(M)$ satisfies the conditions necessary for $\langle M, *, \emptyset, \bot_M, s_M \rangle$ to be a phase structure.

We are not quite finished: we still have to check that $\hat{s}_M = Pr$. Otherwise put, we have to show that $Pr : \mathcal{L} \to Fact(M)$ is an homomorphism, considering $\mathcal{L}$ and $Fact(M)$ as algebras of the same type.

Lemma 2.4.5:

For all $A \in \mathcal{L}$, $B \in \mathcal{L}$

(i) $Pr(A \& B) = Pr(A) \& Pr(B)$;

(ii) $Pr(A \oplus B) = Pr(A) \oplus Pr(B)$;

(iii) $Pr(A \otimes B) = Pr(A) \otimes Pr(B)$;

(iv) $Pr(A \parr B) = Pr(A) \parr Pr(B)$.

Proof:

We give proofs of (i) and (iii) ; (ii) and (iv) follow by Lemma 2.4.4 together with the definitions of $(A \oplus B)^\perp$ and $(A \parr B)^\perp$ for formulae A and B of $\mathcal{L}$.

(i) Observe that $\vdash_* A \& B, \Delta$ iff $\vdash_* A, \Delta$ and $\vdash_* B, \Delta$. Hence $\Delta \in Pr(A \& B)$ iff $\Delta \in Pr(A) \cap Pr(B)$.

(iii) Let $\Gamma \in Pr(A \otimes B)$ and fix some $\Sigma \in (Pr(A).Pr(B))^\perp$. Then for all Δ_0 and Δ_1, if $\vdash_* A, \Delta_0$ and $\vdash_* B, \Delta_1$ then $\vdash_* \Delta_0, \Delta_1, \Sigma$. Consider the case of $\Delta_0 = [\![A^\perp]\!]$ and $\Delta_1 = [\![B^\perp]\!]$. Since $\vdash_* A, A^\perp$ and $\vdash_* B, B^\perp$,

We get $\vdash_* A^\perp, B^\perp, \Sigma$. Hence $\vdash_* (A\otimes B)^\perp, \Sigma$ by the $(\otimes)$ rule. Now $\Gamma \in Pr(A\otimes B)$ so $\vdash_* A\otimes B, \Gamma$. By (CUT), we get $\vdash_* \Gamma, \Sigma$.
Hence $\Gamma \in (Pr(A).\,Pr(B))^{\perp\perp} = Pr(A)\otimes Pr(B)$.

Conversely, suppose $\Delta_0 \in Pr(A)$ and $\Delta_1 \in Pr(B)$. Then $\vdash_* A, \Delta_0$ and $\vdash_* B, \Delta_1$. By the rule $(\otimes)$, we have $\vdash_* A\otimes B, \Delta_0, \Delta_1$. Hence $\Delta_0 * \Delta_1 \in Pr(A\otimes B)$.
Hence $\quad Pr(A).\,Pr(B) \subseteq Pr(A\otimes B)$,
and so $\quad Pr(A)\otimes Pr(B) \subseteq Pr(A\otimes B)$. $\square$

And now for the punchline...

Let A be any linear tautology; i.e. A is valid in every phase structure. In particular, A is valid in $\langle M, *, \emptyset, \perp_M, Pr\rangle$. So $\emptyset \in Pr(A)$, hence $\vdash_* A$. Hence $\vdash A$ is provable in **LL**. $\blacksquare$

3. The exponential (modal) operators.

By enriching propositional linear logic with modal, or 'exponential', connectives, we recover expressive power; in particular, sufficient expressive power to be able to interpret intuitionistic logic in the resulting system (section 3.3). Girard's slogan is that 'usual [intuitionistic] logic is obtained from [propositional] linear logic by a passage to the limit'; the mathematical content of this slogan is a result called the Approximation theorem. (Section 4.1).

Girard calls the modalities 'of course' (denoted '!') and 'why not' (denoted '?'); their behaviour is similar to that of necessity and possibility, respectively, in the classical modal logic S4, modulo the wierdness of the underlying propositional logic. (Girard's rationale for the non-standard notation is that he doesn't want linear logic dismissed as 'yet another modal system': Girard [1987], p.27.)

One of the crucial aspects of this extension of linear logic is that the structural rules of contraction and thinning re-appear, but are allowed only in modal contexts.

Why the term 'exponential'? (Pourquoi pas?) One answer is that what else will fill the blank in the sequence 'additive, multiplicative, ____' (Bien sur!) An explanation is that the modal contraction rule results in exponential growth in the size of proof nets under normalization (elimination of cuts): see section 6·4. Also, the exponential ! is connected with the 'internal hom' or 'exponential' functor $\_\Rightarrow\_ : \mathbf{C}^{op} \times \mathbf{C} \longrightarrow \mathbf{C}$ in a Cartesian closed category $\mathbf{C}$; i.e. intuitionistic implication: see sections 5·1 and 5·2.

3·0 The sequent calculus **LL!**

Definition 3·0·0:

The language $\mathcal{L}_!$ of modal linear logic is defined in the same way as the language $\mathcal{L}$ (Definition 1·1·0), with the additional clause:

- if A is a formula of $\mathcal{L}_!$ then so are $!A$ and $?A$.

The expression $A^\perp$, where A is a formula of $\mathcal{L}_!$, is defined in the same way as it is for formulae of $\mathcal{L}$ (Definition 1·1·1), with the additional clause:

if A is a formula of $\mathcal{L}_!$,

$$(!A)^\perp \overset{df}{=} ?(A^\perp) \quad \text{and} \quad (?A)^\perp \overset{df}{=} !(A^\perp).$$

Not unexpectedly, de Morgan duality strikes again. Girard does not give names to his sequent calculi: we have chosen the names **LL** and **LL!** for their obviousness. (the name **LLM** is used in Danos and Regnier [1989] — for the same system we call **LLM**.)

Definition 3·0·1:

The sequent calculus **LL!** consists of the same axiom schemes and inference rules as **LL**, deemed now to apply to $\mathcal{L}_!$-sequents, together with the following inference rules:

$$\frac{\vdash \Delta}{\vdash ?A, \Delta}\,(Th?) \qquad \frac{\vdash ?A, ?A, \Delta}{\vdash ?A, \Delta}\,(C?)$$

$$\frac{\vdash A, \Delta}{\vdash ?A, \Delta}\,(D?) \qquad \frac{\vdash A, ?\Delta}{\vdash !A, ?\Delta}\,(!)$$

If Δ is the sequence $B_1, \ldots, B_n$ then $?\Delta$ is an abbreviation for $?B_1, \ldots, ?B_n$.

Girard uses the name (W?) instead of our (Th?), i.e. 'weakening' rather than 'thinning'. We have changed names because in the relevance logic tradition, (W) is the name of an axiom scheme (in a Hilbert-style system) for contraction — the nomenclature derives from combinatory logic; in Smullyan-ian terms, 'W' is the 'warbler'. The name (D?) is short for 'dereliction': 'who cares' about A??

Again, we are safe to restrict the identity axiom scheme to propositional letters and their duals:

$$\cfrac{\cfrac{\vdash A, A^\perp}{\vdash A, ?(A^\perp)}\,(D?)}{\vdash !A, ?(A^\perp)}\,(!) \qquad \cfrac{\cfrac{\vdash A, A^\perp}{\vdash ?A, A^\perp}\,(D?)}{\vdash ?A, !(A^\perp)}\,(!)$$

(We omit exchanges.)

The modal connectives provide a rather intriguing linkage between the additives and the multiplicatives.

<u>Lemma 3.0.2:</u> (Girard [1987])
The following are provable equiquivalences in **LL!** :

(i) $!(A \& B) \equiv_{LL!} (!A) \otimes (!B)$;

(ii) $?(A \oplus B) \equiv_{LL!} (?A) \parr (?B)$;

(iii) $!\top \equiv_{LL!} \mathbb{1}$;

(iv) $?\mathbb{0} \equiv_{LL!} \bot$.

<u>Proof:</u> We exhibit proofs for (ii) and (iv); (i) and (iii) then follow by duality. Exchanges are, as usual, omitted.

(ii)

$$
\begin{prooftree}
\AxiomC{$\vdash A^\perp, A$}
\RightLabel{(FST $\oplus$)}
\UnaryInfC{$\vdash A^\perp, A \oplus B$}
\RightLabel{(D?)}
\UnaryInfC{$\vdash A^\perp, ?(A \oplus B)$}
\RightLabel{(!)}
\UnaryInfC{$\vdash !(A^\perp), ?(A \oplus B)$}
\AxiomC{$\vdash B^\perp, B$}
\RightLabel{(SND $\oplus$)}
\UnaryInfC{$\vdash B^\perp, A \oplus B$}
\RightLabel{(D?)}
\UnaryInfC{$\vdash B^\perp, ?(A \oplus B)$}
\RightLabel{(!)}
\UnaryInfC{$\vdash !(B^\perp), ?(A \oplus B)$}
\RightLabel{($\otimes$)}
\BinaryInfC{$\vdash !(A^\perp) \otimes !(B^\perp), ?(A \oplus B), ?(A \oplus B)$}
\RightLabel{(C?)}
\UnaryInfC{$\vdash !(A^\perp) \otimes !(B^\perp), ?(A \oplus B)$}
\RightLabel{($\parr$)}
\UnaryInfC{$\vdash ((?A) \parr (?B)) \multimap ?(A \oplus B)$}
\end{prooftree}
$$

$$
\begin{prooftree}
\AxiomC{$\vdash A^\perp, A$}
\RightLabel{(D?)}
\UnaryInfC{$\vdash A^\perp, ?A$}
\RightLabel{(Th?)}
\UnaryInfC{$\vdash A^\perp, ?A, ?B$}
\AxiomC{$\vdash B^\perp, B$}
\RightLabel{(D?)}
\UnaryInfC{$\vdash B^\perp, ?B$}
\RightLabel{(Th?)}
\UnaryInfC{$\vdash B^\perp, ?A, ?B$}
\RightLabel{(\&)}
\BinaryInfC{$\vdash A^\perp \& B^\perp, ?A, ?B$}
\RightLabel{(!)}
\UnaryInfC{$\vdash !(A^\perp \& B^\perp), ?A, ?B$}
\RightLabel{($\parr$)}
\UnaryInfC{$\vdash !(A^\perp \& B^\perp), (?A) \parr (?B)$}
\RightLabel{($\parr$)}
\UnaryInfC{$\vdash ?(A \oplus B) \multimap ((?A) \parr (?B))$}
\end{prooftree}
$$

(iv)

$$\dfrac{\dfrac{\vdash \mathbb{1}}{\vdash \mathbb{1}, ?\mathbb{0}}\,(\mathrm{Th}?)}{\vdash \perp \multimap ?\mathbb{0}}\,(\wp) \qquad\qquad \dfrac{\dfrac{\dfrac{\vdash \top}{\vdash !\top}\,(!)}{\vdash !\top, \perp}\,(\perp)}{\vdash ?\mathbb{0} \multimap \perp}\,(\wp)$$

■

3.1 Topolinear spaces

A semantics for modal linear logic is obtained from the phase space semantics by adding a bit more apparatus. The apparatus in question resembles a topology on Fact(P) (but is not quite one). We will have closed facts ($?G$) and open facts ($!G$). The closedness in this sense is quite different from closure in the sense of the closure operator $(-)^{\perp\perp}$; all elements of Fact(P) are closed in the latter sense. (Maybe this is why Girard makes no mention of $(-)^{\perp\perp}$ as a closure operator. We prefer to call a closure operator a closure operator.)

Definition 3.1.0:
A topolinear space is a quintuple $\langle P, \cdot, 1, \perp_P, \mathbb{F}\rangle$ where $\langle P, \cdot, 1, \perp_P\rangle$ is a phase space and $\mathbb{F} \subseteq \mathrm{Fact}(P)$ is a family of facts of P satisfying the following conditions:

(i) for any $X \subseteq \mathbb{F}$, $\bigcap X \in \mathbb{F}$; in particular, $\top \in \mathbb{F}$, $(\top = P)$;

(ii) if $F_1, \ldots, F_n \in \mathbb{F}$ then $F_1 \wp \ldots \wp F_n \in \mathbb{F}$;

(iii) $\bigcap \mathbb{F} = \perp_P$;

(iv) if $F \in \mathbb{F}$ then $F \wp F = F$. ($\wp$ is idempotent on $\mathbb{F}$)

$G \in Fact(P)$ is a <u>closed fact</u> iff $G \in \mathbb{F}$.
$G \in Fact(P)$ is an <u>open fact</u> iff $G^{\perp} \in \mathbb{F}$.

As before, $G \in Fact(P)$ is <u>verified</u> in $\langle P, \cdot, 1, \perp_P, \mathbb{F} \rangle$ iff $1 \in G$.

Let $G \in Fact(P)$.

The <u>affirmation</u> of G, $!G$ (of course G) is defined as follows:

$$!G \overset{df}{=} (\cup\{H \mid H \subseteq G \text{ and } H^{\perp} \in \mathbb{F}\})^{\perp\perp}.$$

The <u>consideration</u> of G, $?G$ (why not G) is defined as follows:

$$?G \overset{df}{=} \cap\{F \mid G \subseteq F \text{ and } F \in \mathbb{F}\}.$$

<u>Lemma 3.1.1</u>:
Let $G \in Fact(P)$.

(i) $(!G)^{\perp} = ?(G^{\perp})$ and $(?G)^{\perp} = !(G^{\perp})$

(ii) $!G$ is the largest (w.r.t. $\subseteq$) open fact included in G, and $?G$ is the smallest (w.r.t. $\subseteq$) closed fact containing G.

<u>Proof</u>:
(i) $$\begin{aligned}(!G)^{\perp} &= (\cup\{H \mid H \subseteq G \text{ and } H^{\perp} \in \mathbb{F}\})^{\perp} \\ &= \cap\{H^{\perp} \mid H \subseteq G \text{ and } H^{\perp} \in \mathbb{F}\} \quad \text{by Lemma 2.0.4,} \\ &= \cap\{H^{\perp} \mid G^{\perp} \subseteq H^{\perp} \text{ and } H^{\perp} \in \mathbb{F}\} \\ &= ?(G^{\perp}).\end{aligned}$$

$(?G)^{\perp} = !(G^{\perp})$ similarly.

(ii) follows from (i) and the definitions. ∎

So for all $G \in \mathrm{Fact}(P)$, $1 \in\, !G \multimap G$ and $1 \in G \multimap ?G$.
Also,

G is closed iff $G = ?F$ for some $F \in \mathbb{F}$; and
G is open iff $G = !(F^{\perp})$ for some $F \in \mathbb{F}$.

Lemma 3.1.2:
For all $G \in \mathrm{Fact}(P)$, $!G = !!G$ and $??G = ?G$.

Proof: We have $!!G \subseteq\, !G$.
Now $!!G = (\bigcup \{ H \mid H \subseteq\, !G \text{ and } H^{\perp} \in \mathbb{F} \})^{\perp\perp}$.
Since $(!G)^{\perp} \in \mathbb{F}$, we must have $!G \subseteq\, !!G$.
$??G = ?G$ follows by duality. ∎

Lemma 3.1.3:

$$!\top = \mathbb{1} \quad \text{and} \quad ?\mathbb{0} = \perp_P$$

Proof:
$$\begin{aligned} !\top &= (\bigcup \{ H \mid H \subseteq \top \text{ and } H^{\perp} \in \mathbb{F} \})^{\perp\perp} \\ &= (\bigcup \{ H \mid H^{\perp} \in \mathbb{F} \})^{\perp\perp} \\ &= (\bigcap \{ H^{\perp} \mid H^{\perp} \in \mathbb{F} \})^{\perp}, \text{ by lemma 2.0.4.} \\ &= (\bigcap \mathbb{F})^{\perp} \\ &= (\perp_P)^{\perp}, \quad \text{by condition (iii) on } \mathbb{F}. \\ &= \mathbb{1}. \end{aligned}$$
∎

Corollary 3.1.4: If $1 \in\, !G$ then $!G = \mathbb{1}$.
Hence $\mathbb{1}$ is the sum (supremum) of all affirmations, (which sounds better than '$\perp_P$ is the intersection of all considerations'). ∎

The corresponding syntactic result is readily verified: if $\vdash !A$ is provable in **LL!** then $!A \equiv_{LL!} \mathbb{1}$.

If we set $\mathbb{G} = \{ G \in \mathrm{Fact}(P) \mid G^{\perp} \in \mathbb{F} \}$ then we get a list of properties of open facts just by dualizing the conditions on $\mathbb{F}$:

(i) for any $Y \subseteq \mathbb{G}$, $(\bigcup Y)^{\perp\perp} \in \mathbb{G}$;

(ii) if $G_1, \ldots, G_n \in \mathbb{G}$, then $G_1 \otimes \ldots \otimes G_n \in \mathbb{G}$;

(iii) $(\bigcup \mathbb{G})^{\perp\perp} = \mathbb{1}$;

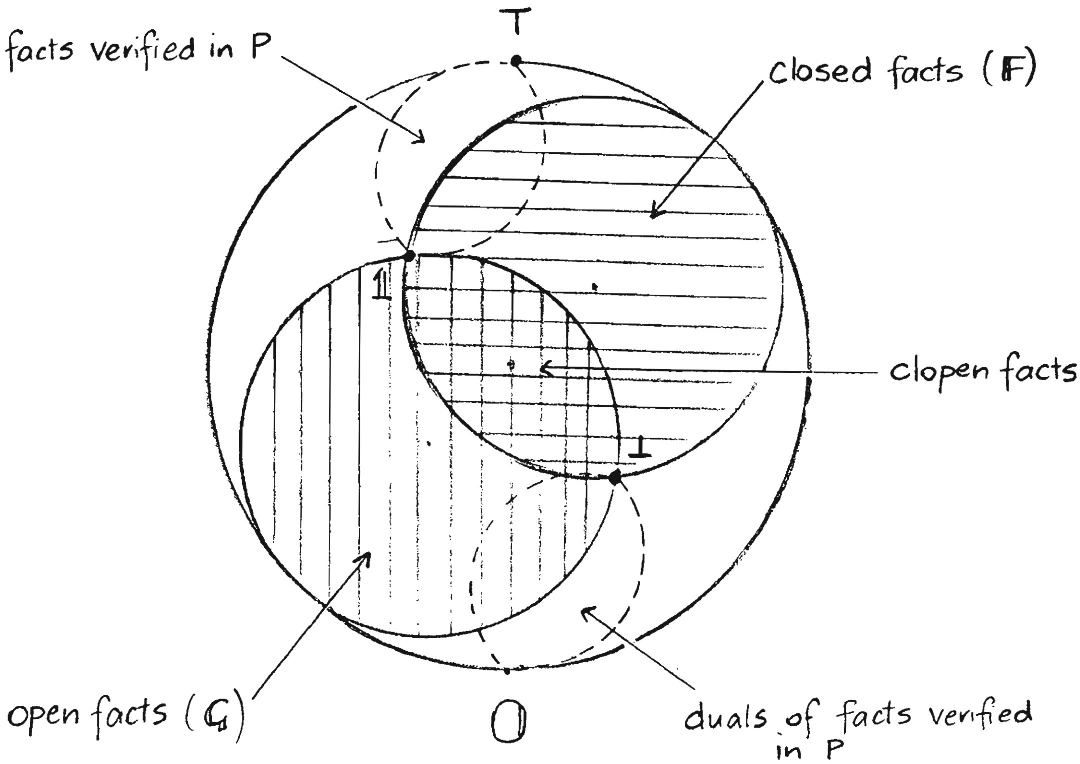
(iv) if $G \in \mathbb{G}$ then $G \otimes G = G$.

In summary, we have the following verification conditions: for any $G \in \mathrm{Fact}(P)$,

$1 \in\, !G$ iff $!G = \mathbb{1}$;

$1 \in\, ?G$ iff for all $F \supseteq G$ with $F \in \mathbb{F}$, $1 \in F$.

The general picture of a topolinear Fact(P) is as follows (cf. the picture following Examples 2.0.7).



3·2 Soundness and Completeness of **LL!**

Definition 3·2·0:
A topolinear structure for $\mathcal{L}_!$ is a sextuple $\langle P, \cdot, 1, \perp_P, \mathbb{F}, s_P \rangle$ where $\langle P, \cdot, 1, \perp_P, \mathbb{F} \rangle$ is a topolinear space and $s_P : \mathrm{Atom}(\mathcal{L}_!) \longrightarrow \mathrm{Fact}(P)$ is a function satisfying the same three conditions as in Definition 2·3·0.
(Note that $\mathrm{Atom}(\mathcal{L}_!) = \mathrm{Atom}(\mathcal{L})$.)

The function s_P has a unique extension $\hat{s}_P : \mathcal{L}_! \longrightarrow \mathrm{Fact}(P)$ which, in addition to respecting $\&$, $\oplus$, $\otimes$ and $⅋$ (as in Observation 2·3·1), satisfies, for all formulae $A, B \in \mathcal{L}_!$,

$$\hat{s}_P(!A) = !\,\hat{s}_P(A) \quad \text{and} \quad \hat{s}_P(?A) = ?\,\hat{s}_P(A).$$

A formula A of $\mathcal{L}_!$ is valid in a topolinear structure $\langle P, \cdot, 1, \perp_P, \mathbb{F}, s_P \rangle$ iff $1 \in \hat{s}_P(A)$.
A sequence Γ of formulae of $\mathcal{L}_!$, say $A_1, \dots, A_n$, is valid in a topolinear structure $\langle P, \cdot, 1, \perp_P, \mathbb{F}, s_P \rangle$ iff $1 \in \hat{s}_P(A_1 ⅋ \dots ⅋ A_n)$; $\hat{s}_P(\Gamma)$ for short.

Theorem 3·2·1: (Girard [1987])
The sequent calculus **LL!** is sound with respect to validity in topolinear structures.

Proof: by induction on a proof π in **LL!** of $\vdash \Gamma$.
Let $\langle P, \cdot, 1, \perp_P, s_P \rangle$ be any topolinear structure for $\mathcal{L}_!$.
Again, s is an abbreviation for $\hat{s}_P$.

The first nine cases of the induction are as in the proof of theorem 2·3·3.

(x) π is obtained from π_0 by an application of the rule (Th?):

$$\frac{\vdash \Delta}{\vdash ?A, \Delta}(Th?)$$

Let $s(A)=F$ and $s(\Delta)=G$. Assume $1 \in G$. Then $G^\perp \subseteq \perp$. But since $?F \in \mathbb{F}$, we have $\perp \subseteq ?F$. Hence $G^\perp \subseteq ?F$, so $1 \in G \mathbin{⅋} ?F = ?F \mathbin{⅋} G$.

(xi) π is obtained from π_0 by an application of the rule (C?):

$$\frac{\vdash ?A, ?A, \Delta}{\vdash ?A, \Delta}(C?)$$

Let $s(A)=F$ and $s(\Delta)=G$. Assume $1 \in ?F \mathbin{⅋} ?F \mathbin{⅋} G$. Since $?F \in \mathbb{F}$, we have $?F \mathbin{⅋} ?F = ?F$ (idempotence of $⅋$ on $\mathbb{F}$). Hence $1 \in ?F \mathbin{⅋} G$.

(xii) π is obtained from π_0 by an application of the rule (D?):

$$\frac{\vdash A, \Delta}{\vdash ?A, \Delta}(D?)$$

Let $s(A)=F$ and $s(\Delta)=G$. Assume $1 \in F \mathbin{⅋} G$. Hence $F^\perp \subseteq G$. But $!(F^\perp) \subseteq F^\perp$, hence $!(F^\perp) \subseteq G$. So $1 \in ?F \mathbin{⅋} G$.

(xiii) π is obtained from π_0 by an application of the rule (!):

$$\frac{\vdash A, ?B_1, \ldots, ?B_n}{\vdash !A, ?B_1, \ldots, ?B_n}(!)$$

Let $s(A)=G$ and $s(B_i)=F_i$, $i=1,\ldots,n$.
Assume $1 \in G \mathbin{⅋} ?F_1 \mathbin{⅋} \ldots \mathbin{⅋} ?F_n$. Hence $G^\perp \subseteq (?F_1 \mathbin{⅋} \ldots \mathbin{⅋} ?F_n)$.
Now $?F_1 \mathbin{⅋} \ldots \mathbin{⅋} ?F_n$ is closed since each $?F_i$ is closed, and $?(G^\perp)$ is the smallest closed fact containing $G^\perp$,
So $?(G^\perp) \subseteq (?F_1 \mathbin{⅋} \ldots \mathbin{⅋} ?F_n)$.
Hence $1 \in !G \mathbin{⅋} (?F_1 \mathbin{⅋} \ldots \mathbin{⅋} ?F_n)$. ∎

Theorem 3·2·2: (Girard [1987])
The sequent calculus LL! is complete with respect to validity in topolinear structures.

Proof:
We adapt the proof of completeness of **LL**. Recall the phase structure $\langle M, *, \emptyset, \perp_M \rangle$, where

$$\perp_M = \{ \Delta \in M \mid \vdash_* \Delta \}.$$

In this context, '$\vdash_* \Delta$' is an abbreviation for '$\vdash \Delta$ is provable in **LL!***', where **LL!*** is the multi-set version of **LL!**. As before, we define the function $Pr : \mathcal{L}_! \longrightarrow Fact(M)$ by

$$Pr(A) = \{ \Gamma \in M \mid \vdash_* A, \Gamma \}.$$

Now set $\mathbb{E} = \{ Pr(?A) \mid A \in \mathcal{L}_! \}$
and $\mathbb{F} = \{ \cap X \mid X \subseteq \mathbb{E} \}$.

To complete the proof, we need to show that
(I) $\mathbb{F}$ satisfies conditions (i)–(iv) of Definition 3·1·0, and hence $\langle M, *, \emptyset, \perp_M, \mathbb{F} \rangle$ is a topolinear space;
(II) $Pr(?A) = ?\,Pr(A)$
and $Pr(!A) = !\,Pr(A)$ for all $A \in \mathcal{L}_!$.

Recall **Lemma 2·4·1**. In this context, we have the result: $A \equiv_{LL!} B$ iff $Pr(A) = Pr(B)$.

Exercise 3·2·3:
Verify the provable equivalence $?A \equiv_{LL!} ?A \parr ?A$.

Lemma 3·2·4: (Girard [1987])

The set $\mathbb{E} = \{ Pr(?A) \mid A \in \mathcal{L}_1 \}$ satisfies the following conditions:

(ii) $\mathbb{E}$ is closed with respect to finite ⅋'s;

(iii) $\perp_m = \bigcap \mathbb{E}$.

(iv) for all $Pr(?A) \in \mathbb{E}$, $Pr(?A) = Pr(?A) ⅋ Pr(?A)$.

Proof:

(ii) Recall that $(?A) ⅋ (?B) \equiv_{LL!} ?(A \oplus B)$. (Lemma 3·0·2).

Then
$$Pr(?A) ⅋ Pr(?B) = Pr((?A) ⅋ (?B))$$
$$= Pr(?(A \oplus B)) \in \mathbb{E}.$$

By the obvious induction, $\mathbb{E}$ is closed with respect to finite ⅋'s.

(iii) $Pr(?0) \in \mathbb{E}$ and $Pr(\perp) = Pr(?0)$ since $\perp \equiv_{LL!} ?0$

Hence $\perp_m = Pr(\perp) \in \mathbb{E}$.

Let $\Gamma \in \perp_m$. Then $\vdash_* \Gamma$, hence $\vdash_* \Gamma, ?A$ by the rule (Th?). Hence $\Gamma \in Pr(?A)$.

Thus $\perp_m \subseteq Pr(?A)$ for all $Pr(?A) \in \mathbb{E}$,

hence $\perp_m = \bigcap \mathbb{E}$.

(iv) Since $?A \equiv_{LL!} ?A ⅋ ?A$,
$$Pr(?A) = Pr(?A ⅋ ?A) = Pr(?A) ⅋ Pr(?A).$$
□

Now if $\mathbb{F} = \{ \bigcap X \mid X \subseteq \mathbb{E} \}$

then clearly

(i) $\mathbb{F}$ is closed with respect to arbitrary intersections;

and (iii) $\perp_m = \bigcap \mathbb{F}$.

To verify that $\mathbb{F}$ satisfies the remaining two conditions, we need the following result.

<u>Lemma 3.2.5:</u> (Girard [1987])
Let $\langle P, \cdot, 1, \perp_P \rangle$ be any phase space and let $\{G_i\}_{i \in I}$ and $\{H_j\}_{j \in J}$ be families of facts of P.

then
$$\bigcap_{(i,j) \in I \times J} (G_i \invamp H_j) = \left(\bigcap_{i \in I} G_i\right) \invamp \left(\bigcap_{j \in J} H_j\right)$$

i.e. $\invamp$ distributes over arbitrary intersections.

<u>Proof:</u>
$$p \in \bigcap_{i,j} (G_i \invamp H_j)$$
iff $$p \in \bigcap_{i,j} (G_i^{\perp} \cdot H_j^{\perp})^{\perp}$$
iff $$\forall i \in I, \forall j \in J, \forall q \in G_i^{\perp}, \forall r \in H_j^{\perp} \ (pqr \in \perp)$$
iff $$\forall i \in I, \forall q \in G_i^{\perp}, \forall j \in J, \forall r \in H_j^{\perp} \ (pqr \in \perp)$$
iff $$\forall s \in \left(\bigcup_i G_i^{\perp}\right) \ \forall t \in \left(\bigcup_j H_j^{\perp}\right) \ (pst \in \perp)$$
iff $$\forall s \in \left(\bigcap_i G_i\right)^{\perp} \ \forall t \in \left(\bigcap_j H_j\right)^{\perp} \ (pst \in \perp)$$
iff $$p \in \left(\left(\bigcap_i G_i\right)^{\perp} \cdot \left(\bigcap_j H_j\right)^{\perp}\right)^{\perp}$$
iff $$p \in \left(\bigcap_i G_i\right) \invamp \left(\bigcap_j H_j\right)$$

The equivalence of lines 5 and 6 is due to Lemma 2.0.4.

$\square$

(ii) $\mathbb{F}$ is closed with respect to finite $⅋$'s since

$$\left(\bigcap_{i\in I} Pr(?A_i)\right) ⅋ \left(\bigcap_{j\in J} Pr(?B_j)\right) = \bigcap_{(i,j)\in I\times J} \left(Pr(?A_i) ⅋ Pr(?B_j)\right)$$
$$= \bigcap_{(i,j)\in I\times J} Pr(?(A_i \oplus B_j)).$$

and (iv) $⅋$ is idempotent on $\mathbb{F}$:

$$\left(\bigcap_{i\in I} Pr(?A_i)\right) ⅋ \left(\bigcap_{i\in I} Pr(?A_i)\right) = \bigcap_{i\in I} \left(Pr(?A_i) ⅋ Pr(?A_i)\right)$$
$$= \bigcap_{i\in I} Pr(?A_i).$$

We have now established that $\langle M, *, \emptyset, \perp_M, \mathbb{F}\rangle$ is a topolinear space.

Our remaining task is the verification of $?Pr(A) = Pr(?A)$; since $Pr(A^\perp) = Pr(A)^\perp$ (Lemma 2.4.4), we can readily derive $!Pr(A) = Pr(!A)$.

<u>Lemma 3.2.6:</u> (Girard [1987])

$\vdash A \multimap ?B$ is provable in LL!

iff $\vdash ?A \multimap ?B$ is provable in LL!

<u>Proof:</u>
If $\vdash A \multimap ?B$ is provable in LL! then so is $\vdash A^\perp, ?B$.

$$\dfrac{\dfrac{\vdash A^\perp, ?B}{\vdash !(A^\perp), ?B}\,(!)}{\vdash ?A \multimap ?B}\,(⅋)$$

Conversely, if $\vdash ?A \multimap ?B$ is provable in **LL!** then so is $\vdash !(A^\perp), ?B$.

$$\dfrac{\dfrac{\dfrac{\vdash A, A^\perp}{\vdash ?A, A^\perp}(D?) \qquad \begin{matrix}\vdots \\ \vdash !(A^\perp), ?B\end{matrix}}{\vdash A^\perp, ?B}(\text{CUT})}{\vdash A \multimap ?B}(\wp)$$

$\square$

Now, $?\,Pr(A)$ is the smallest fact in $\mathbb{F}$ containing $Pr(A)$.

$$\begin{aligned} ?\,Pr(A) &= \bigcap \{ \bigcap X \mid Pr(A) \subseteq \bigcap X \text{ and } X \subseteq \mathbb{E} \} \\ &= \bigcap \{ Pr(?B) \mid Pr(A) \subseteq Pr(?B) \} \\ &= \bigcap \{ Pr(?B) \mid \vdash_* A \multimap ?B \} \\ &= \bigcap \{ Pr(?B) \mid \vdash_* ?A \multimap ?B \} \\ &= \bigcap \{ Pr(?B) \mid Pr(?A) \subseteq Pr(?B) \} \\ &= Pr(?A). \end{aligned}$$

$\blacksquare$

3.3 A translation of intuitionistic logic

In **LL!**, the modal versions of contraction and thinning yield as theorems

$$!A \multimap (!A \otimes !A) \qquad \text{and} \qquad (!A \otimes !B) \multimap !A.$$

We can think of occurrences of '!' and '?' which are inside the scope of one of the binary propositional connectives as markers indicating that contraction and/or thinning may have been used. (Cut-free derivations of $(!A) \wp (?(A^\perp))$ are an exception.) Since the sequent calculus for intuitionistic logic, LJ, has contraction and thinning among its inference rules, one would expect that a translation of intuitionistic logic into modal linear logic would make heavy use of the modalities. (cf. the translation of intuitionistic logic into the classical modal logic S4.) The following translation does make heavy use of the modalities, but not uniformly.

<u>Definition 3·3·0</u>:
Let $\mathcal{L}_J$ be a language for intuitionistic propositional logic, generated from propositional letters and constants t and f using the unary connective $\neg$ and the binary connectives $\wedge$, $\vee$ and $\Rightarrow$.

We define a translation function $(\,)^\circ : \mathcal{L}_J \longrightarrow \mathcal{L}_!$ by induction on formulae as follows:

$$\begin{aligned}
A^\circ &= A \quad \text{if } A \text{ is a propositional letter;}\\
t^\circ &= \top\ ;\\
f^\circ &= 0\ ;\\
(A \wedge B)^\circ &= A \,\&\, B\ ;\\
(A \vee B)^\circ &= !(A^\circ) \oplus !(B^\circ)\ ;\\
(A \Rightarrow B)^\circ &= !(A^\circ) \multimap B^\circ\ ;\\
(\neg A)^\circ &= !(A^\circ) \multimap 0\ .
\end{aligned}$$

The mapping can be extended to a language for intuitionistic predicate logic, with quantifiers $\forall$ and $\exists$, as follows:

$$\begin{aligned}
(\forall x. A)^\circ &= \bigwedge x. A^\circ\ ;\\
(\exists x. A)^\circ &= \bigvee x. !(A^\circ)\ .
\end{aligned}$$

We will concentrate on the translation for propositional logics; keen readers can supply the extra details themselves.

At the moment, the most we can say about the virtue of this translation is that it works. In fact, it works very well: the translation is faithful, not only with respect to provable formulae but also with respect to proofs; we prove this below. An explanation as to <u>why</u> the translation works is to be found in coherent space semantics (Section 5).

Note that the translation of intuitionistic negation involves the additive falsum $\mathbf{0}$ rather than the multiplicative falsum $\perp$. If we had

$$(\neg A)^\circ = \,!(A^\circ) \multimap \perp$$

then $\quad (\neg A)^\circ \equiv_{LL:} (!(A^\circ))^\perp$.

Girard's comment is that intuitionistic negation has always been widely criticized (Girard [1987], p.79).

There is a formal analogy between the above translation and the definition of Kleene's 'slash' for formulae of Heyting Arithmetic. (Girard attributes this observation to Andrej Ščedrov.) The points at which 'extra' !'s are needed correspond to the points in the definition of '$\Gamma | E$' where the extra clause 'and $\Gamma \vdash E$ is provable in Heyting Arithmetic' is required. (See, for example, Moschovakis [1980], Definition 1.9) What, if anything, this means is not known.

In what follows, we will work with the two-sided sequent calculus for modal linear logic, **DLL!** ('D' for 'double'); the system is presented in Appendix B. **DLL!** makes for a smoother transition to Gentzen's sequent calculus for intuitionistic logic **LJ**, and from Gentzen's natural deduction system for intuitionistic logic **NJ** (actually, just the propositional subsystems thereof).

<u>Theorem 3·3·1</u>: (Girard [1987])
Let A be any formula of $\mathcal{L}_J$.
Given a cut-free proof π of $\vdash A^\circ$ in **DLL!**,
we can construct a (unique) cut-free proof $J(\pi)$ of $\vdash A$ in **LJ**.

<u>Proof</u>:
Let π be a cut-free proof of $\vdash A^\circ$ in **DLL!**.
Now A° is a formula in the $\{0, \&, \oplus, \multimap, !\}$ fragment of the language $\mathcal{L}_{D!}$ (in which $\multimap$, and $(-)^\perp$ are primitive). Hence π involves only rules from the $\{0, \&, \oplus, \multimap, !\}$ subsystem of **DLL!**, i.e. the identity axiom scheme, (EXCH), (CUT), the axiom scheme (0L) for 0 and logical rules for the connectives $\&, \oplus, \multimap$ and $!$. By examining these rules, we can convince ourselves that all sequents occurring in the proof π contain only <u>one</u> formula on their right-hand sides. Now we obtain $J(\pi)$ from π as follows: (i) erase all occurrences of $!$; (ii) replace each occurrence of 0 with f; and (iii) replace each occurrence of $\&, \oplus, \multimap$ with $\wedge, \vee, \Rightarrow$ respectively. Then $J(\pi)$ is a cut-free proof of $\vdash A$ in **LJ**. ∎

Theorem 3·3·2: (Girard [1987])
Let A be any formula of $\mathcal{L}_J$.
Given a deduction d of [Δ] A in NJ,
i.e. d is a deduction of A from a set of assumptions Δ,
we can construct a (unique) proof $(d)^\circ$ of $!\Delta^\circ \vdash A^\circ$ in DLL!
(where if $\Delta = \{C_1, \ldots, C_n\}$ then $!\Delta^\circ \vdash A^\circ$ means $!(C_1^\circ), \ldots, !(C_n^\circ) \vdash A$).

Proof:
The proof $(d)^\circ$ is defined by induction on d.

(i) d is the deduction of [A] A consisting of the assumption A.
Then $(d)^\circ$ is

$$\frac{A^\circ \vdash A^\circ}{!A^\circ \vdash A^\circ}\ (LD!)$$

(ii) d is a deduction of $[\Delta_1, \Delta_2]\ A_1 \wedge A_2$ obtained from a deduction d_1 of $[\Delta_1]\ A_1$ and a deduction d_2 of $[\Delta_2]\ A_2$ by the rule of $\wedge$ introduction.
Then $(d)^\circ$ is as follows:

$$\dfrac{\dfrac{\begin{array}{c}(d_1)^\circ\\ \vdots\\ !\Delta_1^\circ \vdash A_1^\circ\end{array}}{!\Delta_1^\circ, !\Delta_2^\circ \vdash A_1^\circ}\ \text{several } (LTh!) \qquad \dfrac{\begin{array}{c}(d_2)^\circ\\ \vdots\\ !\Delta_2^\circ \vdash A_2^\circ\end{array}}{!\Delta_1^\circ, !\Delta_2^\circ \vdash A_2^\circ}\ \text{several } (LTh!)}{!\Delta_1^\circ, !\Delta_2^\circ \vdash A_1^\circ \,\&\, A_2^\circ}\ (R\&)$$

And $(A_1 \wedge A_2)^\circ = A_1^\circ \,\&\, A_2^\circ$.

(iii) d is a deduction of $[\Delta]\, A_1$ obtained from a deduction d_1 of $[\Delta]\, A_1 \wedge A_2$ by the first $\wedge$ elimination rule. Then $(d)^\circ$ is as follows:

$$\dfrac{\begin{matrix}(d_1)^\circ \\ \vdots \\ !\Delta^\circ \vdash A_1^\circ \,\&\, A_2^\circ\end{matrix} \qquad \dfrac{A_1^\circ \vdash A_1^\circ}{A_1^\circ \,\&\, A_2^\circ \vdash A_1^\circ}\,(L\&1)}{!\Delta^\circ \vdash A_1^\circ}\,(\mathrm{CUT})$$

(iv) the case for the second $\wedge$ elimination rule is symmetric to (iii).

(v) d is a deduction of $[\Delta]\, A_1 \vee A_2$ obtained from a deduction d_1 of $[\Delta] A_1$ by the first $\vee$ introduction rule. Then $(d)^\circ$ is as follows:

$$\dfrac{\dfrac{\begin{matrix}(d_1)^\circ \\ \vdots \\ !\Delta^\circ \vdash A_1^\circ\end{matrix}}{!\Delta^\circ \vdash\, !(A_1^\circ)}\,(R!)}{!\Delta^\circ \vdash\, !(A_1^\circ) \oplus !(A_2^\circ)}\,(R\oplus 1)$$

And $(A_1 \vee A_2)^\circ = \,!(A_1^\circ) \oplus !(A_2^\circ)$.

(vi) The case for the second $\vee$ introduction rule is symmetric to (v).

(vii) d is a deduction of $[\Delta, \Gamma_1, \Gamma_2]\, A$ obtained from deductions e of $[\Delta]\, B_1 \vee B_2$,
d_1 of $[\Gamma_1, \Sigma_1]\, A$,
and d_2 of $[\Gamma_2, \Sigma_2]\, A$,
where Σ_1 and Σ_2 consist of a number of repetitions of B_1 and B_2 respectively (possibly zero) by $\vee$ elimination.

Then $(d)^\circ$ is as follows:

$$
\dfrac{\begin{array}{c}(e)^\circ \\ \vdots \\ !\Delta^\circ \vdash !C_1^\circ \oplus !C_2^\circ\end{array} \qquad \dfrac{\dfrac{\dfrac{\begin{array}{c}(d_1)^\circ \\ \vdots \\ !\Gamma_1^\circ, !\Sigma_1^\circ \vdash A^\circ\end{array}}{!\Gamma_1^\circ, !C_1^\circ \vdash A^\circ}[1]}{!\Gamma_1^\circ, !\Gamma_2^\circ, !C_1^\circ \vdash A^\circ}[2] \qquad \dfrac{\dfrac{\begin{array}{c}(d_2)^\circ \\ \vdots \\ !\Gamma_2^\circ, !\Sigma_2^\circ \vdash A^\circ\end{array}}{!\Gamma_2^\circ, !C_2^\circ \vdash A^\circ}[1]}{!\Gamma_1^\circ, !\Gamma_2^\circ, !C_2^\circ \vdash A^\circ}[2]}{!\Gamma_1^\circ, !\Gamma_2^\circ, !C_1^\circ \oplus !C_2^\circ \vdash A^\circ}(L\oplus)}{!\Delta^\circ, !\Gamma_1^\circ, !\Gamma_2^\circ \vdash A^\circ}(\mathrm{CUT})
$$

[1] indicates several $(LC!)$ or one $(LTh!)$;
[2] indicates several $(LTh!)$.

(viii) d is a deduction of $[\Delta]\, A \Rightarrow B$ obtained from a deduction d_1 of $[\Delta, \Gamma]\, B$, where Γ consists of a a number of repetition of **A** (possibly zero) by $\Rightarrow$ introduction. Then $(d)^\circ$ is as follows:

$$
\dfrac{\dfrac{\begin{array}{c}(d_1)^\circ \\ \vdots \\ !\Delta^\circ, !\Gamma^\circ \vdash B^\circ\end{array}}{!\Delta^\circ, !A^\circ \vdash B^\circ}\text{several }(LC!)\text{ or one }(LTh!)}{!\Delta^\circ \vdash !A^\circ \multimap B^\circ}(R\multimap)
$$

And $\quad (A \Rightarrow B)^\circ = !A^\circ \multimap B^\circ$

(ix) d is a deduction of $[\Delta, \Gamma]\, B$ obtained from a deduction d_1 of $[\Delta]\, A$ and a deduction d_2 of $[\Gamma]\, A \Rightarrow B$, by $\Rightarrow$ elimination.

Then $(d)^\circ$ is as follows:

$$
\dfrac{\begin{matrix}(d_2)^\circ\\ \vdots\\ !\Gamma^\circ \vdash !A^\circ \multimap B^\circ\end{matrix}
\qquad
\dfrac{\dfrac{\begin{matrix}(d_1)^\circ\\ \vdots\\ !\Delta^\circ \vdash A^\circ\end{matrix}}{!\Delta^\circ \vdash !A^\circ}\,(R!)
\qquad B^\circ \vdash B^\circ}{!\Delta^\circ,\ !A^\circ \multimap B^\circ \vdash B^\circ}\,(L\multimap)}
{!\Gamma^\circ,\ !\Delta^\circ \vdash B^\circ}\,(\mathrm{CUT})
$$

(x) d is a deduction of $[\Delta]A$ obtained from a deduction d_1 of $[\Delta]f$ by the f rule.
Recall that $(f)^\circ = \mathbf{0}$.

Then $(d)^\circ$ is as follows:

$$
\dfrac{\begin{matrix}(d_1)^\circ\\ \vdots\\ !\Delta^\circ \vdash \mathbf{0}\end{matrix}
\qquad
\begin{matrix}\text{instance of axiom}\\ \text{Scheme for } \mathbf{0}\\ \mathbf{0} \vdash B^\circ\end{matrix}}
{!\Delta^\circ \vdash B^\circ}\,(\mathrm{CUT})
$$

We dont have to deal with $\neg$ introduction or $\neg$ elimation as we can take $\neg A \overset{df}{\equiv} A \Rightarrow f$. ∎

4. What does it all mean?

4.0 A steady-state economy

In this section we give an intuitive, informal account of the connectives of propositional linear logic. Our discussion draws on Martí-Oliet and Meseguer [1989], Lafont [1988a], Appendix A, and Girard [1989], Section II.

We think of formulae as denoting states and interpret the linear implication connective $\multimap$ as expressing the possibility of transition between two given states. So

$$A \multimap B$$

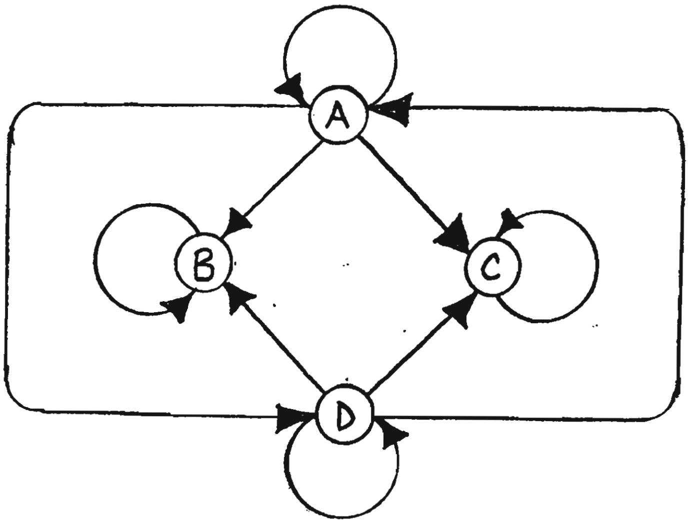
is read as meaning that states of type B are accessible from states of type A.

Consider the following example:

A := having a one dollar coin;
B := getting a felafel;
C := getting a doughnut;
D := having five twenty cent coins.

Our system is a little economy: transitions are monetary transactions. We rule out barter, i.e. exchange of one sort of non-monetary good for another. All resources or commodoties in our economy are of equal value, i.e. worth one dollar. Our guiding principle is that this is a 'steady-state' economy: the total value of resources after a transaction is the same as it was before that transaction. So no value is lost and no value is accrued.

The basic permissible transactions in our economy are given by the following diagram.



More formally, we need a language of propositional linear logic generated by four propositional letters A, B, C and D, and a theory with six non-logic axioms (given by the arrows other than the reflexive ones). With respect to the two-sided sequent calculus **DLL**, the non-logical axioms are $A \vdash B$, $A \vdash C$ etc. For more on linear theories and their connections with petri nets, all cast in a category-theoretic framework, see Martí-Oliet and Meseguer [1989].

Returning to our informal discussion, we have

$A \multimap B :=$ with a one dollar coin we can get a felafel;
$D \multimap A :=$ we can exchange five twenty cent coins for a one dollar coin;
$A \multimap A :=$ We start with a dollar coin and end up with a dollar coin (maybe a different coin).

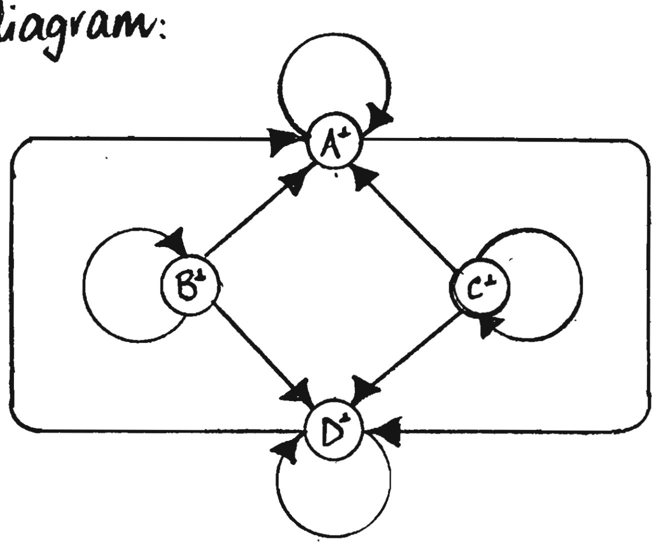
Instances of A, B, C and D correspond to <u>credits</u> on our ledger; their negations are <u>debits</u>. First, the multiplicative falsum:

$\bot :=$ being obliged to pay.

Then we have:

$B^{\bot} \equiv_{LL} B \multimap \bot :=$ We have a felafel and then are obliged to pay, i.e. we eat or otherwise dispose of the felafel.

The dual diagram:



represents permissible debt transactions. For example,

$B^{\bot} \multimap A^{\bot} :=$ if we eat a felafel then we can fulfil our obligation to pay by handing over a dollar coin;

$A^{\bot} \multimap D^{\bot} :=$ a debt of a one dollar coin can be replaced by a debt of five twenty cent coins.

The multiplicative conjunction is interpretted as an <u>accumulation</u> of resources. We have $A \multimap B$ and $A \multimap C$ but from these we <u>cannot</u> derive $A \multimap (B \otimes C)$.

$A \multimap (B \otimes C)$:= with a one dollar coin we can get <u>two</u> dollars worth of goods, one felafel <u>and</u> one doughnut.

This would mean getting something for free. The best we can do is $(A \otimes A) \multimap (B \otimes C)$. Returning to our favourite formulae, characteristic of contraction and thinning respectively,

$A \multimap (A \otimes A)$:= producing a dollar coin out of thin air;

$(A \otimes B) \multimap A$:= having a felafel vapourize before our eyes.

But what about the additive conjunction? From $A \multimap B$ and $A \multimap C$ we <u>can</u> derive $A \multimap (B \& C)$. Girard sees & as involving the superposition of states:

$A \multimap (B \& C)$:= having a one dollar coin, we can <u>choose</u> between getting a felafel and getting a doughnut; <u>both</u> possibilities are available — we get to choose which <u>one</u> is realized.

Recall that & is idempotent (while $\otimes$ is not): Choosing between a felafel and a felafel is no choice at all.

With &, something <u>external</u> to the system (in this case, us) gets to make a choice. There is also a choice involved with $\oplus$, but the choice is not ours to make. From $A \multimap C$, we can derive $A \multimap (C \oplus D)$.

$A \multimap (C \oplus D)$:= starting with a one dollar coin, we will get <u>either</u> a doughnut <u>or</u> five twenty cent coins; the choice is made by some mechanism <u>internal</u> to the system.

In this system, both C and D are accessible from **A**. We can also derive $A \multimap (C \oplus (D \otimes D \otimes D))$; in that case, the internal mechanism will always choose C.

The choice involved with $\oplus$ may seem a bit trivial: the 'internal mechanism' <u>should</u> always choose the disjunct from which the disjunction was inferred. Maybe it should, but sometimes it <u>can't</u> make the decision on that basis. Consider the following proof in **LL** (which we've seen before but is repeated here to make the point):

$$\dfrac{\dfrac{\dfrac{\vdash C^{\perp}, C}{\vdash C^{\perp}, C \oplus D}\,(\mathrm{FST}\oplus) \qquad \dfrac{\vdash D^{\perp}, D}{\vdash D^{\perp}, C \oplus D}\,(\mathrm{SND}\oplus)}{\vdash C^{\perp} \& D^{\perp}, C \oplus D}\,(\&)}{\vdash C \oplus D \multimap C \oplus D}\,(⅋)$$

With regard to the '$C \oplus D$' occurring in the consequent of the final implication, backtracking through the proof to see which of the two $\oplus$ rules were used will be of no help in trying to predict the decision of the 'internal mechanism'.

As one might guess from the above discussion, things are different when & or $\oplus$ occur in the antecedent of an implication, (or on the left hand side of a sequent). It seems as though the 'external/internal choice' characterization is reversed. From $A \multimap B$ and $D \multimap B$, we can derive $(A \oplus D) \multimap B$. Recalling that $(A \oplus D) \multimap B \equiv_{LL} (A \multimap B) \& (D \multimap B)$, the obvious reading is

$(A \oplus D) \multimap B$:= <u>We</u> can <u>choose</u> between spending a one dollar coin and spending five twenty cent coins when purchasing a felafel; both possibilities are available.

Now consider again $(C \oplus D) \multimap (C \oplus D)$. If <u>we</u> choose C in the antecedent then <u>it</u> (the 'internal mechanism') must choose C in the consequent (since D is not accessible from C). But if we choose D in the antecedent, then it can take its pick. (There seems to be a need for a general policy about priority of choices when there is competition; something like 'we always choose first, of course!' might do it.) For 'dual' reasons, the choice between starting places in, say, $(A \& D) \multimap B$ is most naturally read as an internal choice.

Note, however, that the 'accumulation' reading of $\otimes$ works, regardless of which side of the $\multimap$ the $\otimes$ occurs. For example:

$(A \otimes A \otimes D) \multimap (B \otimes C \otimes C)$:= With two one dollar coins and five twenty cent coins we can get one felafel and two doughnuts.

The multiplicative disjunction $\wp$ is more problematic. As Girard ([1989], p.73) rightly says, '... the meaning of '$\wp$' is not that easy.' One way of thinking of it is in terms of $\multimap$, i.e. $A \wp B = A^{\perp} \multimap B$ by definition. This is certainly the best way of thinking of the 'excluded middle' axioms $A \wp A^{\perp}$. The other way of thinking of $\wp$ is as the dual of $\otimes$: instead of accumulation of resources we have accumulation of debts. For example:

$(B^{\perp} \wp C^{\perp}) \multimap (A^{\perp} \wp A^{\perp})$:= We can replace a debt of one felafel and one doughnut by a debt of two one dollar coins.

This, however, gets us no closer to understanding what the $\wp$ of positive formulae means. We are left with the feeling that $\wp$ is by far the wierdest of the connectives of linear logic.

4·1 A licence to print money (!) and limited versions thereof.

When we adjoin the modal operators to linear logic, the steady-state economy is replaced by economic chaos:

$!A$:= unlimited possibilities for duplicating one dollar coins.

The inference from $\vdash A, ?\Delta$ to $\vdash !A, ?\Delta$ using (!) is analogous to putting A in a memory register so that it can be used ad nauseum. As Girard notes ([1989], p.84) the four modal rules of **LL!** differ from the rules for the additives and multiplicatives in that they do not completely characterize their connectives. If we were to introduce a second pair of additives &' and ⊕' with the same rules as for & and ⊕ then $A \&' B$ and $A \oplus' B$ will be provably equivalent to $A \& B$ and $A \oplus B$ respectively. The same holds for ⊗ and ⅋, but it does <u>not</u> hold for ! and ?. To establish $!A \equiv !'A$ we need proofs of both $\vdash ?A^{\perp}, !'A$ and $\vdash ?'A^{\perp}, !A$. We can get both $\vdash ?A^{\perp}, A$ and $\vdash ?'A^{\perp}, A$ but then get stuck because we have the wrong sort of question mark. However, since we want ! and ? to be dual, then given the (!) rule, the 'inverse' rule (D?) is forced upon us; (D?) in conjunction with (CUT) is analogous to retrieving data from a memory register. Continuing the metaphor, the rules (Th?) and (C?) are 'optional extras' which give us power to manipulate data in the memory register. This power was crucial in the translation of an **NJ** derivation into a **DLL!** proof (Theorem 3.3.2).

A note of caution is in order: the modal operators introduced in Girard and Lafont [1987] and Lafont [1988b], in the context of <u>intuitionistic</u> linear logic, do <u>differ</u> from those under discussion here; see Lafont [1988b], pp. 164-165 and Seely [1989], p. 379.

The operators ! and ? of **LL!** are perhaps best thought of as infinite generalizations of ⊗ and ⅋, similar to the sense in which the quantifiers Λ and V are infinite generalizations of & and ⊕, but not quite.

In Girard [1987] we have the proposal:

$$!A \approx \bigotimes_{\omega} (\mathbb{1} \& A) ;$$

$$?A \approx \bigparr_{\omega} (\bot \oplus A) .$$

(Since we have trouble understanding what $A \parr B$ means, an infinitary $\parr$ is going to fair no better at the level of comprehension.) Note that $\vdash (\mathbb{1} \& A) \multimap A$ and $\vdash A \multimap (\bot \oplus A)$ are provable in **LL**, but in general their converses are not. $\vdash A \multimap (\mathbb{1} \& A)$ is provable in **LL!** when A is $!B$, or more generally, when $\vdash A \multimap \mathbb{1}$ is provable. A story might be of some help. When we want to make use of $!A$, we begin by considering the first in our string of $(\mathbb{1} \& A)$'s. A choice has to be made (either by us or by <u>it</u>) between $\mathbb{1}$ and A. The choice of $\mathbb{1}$ is 'default mode' — $\mathbb{1}$ contains no <u>new</u> information. If the choice is ours, then we choose as many copies of A as we need to get on with the proof. For example, if there is a cut with $?A^\bot$ then the number of copies of A we choose may depend on the number of copies of $A^\bot$ <u>it</u> has chosen from the list of $(\bot \oplus A^\bot)$'s. If we are simulating an NJ derivation (as in theorem 3.3.2) in which A is an assumption formula which is used k times, then we'll keep on going through the $(\mathbb{1} \& A)$'s until we've got k copies of A. We have an unlimited number of <u>possibilities</u> for reproducing A, in contrast to the scenario in which $!A$ is

$$\bigotimes_{\omega} A ;$$

the latter gives us an unlimited number of actual copies of A.

The story gives some informal content to Girard's slogan that 'intuitionistic logic is obtained from [non-modal] linear logic by a passage to the limit.' Now for the mathematical content.

Definition 4.1.0:

Let A be any formula in the language $\mathcal{L}$ of propositional linear logic. For each positive integer n, we define

$$!_n A \stackrel{\mathrm{df}}{=} (\mathbb{1} \& A) \otimes \ldots \otimes (\mathbb{1} \& A) \qquad (n \text{ times});$$

$$?_n A \stackrel{\mathrm{df}}{=} (\bot \oplus A) \parr \ldots \parr (\bot \oplus A) \qquad (n \text{ times}).$$

Lemma 4.1.1:

The following are derived rules in **LL**:

$$\frac{\vdash \Delta}{\vdash ?_1 A, \Delta}\,(\text{ap. Th?}) \qquad \frac{\vdash ?_n A, ?_m A, \Delta}{\vdash ?_{n+m} A, \Delta}\,(\text{ap. C?})$$

$$\frac{\vdash A, \Delta}{\vdash ?_1 A, \Delta}\,(\text{ap. D?}) \qquad \frac{\vdash A, ?_{\underset{\sim}{n}} \Delta}{\vdash !_k A, ?_{k\underset{\sim}{n}} \Delta}\,(\text{ap.} !)$$

where $n, m, k \geqslant 1$, $?_{\underset{\sim}{n}} \Delta$ abbreviates $?_{n_1} C_1, \ldots, ?_{n_p} C_p$ with $n_i \geqslant 1$, $i = 1, \ldots, p$, and $?_{k\underset{\sim}{n}} \Delta$ abbreviates $?_{kn_1} C_1, \ldots, ?_{kn_p} C_p$. ('ap.' is for approximation.)

Proof:

Almost immediate. (ap. C?) requires only the ($\parr$) rule, (ap. D?) uses the (SND $\oplus$) rule with $\bot$ as first disjuct and (ap. Th?) requires an application of the rule ($\bot$) followed by (FST $\oplus$) with A as second disjunct. We give a derivation for (ap.!). Let Π_0 be a proof in **LL** of $\vdash A, ?_n B$ for some $n \geq 1$. Assume that from $\vdash A, ?_n B$ we can derive in **LL** the sequent $\vdash !_k A, ?_{kn} B$, for $k \geq 1$. Then

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash \mathbb{1}}{\vdash \mathbb{1}, ?_n B}\,[a] \qquad \begin{matrix}\Pi_0 \\ \vdots \\ \vdash A, ?_n B\end{matrix}}{\vdash \mathbb{1} \& A,\ ?_n B}\,(\&) \qquad \dfrac{\begin{matrix}\Pi_0 \\ \vdots \\ \vdash A, ?_n B\end{matrix}}{\vdash !_k A,\ ?_{kn} B}\,\begin{bmatrix}\text{induction} \\ \text{hypothesis}\end{bmatrix}}{\vdash (\mathbb{1} \& A) \otimes !_k A,\ ?_n B,\ ?_{kn} B}\,(\otimes)}{\vdash !_{k+1} A,\ ?_{n(k+1)} B}\,(⅋)$$

[a] denotes n (ap.Th?)'s together with n (⅋)'s. The base case of the induction is just the top left-hand part of the above. ■

Not suprisingly, the 'thinning-like' aspects of the rules for $\bot$ and $\oplus$ are exploited in giving an approximation of the modal thinning rule. In a less direct way, the implicit contraction involved in the rule (&) is used to get the nice polynomial property in (ap.!).

<u>Lemma 4.1.2:</u>

The following are derived rules in **LL**:

for any $n < m$,

$$\dfrac{\vdash ?_n A, \Delta}{\vdash ?_m A, \Delta}\,(\text{ap.}?\uparrow) \qquad\qquad \dfrac{\vdash !_m A, \Delta}{\vdash !_n A, \Delta}\,(\text{ap.}!\downarrow)$$

<u>Proof:</u>

(ap.?↑) just involves multiple applications of (ap.Th?) followed by (⅋)'s. (ap.!↓) uses (ap.?↑) together with (CUT):

$$\cfrac{\cfrac{\vdash ?_n A^\perp,\ !_n A}{\vdash ?_m A^\perp,\ !_n A}\,(ap.?\uparrow) \qquad \vdash !_m A,\ \Delta}{\vdash !_n A,\ \Delta}\,(CUT)$$

■

Suppose that we did translate **!A** as a straight infinitary $\otimes$, and hence had approximants

$$!'_n A \stackrel{df}{=} A \otimes \ldots \otimes A \qquad (n \text{ times});$$
$$?'_n A \stackrel{df}{=} A \parr \ldots \parr A \qquad (n \text{ times}).$$

Then the approximation of the modal thinning rule, (ap. Th?') is not sound with respect to phase space semantics, and hence the same fate befalls the analogous increase and decrease rules (ap. ?'↑) and (ap. !'↓), (which of course means these rules aren't derivable in **LL**).

To see that we can have a fact G fail to be verified but have $G \otimes G$ verified, consider the phase space $P = \langle \mathbb{Z}/5\mathbb{Z}, +, 0, \perp_P \rangle$ where $\perp_P = \{1, 2\}$ and $\mathbb{1} = \{0\}$. Let

$$G = \{4\}^\perp = \{n \mid n+4 \in \{1,2\}\ [\text{mod } 5]\} = \{2,3\}.$$

So the identity $0 \notin G$. But $GG = \{0,1,4\}$, hence $0 \in G \otimes G = (GG)^{\perp\perp}$. In fact, $G \otimes G = \mathbf{T}$.

To put the complaint more directly, the would-be approximation (ap. Th?') just is full-blown thinning:

$$\frac{\vdash \Delta}{\vdash A, \Delta}$$

And now to return to the task at hand.

<u>Theorem 4.1.3</u>: Approximation Theorem (Girard [1987])

If π is a cut-free proof in **LL!** of $\vdash A_1, \ldots, A_p$ and, for each $i = 1, \ldots, p$, we assign to each occurrence of ! in A_i a positive integer (called the <u>index</u> of that occurrence of !)

then, for each $i = 1, \ldots, p$ and each occurrence of ? in A_i we can specify an index (positive integer) in such a way that if $A_i^\bullet$ is the result of replacing each occurrence of ! in A_i by $!_k$, where k is the index of that occurrence of !, and replacing each occurrence of ? in A_i by $?_m$, where m is the index specified for that occurrence of ?, then there is a cut-free proof $(\pi)^\bullet$ in **LL** of $\vdash A_1^\bullet, \ldots, A_p^\bullet$.

<u>Proof</u>:

By induction on the cut-free proof π.

(i) π is an instance of the axiom scheme $\vdash A, A^\perp$: the identity axiom scheme is restricted to literals, so there is nothing to do; similarly if π is the axiom $\vdash \mathbb{1}$.

(ii) π is obtained from π_0 by the either the rule (EXCH) or the rule ($\perp$): obvious.

(iii) π is an instance of the axiom scheme $\vdash \top, A_1, \ldots, A_n$: the ! indices for each A_i place no restriction on the ? indices; we can set them equal to 1.

(iv) π is obtained from π_0 by the rule (FST $\oplus$):

$$\frac{\vdash A, \Delta}{\vdash A \oplus B, \Delta}\ (\text{FST}\oplus)$$

Assign an index to each occurrence of ! in $A \oplus B, \Delta$; this induces an assignment of ! indices in A, Δ. The induction hypothesis gives us a proof $(\pi_0)^\bullet$ of $\vdash A^\bullet, \Delta^\bullet$. Set all ? indices in B to 1 to give $B^\bullet$. Then $(\pi)^\bullet$ is obtained from $(\pi_0)^\bullet$ by applying (FST $\oplus$) with respect to $B^\bullet$. Likewise for the rule (SND $\oplus$).

(v) π is either obtained from π_0 and π_1 by ($\otimes$), or else obtained from π_2 by ($⅋$): the occurrences of ! and ? in the conclusion sequent are exactly those of the premise sequents (or sequent) so the induction hypothesis gives us all we need.

(vi) π is obtained from π_0 by the rule (Th?):

$$\frac{\vdash \Delta}{\vdash ?A, \Delta}\ (\text{Th?})$$

Assign an index to each occurrence of ! in $?A, \Delta$, inducing an assignment of ! indices in Δ. By the induction hypothesis, we have a proof $(\pi_0)^\bullet$ of $\vdash \Delta^\bullet$. Set all ? indices in A to 1 to give $A^\bullet$. Then apply the rule (ap. Th?) to $(\pi_0)^\bullet$.

(vii) π is obtained from π_0 by the rule (D?):

$$\frac{\vdash A, \Delta}{\vdash ?A, \Delta}\ (\text{D?})$$

As in case (vi), except that the induction hypothesis gives us a proof $(\pi_0)^\bullet$ of $\vdash A^\bullet, \Delta^\bullet$. Apply the rule (ap. D?) to $(\pi_0)^\bullet$ to give a proof $(\pi)^\bullet$ of $\vdash ?_1 A^\bullet, \Delta^\bullet$.

(viii) Π is obtained from Π_0 by the rule (!):

$$\frac{\vdash A,\ ?\Delta}{\vdash\ !A,\ ?\Delta}\ (!)$$

Assign an index to each occurrence of ! in $?A, \Delta$; suppose the index of the first ! in $!A$ is k. The induction hypothesis gives a proof $(\Pi_0)^\bullet$ of $\vdash A^\bullet, ?_{\underset{\sim}{n}} \Delta^\bullet$. Now apply (ap.!) to get a proof $(\Pi)^\bullet$ of $\vdash\ !_k A^\bullet, ?_{k\underset{\sim}{n}} \Delta^\bullet$.

The remaining two cases, the modal contraction rule (C?) and the rule (&), pose greater difficulties precisely because of their contractive nature.

(ix) Π is obtained from Π_0 by the rule (C?):

$$\frac{\vdash ?A, ?A, \Delta}{\vdash ?A, \Delta}\ (C?)$$

Assign an index to each occurrence of ! in $?A, \Delta$. This induces an assignment of ! indices in $?A, ?A, \Delta$; in particular, the corresponding ! indices in the two occurrences of $?A$ are identical. The induction hypothesis gives us a proof $(\Pi_0)^\bullet$ of $\vdash ?_n A', ?_m A'', \Delta^\bullet$ where A' and A'' are both approximants of A, but may differ with respect to ? indices. If $A' = A''$ then apply the rule (ap.C?) to get a proof $(\Pi)^\bullet$ of $\vdash ?_{n+m} A', \Delta^\bullet$. Otherwise, there are $q \geq 1$ occurrences of ? in A such that if i and j are the indices specified for that ? in A' and A'' respectively, then $i \neq j$. The following procedure is required.

<u>Step one</u>. Find the largest subformula $?D$ of A such that $?_i D'$ and $?_j D''$ are the corresponding subformulae of A' and A'' respectively, with D' and D'' both approximants of D, and $i \neq j$. If there are two or more occurrences of a subformula $?D$ of A with this property, or else there are two or more distinct subformulae of A with this property and all of maximal size,

then take the one that is in the scope of the least number of connectives; if there is still a tie, take the leftmost. Assume $i<j$. (when $i>j$, the procedure is symmetric).

Step two. 'Back-track' up each branch of the proof $(\Pi_0)^\bullet$, making a note of those occurrences of $?_i D'$ which are subformulae of subformulae of A' and are direct ancestors of the occurrence of the $?_i D'$ in A' under investigation. Call these the lineage of the $?_i D'$.

Step three. On each branch of $(\Pi_0)^\bullet$ which involves the lineage of the $?_i D'$, find the lowest sequent in which one of the lineage of the $?_i D'$ occurs as a formula, i.e. the sequent which is the premis of a rule in virtue of which one of the lineage of the $?_i D'$ first becomes a proper subformula of some formula. Call such a sequent free for $?_i D'$. On each branch of $(\Pi_0)^\bullet$ with a sequent of the form $\vdash \Gamma, ?_i D', \Sigma$ free for $?_i D'$, apply the derived rule $(\mathrm{ap}.?\uparrow)$ to obtain a sequent of the form $\vdash \Gamma, ?_j D', \Sigma$ then return to the proof $(\Pi_0)^\bullet$ and replace all lower occurrences of $?_i D'$ which are in the lineage of the $?_i D'$ by $?_j D'$. A branch of $(\Pi_0)^\bullet$ which involves the lineage of the $?_i D'$ will only fail to have a sequent free for $?_i D'$ if the earliest member of the lineage of the $?_i D'$ on that branch is either a subformula of the 'new' disjunct introduced by an application of one of the $\oplus$ rules or else is a proper subformulae of a formula occurring in an instance of the axiom scheme for T. Now duplicate that application of a $\oplus$ rule (that instance of the T axiom scheme) except for replacing that (those) occurrence(s) of $?D'$ which are in the lineage of the $?_i D'$ by $?_j D'$, and do the same for all lower occurrences of $?_i D'$ which are in the lineage of the $?_i D'$.

The result of these modications to the proof $(\Pi_0)^\bullet$ will be a proof μ_1 in **LL** of $\vdash ?_n A''', ?_m A'', \Delta^\bullet$ where A''' is the same as A' except that the occurrence of $?_i D'$ has been transformed into $?_j D'$. We claim that A''' and A'' have exactly $q-1$ discrepant pairs of ? indices and hence, by the obvious induction, we will have after q iterations of the three-step procedure a proof μ_q in **LL** of $\vdash ?_n A^\bullet, ?_m A^\bullet, \Delta^\bullet$. Our claim is based on the fact that by always working on the outermost discrepant ? indices and by only increasing indices in the lineage of the occurrence of the subformula under investigation, we never <u>create</u> a discrepancy of ? indices and once a discrepancy has been fixed, we never have to attend to it again.

(x) Π is obtained from Π_0 and Π_1 by the rule (&):

$$\frac{\vdash A, C_1, \ldots, C_r \qquad \vdash B, C_1, \ldots, C_r}{\vdash A\& B, C_1, \ldots, C_r.}\ (\&)$$

This time we have proofs $(\Pi_0)^\bullet$ and $(\Pi_1)^\bullet$ in **LL** of $\vdash A^\bullet, C_1', \ldots, C_r'$ and $\vdash B^\bullet, C_1'', \ldots, C_r''$ respectively, where for $i = 1, \ldots, r$, C_i' and C_i'' are both approximants of C_i but may differ with respect to ? indices. The procedure is analogous to that given in case (ix). For each discrepant pair of ? indices, we have to either make suitable modifications to ? indices in $(\Pi_0)^\bullet$, or else do likewise for $(\Pi_1)^\bullet$. The result gives proofs μ_0 and μ_1 in **LL** of $\vdash A^\bullet, C_1^\bullet, \ldots, C_r^\bullet$ and $\vdash B, C_1^\bullet, \ldots, C_r^\bullet$ respectively; then obtain the proof $(\Pi)^\bullet$ of $\vdash A^\bullet \& B^\bullet, C_1^\bullet, \ldots, C_r^\bullet$ by (&).

∎

Unfortunately, the effort required to fill in the missing details in Girard's proof [1987], p.93, turned out to be much greater than the author first anticipated.

An obvious consequence of the Approximation Theorem is that given any <u>theorem</u> of propositional intuitionistic logic (or provable sequent of propositional **LJ**) we can produce approximants of its translate which are provable in **LL**. However, we don't have approximants for the translate in **LL!** of each <u>proof</u> in propositional **LJ** (going via Gentzen's translation of **LJ** proofs into **NJ** derivations, then applying Theorem 3.3.2); the hypothesis of the Approximation Theorem that the proof in **LL!** be cut-free is crucial since we need the subformula property.

The polynomial structure underlying the 'exponential' (modal) connectives ! and ? is of particular note.

<u>Corollary 4.1.4:</u>

If π is a cut-free proof in **LL!** of $\vdash \Delta$
and $x_1, \ldots, x_s$ are distinct variables associated with the s occurrences of ! in Δ in, say, left to right order,
then for each occurrence of ? in Δ there is a polynomial function $p(x_1, \ldots, x_s)$ such that, given assignments $k_1, \ldots, k_s$ of positive integers to the variables $x_1, \ldots, x_s$, if $\Delta^\bullet$ is obtained from Δ by replacing the ith occurrence of ! in Δ by $!_{k_i}$, for $i = 1, \ldots, s$, and replacing each occurrence of ? in Δ by $?_{p(\underline{k})}$, where p is the polynomial for that ? and $p(\underline{k}) = p(k_1, \ldots, k_s)$,
then there is a cut-free proof $(\pi)^\bullet$ in **LL** of $\vdash \Delta^\bullet$.

Proof:

By induction on the cut-free proof π. In cases except (C?) and (&), the polynomial in question falls out of the proof of the Approximation theorem. Suppose we have a proof in **LL** of $\vdash ?_f A', ?_g A'', \Delta^\circ$, i.e. the polynomials for the displayed ? in $\vdash ?A, ?A, \Delta$ are f and g respectively, and A' and A'' are 'polynomial' approximants of A. As in case (ix) of the proof above, we start with the outermost and leftmost occurrence of ? in A which gives rise to a discrepancy between A' and A''. Suppose p is the polynomial for that occurrence of ? in A' and q is the polynomial for that occurrence of ? in A'' and $p \neq q$. To repair the discrepancy, we replace <u>both</u> p and q by the polynomial $\max\{p, q\} = p + (q \dot{-} p)$, and do the same for <u>both</u> the ancestors of that ? in A' and the ancestors of that ? in A''. A similar manouvre works for the rule (&). ∎

In recent work, Girard, Ščedrov and Scott [1990] have developed a system called Bounded Linear Logic (**BLL**) with modalities of the form $!_{x<p} A$ where p is a certain type of polynomial not containing the variable x. (They use a two-sided sequent calculus and ignore '?'.) **BLL** also has full, impredicative second-order quantification so types of natural numbers are definable, but the bounded !'s give rise to distinct <u>levels</u> of natural numbers. Their main result is that there is a one-one correspondance between the class **P** of polynomial-time computable functions and a certain class of closed terms in **BLL**.

5. Coherent space semantics

The phase space semantics provided, in a Tarskian manner, an algebraic interpretation of formulae of linear logic. An alternative approach to semantics, that of Heyting, involves the modelling of proofs. In this tradition, proofs are associated with functions or relations on some kind of constructive space. Dana Scott's theory of domains (eg. Scott [1982]) is prominent in this tradition. Girard reworks Scott's theory to create a new kind of domain which he calls coherent spaces. It is within this framework that we get to see how linear implication emerges from a decomposition of intuitionistic implication. In this section we draw on material from Girard, Lafont and Taylor [1989] and Lafont [1988a] in order to fill in the background of Chapter 3 of Girard [1987].

5.0 Coherent spaces and webs

Definition 5.0.1:
A coherent space X is a family of sets satisfying the following conditions:
(i) if $a \in X$ and $b \subseteq a$ then $b \in X$;
(ii) if $S \subseteq X$ and for all $a, b \in S$, $a \cup b \in X$ then $\bigcup S \in X$.
If $a \in X$ then a is called an object of X.

Considering a coherent space X as partially ordered by inclusion, (i) says that X is closed downward.

As a consequence, $\emptyset \in X$; $\emptyset$ is the <u>undefined object</u> of X. Furthermore, if $a, b \in X$ then $a \cap b \in X$ by (i). Indeed, if S is any <u>non-empty</u> subfamily of X, then $\bigcap S \in X$. When $a, b \in X$, $a \cup b$ will often fail to be an object of X. For most coherent spaces X, $\bigcap \emptyset = \bigcup X \notin X$. Call a subfamily $S \subseteq X$ (binarily) <u>linked</u> iff for all $a, b \in S$, $a \cup b \in X$. Combining conditions (i) and (ii), we have $\bigcup S \in X$ iff S is linked. Condition (ii) is known as binary completeness.

Recall that a family of sets S is (upwards) <u>directed</u> iff for all $a, b \in S$ there exists $c \in S$ such that $a \cup b \subseteq c$. For a coherent space X, if $S \subseteq X$ is directed then S is linked, but not conversely. If S is directed, we have $\bigcup^{\uparrow} S \in X$. For any object $a \in X$, the collection of all finite subsets of a is directed, and

$$a = \bigcup{}^{\uparrow}\{ a_0 \mid a_0 \subseteq a \text{ and } a_0 \text{ finite} \}.$$

This means that coherent spaces are, in the terminology of universal algebra, <u>algebraic</u> conditionally complete inf semi-lattices with binary completeness with respect to sups. (See, for example, Burris and Sankappanavar [1981].) In what follows, we'll be particularly interested in the directed family

$$X_{fin} \overset{df}{=} \{ a \in X \mid a \text{ finite} \}$$

where X is a coherent space.

Consider a few examples of (very simple) coherent spaces.

$\mathrm{Emp} \stackrel{\mathrm{df}}{=} \{\emptyset\}$;

$\mathrm{Sgl} \stackrel{\mathrm{df}}{=} \{\emptyset, \{@\}\}$ where @ is some arbitrarily chosen, fixed element;

$\mathrm{Bool} \stackrel{\mathrm{df}}{=} \{\emptyset, \{t\}, \{f\}\}$;

$\mathrm{Int} \stackrel{\mathrm{df}}{=} \{\emptyset\} \cup \{\{n\} \mid n \in \mathbb{N}\}$.

Definition 5.0.2:

Let X be a coherent space. The web of X, denoted $W(X)$, is a reflexive, unoriented graph defined as follows:

(i) the domain of the graph,

$$|X| \stackrel{\mathrm{df}}{=} \bigcup X = \{x \mid \{x\} \in X\};$$

(ii) the edge relation, coherence modulo X, is given by

$$x \supset x' \,[\mathrm{mod}\, X] \quad \text{iff} \quad \{x, x'\} \in X.$$

The second identity in (i) is due to the down closure of X. It is important to note that the coherence mod X relation is not in general transitive: when $x \supset x'$ [mod X] and $x' \supset x''$ [mod X], we will have $x \supset x''$ [mod X] only if $\{x, x', x''\} \in X$.

We can now see a coherent space X as a subset of $\mathcal{P}(|X|)$. Observe that, for any subset $a \subseteq |X|$,

$$a \in X \quad \text{iff} \quad \text{for all finite } a_0 \subseteq a, \; a_0 \in X.$$

The crucial point is that not all finite subsets of $|X|$ are objects of X, except in extreme cases.

Proposition 5.0.3 : (Girard [1987])
The map W from the class of coherent spaces to the class of reflexive, unoriented graphs given by $X \mapsto W(X)$ is a bijection. Moreover, the coherent space may be recovered from its web by means of the equivalence:

$$a \in X \text{ iff } a \subseteq |X| \text{ and for all } x, x' \in a\,(x \frown x' \,[\mathrm{mod}\, X]).$$

Proof:

We first establish the equivalence. Let $a \in X$. Then $a \subseteq |X|$, and for any $x, x' \in a$, we have $\{x, x'\} \subseteq a$ hence $\{x, x'\} \in X$ by down closure. Conversely, assume $a \subseteq |X|$ and for all $x, x' \in a$, $x \frown x' \,[\mathrm{mod}\, X]$. Then $\{x\} \cup \{x'\} \in X$ for all $x, x' \in a$. Hence $\bigcup \{\{x\} \mid x \in a\} = a \in X$ by binary completeness.

In virtue of the equivalence, we can say that an object of X is a <u>coherent subset</u> of $|X|$; as such, it is the underlying set of a <u>complete subgraph</u> of $W(X)$. Translating the conditions in the definition of coherent spaces into graph-theoretic terms, down closure says that any subgraph of a complete subgraph is complete, and binary completeness says that if S is a family of complete subgraphs, any two of which are <u>linked</u> in the sense that between any node of one and every node of the other, there is an edge, then the union of S is a complete subgraph. Both of these properties hold of reflexive, unoriented graphs. That gets surjectivity; injectivity is obvious. ■

We will informally assume, but not stipulate definitionally, that webs are countable (which means coherent spaces may have the power of the continuum). If one is particularly concerned with constructivity, then one should assume that the coherent spaces in question have webs whose coherence relation is <u>recursive</u>; we will frequently have to 'exclude middles' and assume that for all $x, x' \in |X|$, if $x \neq x'$ then either $x \frown x'$ [mod X] or <u>not</u> ($x \frown x'$ [mod X]); i.e. either $\{x, x'\} \in X$ or $\{x, x'\} \notin X$. Which means membership and identity had better be recursive. In analogy with Scott's theory of domains, we can think of the $x \in |X|$ as finite pieces of data.

In what follows, we will work mainly with webs; in particular, we define coherent spaces by specifying the domain and coherence relation of the web.

If X and Y are coherent spaces then a graph homomorphism from W(X) into W(Y) is a function $f: |X| \to |Y|$ such that

$$x \frown x' \text{ [mod X]} \quad \text{iff} \quad f(x) \frown f(x') \text{ [mod Y]}$$

for all $x, x' \in X$. Such a function induces a (unique) function $\bar{f}: X \to Y$ defined, for each $a \in X$, by

$$\bar{f}(a) = \{ f(x) \mid x \in a \}.$$

<u>Observation 5.0.4:</u>

If X and Y are coherent spaces and $f: |X| \to |Y|$ is a graph homomorphism from W(X) into W(Y) then the function $\bar{f}: X \to Y$ has the following properties:

(I) monotonicity: if $a, a' \in X$ and $a \subseteq a'$ then $\bar{f}(a) \subseteq \bar{f}(a')$;

(II) preservation of unions (those that there are):
if $S \subseteq X$ is linked then $\bar{f}(\bigcup S) = \bigcup\{\bar{f}(a) \mid a \in S\}$;

(III) preservation of non-empty intersections:
if S is non-empty then $\bar{f}(\bigcap S) = \bigcap\{\bar{f}(a) \mid a \in S\}$;

(IV) preservation of singletons: for all $x \in |X|$, $\bar{f}(\{x\}) = \{f(x)\}$;

(V) strong preservation of undefined objects: $\bar{f}(a) = \emptyset$ iff $a = \emptyset$.

(Verification involves mindlessly writing out definitions.)

In short, graph homomorphisms induce functions on coherent spaces which preserve every bit of structure there is. Let us say that a function $g : X \to Y$ is a coherent space homomorphism iff g satisfies conditions (I)–(V) above. Such a g uniquely detemines a graph homomorphism $\hat{g} : |X| \to |Y|$ defined by the equivalence

$$\hat{g}(x) = y \quad \text{iff} \quad g(\{x\}) = \{y\}.$$

Hence we have an isomorphism from the category of coherent spaces with coherent space homomorphisms onto the category of reflexive, unoriented graphs with graph homomorphisms given by

$$X \longmapsto W(X)$$
$$g : X \to Y \longmapsto \hat{g} : |X| \to |Y|.$$

We say that coherent spaces X and Y are canonically isomorphic, written $X \approx Y$, iff there is a graph isomorphism $f : |X| \to |Y|$ defined uniformly for all arguments, by which we mean natural in the category-theoretic sense.

In what follows, the classes of functions we need to characterize the function spaces $X \Rightarrow Y$ and $X \multimap Y$ will preserve rather less structure than coherent space homomorphisms (and hence be more interesting). The list (I)–(V) of properties is useful in providing a yard-stick (although note that the list contains redundancies: eg. (II) implies (I)) as well as clarifying what we take Girard to mean by 'canonical isomorphism' — Girard [1987], pp. 48–49.

Recall our examples of coherence spaces. The domain of their webs are as follows:

$|\mathrm{Sgl}| = \{@\}$

$|\mathrm{Bool}| = \{t, f\}$

$|\mathrm{Int}| = \mathbb{N}$

In each case, the coherence relation is such that for all $x, x' \in |X|$, $x \supset x'\,[\mathrm{mod}\,X]$ iff $x = x'$, hence the webs are <u>discrete graphs</u>. Such coherence spaces are called <u>flat</u>. Up to isomorphism, there is only one flat coherent space of a given cardinality. For the case of cardinality zero we have Emp, where $|\mathrm{Emp}| = \emptyset$.

At the other extreme are coherent spaces X such that for <u>all</u> $x, x' \in |X|$, $x \supset x'\,[\mathrm{mod}\,X]$. Here, $W(X)$ is a complete graph. Observe that $\bigcup X = |X| \in X$, so by down closure, $X = \mathcal{P}(|X|)$. Hence X is a complete boolean algebra. We propose the name <u>round</u> for such coherent spaces. Observe that Emp and Sgl are the only coherent spaces that are both flat and round.

A word on notation and terminology is in order. In Lafont [1988a], the construction is reversed: Lafont first defines what we call webs and then defines what we call coherent spaces. A straight translation of Lafont [1988a] into Girard [1987] is as follows:

coherent space, $A \longmapsto |X|$, domain of $W(X)$;
coherent subsets of A, $\mathrm{Coh}(A) \longmapsto X$, coherent space.

Coherent spaces in the sense of Girard [1987] are relatives of <u>domains</u> in the sense of Scott. Following the notation of Scott [1982], we give a 'wobbly' correspondance with Girard [1987]:

given an <u>information system</u> $A = \langle D_A, \Delta_A, \mathrm{Con}_A, \vdash_A \rangle$,

the <u>domain</u> determined by A,	$\lvert A\rvert$	$\leftrightsquigarrow$	X, coherent space;
the data objects of A,	D_A	$\leftrightsquigarrow$	$\lvert X\rvert$, domain of $W(X)$;
the undefined element $\Delta_A \in D_A$,	$\{\Delta_A\}$	$\leftrightsquigarrow$	$\emptyset \in X$
a family of finite subsets of D_A,	Con_A	$\leftrightsquigarrow$	X_{fin}.

Girard drops Scott's entailment relation $\vdash_A \subseteq \mathrm{Con}_A \times D_A$, and replaces it with the rather different relation of coherence modulo X, contained in $|X| \times |X|$. In particular, we <u>don't</u> have: $a \vdash_A y$ iff for all $x \in a$, $x \frown y\ [\mathrm{mod}\ X]$. The relation $\vdash_A$ is transitive in the sense that

if $a \vdash_A y$ for all $y \in b$ and $b \vdash_A z$ then $a \vdash_A z$.

We can have $a \cup b \in X$ and $b \cup \{z\} \in X$ but $a \cup \{z\} \notin X$.

The following auxilliary notions are required.

Definition 5.0.5:
Let X be a coherent space, and let $x, x' \in |X|$.

(i) strict coherence:

$$x \frown x' \, [\mathrm{mod}\, X] \text{ iff } x \supset x' \, [\mathrm{mod}\, X] \text{ and } x \neq x';$$
$$\text{iff } \{x, x'\} \in X \text{ and } x \neq x'.$$

(ii) strict incoherence:

$$x \smile x' \, [\mathrm{mod}\, X] \text{ iff } \underline{\text{not}} \left(x \supset x' \, [\mathrm{mod}\, X] \right);$$
$$\text{iff } \{x, x'\} \notin X.$$

(iii) incoherence:

$$x \asymp x' \, [\mathrm{mod}\, X] \text{ iff not } \left(x \frown x' \, [\mathrm{mod}\, X] \right);$$
$$\text{iff } \{x, x'\} \notin X \text{ or } x = x'.$$

Definition 5.0.6:
If X is a coherent space then its linear negation $X^\perp$ is defined by

$$|X^\perp| \overset{\mathrm{df}}{=} |X|;$$

$$x \supset x' \, [\mathrm{mod}\, X^\perp] \text{ iff } x \asymp x' \, [\mathrm{mod}\, X].$$

So linear negation exchanges coherence and incoherence. Note that we have the identity $X^{\perp\perp} = X$. Hence we have a tertium non datur:

for all $x, x' \in |X|$, either $x \supset x' \, [\mathrm{mod}\, X]$ or $x \supset x' \, [\mathrm{mod}\, X^\perp]$.

Actually, that is cheating: the above translates as

for all $x, x' \in |X|$, either $\{x, x'\} \in X$ or $\{x, x'\} \notin X$ <u>or</u> $x = x'$.

How about <u>quartum non datur</u> ?

Observe that the objects $a \in X^{\perp}$, which are (the underlying set of) <u>complete</u> subgraphs in $W(X^{\perp})$, are <u>discrete</u> subgraphs of $W(X)$, i.e. collections of isolated nodes. Graphically, the $(-)^{\perp}$ operation puts in an edge everywhere there wasn't one and removes all the edges that were there, except the reflexive ones. Recalling our previous examples, the linear negation of a flat coherent space is a round coherent space, and vice-versa. For example, $\mathrm{Int}^{\perp}$ is a countable boolean algebra.

<u>Definition 5.0.7:</u>

$$\mathbb{1} \stackrel{\mathrm{df}}{=} \mathrm{Sgl} \;;\quad \perp \stackrel{\mathrm{df}}{=} \mathbb{1}^{\perp} \;;\quad \mathbb{O} \stackrel{\mathrm{df}}{=} \mathrm{Emp} \;;\quad \top \stackrel{\mathrm{df}}{=} \mathbb{O}^{\perp}.$$

You've already seen the problem: Sgl and Emp are both flat and round.

$$|\mathbb{1}| = |\perp| = \{@\}, \qquad @ \frown @ \; [\mathrm{mod}\; \mathbb{1}] \;\; \underline{\text{and}} \;\; @ \frown @ \; [\mathrm{mod} \perp];$$

$$|\mathbb{O}| = |\top| = \emptyset .$$

This is not merely a glitch that can be patched up; we just have to live with it. Our dual constants are still going to behave the way we want them to, and we use the distinct notations to indicate this, but underneath the notation they are, in <u>this</u> semantics, the same.

The $\mathbb{1}/\perp$ and $\mathbb{0}/\top$ difficulty brings to the fore an important point: canonical isomorphisms $\approx$ are not going to correspond to provable equivalence in LL or LL! (while identities in the phase semantics do). If two formulae are provably equivalent then the coherent spaces interpreting them will be canonically isomorphic. A counter-example to the converse is that $\mathbb{1} \approx \perp$ (there is nothing more canonical than identity) but, of course, $\mathbb{1} \equiv_{LL} \perp$ is nonsense. As some consolation, all the sensible canonical isomorphisms will correspond to provable equivalences.

5.1 Direct sums and stable functions

The two additive operations, & and $\oplus$, are variations on the theme of the direct sum (disjoint union): get it?

Definition 5.1.0:

Let X and Y be coherent spaces.
The coherent space X&Y is defined as follows:

$$|X\&Y| \stackrel{df}{=} |X|+|Y| = \{0\}\times|X| \cup \{1\}\times|Y|;$$

$$(0,x) \supset (0,x') \ [\mathrm{mod}\ X\&Y] \quad \text{iff} \quad x \supset x' \ [\mathrm{mod}\ X];$$
$$(1,y) \supset (1,y') \ [\mathrm{mod}\ X\&Y] \quad \text{iff} \quad y \supset y' \ [\mathrm{mod}\ Y];$$
$$(0,x) \supset (1,y) \ [\mathrm{mod}\ X\&Y] \quad \text{for all } x \in |X|,\ y \in |Y|.$$

The coherent space $X \oplus Y$ is defined as follows:

$$|X \oplus Y| \stackrel{df}{=} |X|+|Y|;$$

$$
\begin{array}{lll}
(0,x) \frown (0,x') \ [\mathrm{mod}\ X \oplus Y] & \text{iff} & x \frown x' \ [\mathrm{mod}\ X]; \\
(1,y) \frown (1,y') \ [\mathrm{mod}\ X \oplus Y] & \text{iff} & y \frown y' \ [\mathrm{mod}\ Y]; \\
(0,x) \smile (1,y) \ [\mathrm{mod}\ X \oplus Y] & \text{for all} & x \in |X| \text{ and } y \in |Y|.
\end{array}
$$

The operation & puts in <u>all</u> edges $(0,x) \frown (1,y)$ across the divide between $\{0\} \times |X|$ and $\{1\} \times |Y|$, while the $\oplus$ operation leaves $\{0\} \times |X|$ and $\{1\} \times |Y|$ totally disconnected. This accords (roughly) with the intuitive story about & as meaning that both conjuncts are <u>available</u>, and we get to choose which one is realized, while with $\oplus$, the choice is not ours. <u>Choice</u> is involved in both operations because any given node (i,z) in $|X \& Y| = |X \oplus Y|$ must be in exactly one of $\{0\} \times |X|$ and $\{1\} \times |Y|$.

<u>Observation 5.1.1</u>: (Girard, Lafont & Taylor [1989])

For all objects $c \in X \& Y$, there are unique $a \in X$ and $b \in Y$ such that $c = \{0\} \times a \cup \{1\} \times b$; write $c = a + b$ for short.

For all objects $c \in X \oplus Y$, either $c = \{0\} \times a$ for some $a \in X$ or $c = \{1\} \times b$ for some $b \in Y$.

<u>Observation 5.1.2</u> (Girard [1987])

Let X, Y and Z be coherent spaces.

We have the de Morgan <u>identities</u>

$$(X \& Y)^{\perp} = X^{\perp} \oplus Y^{\perp}, \qquad (X \oplus Y)^{\perp} = X^{\perp} \& Y^{\perp},$$

and canonical isomorphisms expressing the commutativity and associativity of & and $\oplus$, and indicating the status of $\top$ and 0 as identies for & and $\oplus$ respectively:

$$X \& Y \approx Y \& X, \qquad X \oplus Y \approx Y \oplus X,$$
$$(X \& Y) \& Z \approx X \& (Y \& Z), \quad (X \oplus Y) \oplus Z \approx X \oplus (Y \oplus Z),$$
$$X \& \top = X, \qquad X \oplus 0 = X.$$

In each case, the canonical isomorphism in question is the most obvious one.

We shall return to & and ⊕ a little later. Our task for the present is an examination of classes of functions on coherent spaces.

<u>Definition 5.1.3</u>
Let X and Y be coherent spaces.
A function $F : X \to Y$ is <u>continuous</u> iff F satisfies the following conditions:

(I) monotonicity: if $a, a' \in X$ and $a \subseteq a'$ then $F(a) \subseteq F(a')$;

(II′) preservation of <u>directed</u> unions (continuity):
if $S \subseteq X$ is directed then $F(\bigcup^{\uparrow} S) = \bigcup^{\uparrow}\{F(a) \mid a \in S\}$.

Note that monotonicity implies that the family $\{F(a) \mid a \in S\}$ in Y is directed if $S \subseteq X$ is directed: if $a \cup b \subseteq c$ then $F(a) \subseteq F(c)$ and $F(b) \subseteq F(c)$ hence $F(a) \cup F(b) \subseteq F(c)$. Recalling our checklist of properties in Observation 5.0.4, the continuity property (II′) above is of course weaker than the preservation of all the unions there are, which was property (II) on that list. The term 'continuity' derives from the theory of domains: when domains are given a topological interpretation, the property of preserving directed unions corresponds to continuity in the topological sense; see Scott [1982]. Scott also uses the term 'approximable' to refer to a class of functions similar to those we call continuous. That term is most appropriate here: recalling that every object $a \in X$ is the directed union of its finite subsets, continuity implies

$$(\text{FIN}) \qquad F(a) = \bigcup^{\uparrow} \{ F(a_0) \mid a_0 \subseteq a \text{ and } a_0 \in X_{fin} \}$$

So continuous functions are completely determined by their values on the <u>finite</u> objects of X. With little work, it can be shown that (FIN) is actually equivalent to the continuity condition (II').

<u>Lemma 5.1.4</u>: (Girard, Lafont and Taylor [1989])
Let $F : X \to Y$ be continuous.
If $a \in X$ and $y \in F(a)$
then there is a <u>minimal</u> finite $a_0 \subseteq a$ such that $y \in F(a_0)$, i.e. a_0 such that if $b \subseteq a_0$ and $y \in F(b)$ then $a_0 = b$.

<u>Proof:</u>
From the equation (FIN), we know that if $y \in F(a)$ then $y \in F(b)$ for some finite $b \subseteq a$. Now consider all the subsets $c \subseteq b$ such that $y \in F(c)$, and pick one of minimal cardinality. ■

The catch is that, when $y \in F(a)$, there may be <u>more than one</u> minimal finite $a_0 \subseteq a$ such that $y \in F(a_0)$. Our aim is to construct a coherent space whose objects are in one-one correspondance with functions $F : X \to Y$ of some type.

Definition 5.1.5:
Let $F: X \to Y$ be continuous.
The trace of F, denoted $Tr(F)$, is defined as follows:

$$Tr(F) \overset{df}{=} \{ (a,y) \in X_{fin} \times |Y| \mid y \in F(a) \text{ and if } b \subseteq a \text{ and } y \in F(b) \text{ then } a = b \}.$$

Observe that $Tr(F)$ is a set $f \subseteq X_{fin} \times |Y|$ with the property that, for all $(a,y), (a',y') \in f$,

(1) if $a = a'$ then $y \frown y' \, [\mathrm{mod}\, Y]$; and

(2) if $a' \subseteq a$ and $y = y'$ then $a = a'$.

Condition (1) just says that if $y \in F(a)$ and $y' \in F(a)$ then $\{y, y'\} \in Y$; this follows because $\{y, y'\} \subseteq F(a)$. Condition (2) is an immediate consequence of the definition of $Tr(F)$.

Now it can be shown that given any set $f \subseteq X_{fin} \times |Y|$ satisfying conditions (1) and (2), we can define a continuous function $F: X \to Y$ by the formula

(APP) $\qquad F(a) = \{ y \in |Y| \mid \exists a_0 \subseteq a \, ((a_0, y) \in f) \}.$

The proof only makes use of condition (1) and the fact that the a_0 in $(a_0, y) \in f$ are finite. Specifically, if $a_0 \in X_{fin}$ and $\{a_i\}_{i \in I}$ is a directed subfamily of X, then if $a_0 \subseteq \bigcup^{\uparrow}_{i \in I} a_i$ then $a_0 \subseteq a_k$ for some $k \in I$. Technically, the objects $a_0 \in X_{fin}$ are the compact elements of a coherent space X.

<u>Lemma 5.1.6:</u>

Let $F: X \to Y$ be continuous.

For each $a \in X$, define

$$G(a) = \{ y \in |Y| \mid \exists a_0 \subseteq a \, ((a_0, y) \in Tr(F)) \}.$$

Then $G(a) = F(a)$ for all $a \in X$.

<u>Proof:</u>

Let $y \in G(a)$. Then there is an $a_0 \subseteq a$ such that $(a_0, y) \in Tr(F)$. Hence $y \in F(a_0)$. Since F is continuous, $F(a) = \bigcup^{\uparrow} \{ F(a_0) \mid a_0 \subseteq a \text{ and } a_0 \in X_{fin} \}$. Hence $y \in F(a)$. Conversely, suppose $y \in F(a)$. Then there is (at least one) minimal $a_1 \subseteq a$ such that $y \in F(a_1)$. Hence $(a_1, y) \in Tr(F)$ and so $y \in G(a)$. ∎

Now we have a one-one correspondance between continuous functions $F: X \to Y$ and subsets $f \subseteq X_{fin} \times |Y|$ satisfying conditions (1) and (2), hence $X_{fin} \times |Y|$ is a good candidate for the domain of the web of the coherent space we're after. However, we still have to ensure that the subsets f are <u>coherent</u> with respect to some coherence relation. Let F be continuous and suppose both $(a, y) \in Tr(F)$ and $(a', y) \in Tr(F)$. So $y \in F(a)$, $y \in F(a')$ and both a and a' are minimal w.r.t. this property. But that is all we know about a and a' — they may be disjoint; their union may or may not be an element of X; we don't know. Basically, we haven't got enough information about the sets $a \in X_{fin}$ to define a coherence relation. To overcome this deficiency, we consider a smaller class of functions. The extra condition we impose, expressing a property called <u>stability</u>, first came to light in Berry [1978] in work on a semantic characterization of sequential algorithms.

Definition 5·1·7:

Let X and Y be coherent spaces.

A continuous function $F: X \to Y$ is called stable iff F satisfies the following condition:

(III′) stability: if $a, a' \in X$ and $a \cup a' \in X$

then $F(a \cap a') = F(a) \cap F(a')$.

The stability condition is a special case of preservation of intersections. By the obvious induction, if $\{a_i\}_{i \in I}$ is any finite linked family in X, and hence $\bigcup_{i \in I} a_i \in X$, then

$$F\left(\bigcap_{i \in I} a_i\right) = \bigcap_{i \in I} F(a_i).$$

In category-theoretic terms, the stability condition says that F preserves the pullback

$$\begin{tikzcd}
& a \cup a' & \\
a \arrow[ur] & & a' \arrow[ul] \\
& a \cap a' \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

where the arrows are inclusions.

Lemma 5·1·8. (Girard, Lafont & Taylor [1989])

Let $F: X \to Y$ be continuous.

Then F is stable

iff for each $a \in X$, if $y \in F(a)$ then there is a unique minimal $a_0 \in X_{fin}$ such that $y \in F(a_0)$; equivalently, $a_0 = \bigcap \{ b \in X \mid b \subseteq a \text{ and } y \in F(b) \}$.

Proof:

Assume $F: X \to Y$ is stable and suppose $y \in F(a)$. By Lemma 5.1.4, there is a minimal finite $a_0 \subseteq a$ such that $y \in F(a_0)$. Now let $b \subseteq a$ be such that $y \in F(b)$. Since $a_0 \cup b \subseteq a$, we have $a_0 \cup b \in X$. Since F is stable, $F(a_0) \cap F(b) = F(a_0 \cap b)$. Hence $y \in F(a_0 \cap b)$. Now since a_0 is minimal, we must have $a_0 = a_0 \cap b$. Hence $a_0 \subseteq b$. Hence

$$a_0 = \bigcap \{ b \in X \mid b \subseteq a \text{ and } y \in F(b) \}.$$

Conversely, suppose $F: X \to Y$ is continuous and for each $a \in X$ with $y \in F(a)$, there is a smallest $a_0 \subseteq a$ such that $y \in F(a_0)$. Let $a, a' \in X$. Then by monotonicity, $F(a \cap a') \subseteq F(a) \cap F(a')$. Suppose now that $a \cup a' \in X$, and let $y \in F(a) \cap F(a')$. By monotonicity, $y \in F(a \cup a')$. Let $a_0 \subseteq a \cup a'$ be such that $y \in F(a_0)$ and

$$a_0 = \bigcap \{ b \in X \mid b \subseteq a \cup a' \text{ and } y \in F(b) \}.$$

Since $y \in F(a)$ and $y \in F(a')$, we have $a_0 \subseteq a$ and $a_0 \subseteq a'$, hence $a_0 \subseteq a \cap a'$. Hence by monotonicity, $y \in F(a \cap a')$. ∎

Exercise 5.1.9:

Prove the following:

If $F: X \to Y$ is stable then

(III″) preservation of intersections of linked subfamilies of X:

if $S \subseteq X$ is linked and non-empty, hence $\bigcup S \in X$ and $\bigcap S \in X$, then $\quad F(\bigcap S) = \bigcap \{ F(a) \mid a \in S \}$.

Hint: the argument above readily generalizes.

Recall our checklist of properties in Observation 5.0.4. Stable functions are (I) monotone, (II') preserve directed unions, and (III") preserve intersections of linked subfamilies. What about properties (IV) and (V) on that list? What do stable functions do with singletons and the empty set? The short answer is almost anything they like. For example, a constant function $F: X \to Y$ defined by $F(a) = b$ for all $a \in X$, where $b \neq \emptyset$, is stable. For each $a \in X$ and $y \in F(a) = b$, we have $y \in F(\emptyset) = b$, hence $\emptyset$ is the smallest $a_0 \subseteq a$ such that $y \in F(a_0)$.

<u>Lemma 5.1.10</u> (Girard, Lafont & Taylor [1989])
Let $F: X \to Y$ be stable
Then the trace of F,

$$Tr(F) = \{ (a, y) \in X_{fin} \times |Y| \mid y \in F(a) \text{ and if } b \subseteq a \text{ and } y \in F(b) \text{ then } a = b \}$$

has the property that, for all $(a, y), (a', y') \in Tr(F)$,

(1) if $a \cup a' \in X$ then $y \frown\!\!\!\!\smile y' \,[\mathrm{mod}\, Y]$; and

(2) if $a \cup a' \in X$ and $y = y'$ then $a = a'$.

<u>Proof</u>:

(1) We have $y \in F(a)$ and $y' \in F(a')$. If $a \cup a' \in X$ then $\{y, y'\} \subseteq F(a \cup a')$ hence $\{y, y'\} \in Y$.

(2) If $a \cup a' \in X$ and $y = y'$ then $y \in F(a \cup a')$. Let a_0 be the smallest subset of $a \cup a'$ such that $y \in F(a_0)$. Then $a_0 \subseteq a$ and $a_0 \subseteq a$. But then by the minimality clause in the definition of $Tr(F)$, $a = a_0 = a'$. ■

Lemma 5.1.11 (Girard, Lafont and Taylor [1989])
Let X and Y be coherent spaces.
If $f \subseteq X_{fin} \times |Y|$ is such that, for all $(a,y),(a',y') \in f$,

(1) if $a \cup a' \in X$ then $y \supset y'$ [mod Y], and

(2) if $a \cup a' \in X$ and $y = y'$ then $a = a'$,

then there is a unique stable function $F : X \to Y$ defined by

$$\text{(APP)} \qquad F(a) = \{ y \in |Y| \mid \exists a_0 \subseteq a ((a_0, y) \in f) \}.$$

Proof:

First, we verify that F is a function from X into Y; to show $F(a) \in Y$, we must check that $F(a)$ is a coherent subset of $|Y|$. Let $y_0, y_1 \in F(a)$. Then there are $a_0 \subseteq a$ and $a_1 \subseteq a$ such that $(a_0, y_0) \in f$ and $(a_1, y_1) \in f$. But then $a_0 \cup a_1 \subseteq a$, so by (1) above, $y_0 \supset y_1$ [mod Y].

Now we have to show that F is stable.
(i) monotonicity: if $a \subseteq a'$ then clearly $F(a) \subseteq F(a')$.
(ii) Continuity. Let $\{a_i\}_{i \in I}$ be a directed subfamily of X. Put $a = \bigcup^{\uparrow}_{i \in I} a_i$, so $a \in X$. Since $a_i \subseteq a$ for each $i \in I$, we have $\bigcup^{\uparrow}_{i \in I} F(a_i) \subseteq F(a)$ by monotonicity. Conversely, if $y \in F(a)$ then there is a finite $a_0 \subseteq a$ such that $(a_0, y) \in f$, hence $y \in F(a_0)$. Now $a_0 \subseteq \bigcup^{\uparrow}_{i \in I} a_i$, hence $a_0 \subseteq a_k$ for some $k \in I$ since the family $\{a_i\}_{i \in I}$ is directed. By monotonicity, $F(a_0) \subseteq F(a_k)$, hence $y \in \bigcup^{\uparrow}_{i \in I} F(a_i)$.

(iii) stability. Suppose $a \cup a' \in X$. Then $F(a \cap a') \subseteq F(a) \cap F(a')$ by monotonicity. Let $y \in F(a) \cap F(a')$. Then there are finite $a_0 \subseteq a$ and $a_1 \subseteq a'$ such that $(a_0, y) \in f$ and $(a_1, y) \in f$. Now $a_0 \cup a_1 \subseteq a \cup a'$ hence $a_0 \cup a_1 \in X$. So by condition (2), $a_0 = a_1$. We have $y \in F(a_0)$ and $a_0 \subseteq a \cap a'$, hence by monotonicity, $y \in F(a \cap a')$.

Since stable functions are continuous, uniqueness comes from Lemma 5.1.6. ■

<u>Definition 5.1.12</u>:
Let X and Y be coherent spaces.
The coherent space $X \Rightarrow Y$ is defined as follows:

$$|X \Rightarrow Y| \stackrel{\text{def}}{=} X_{fin} \times |Y|;$$

$$(a, y) \frown\!\!\!\!\smile (a', y') \ [\text{mod } X \Rightarrow Y]$$

iff (1) if $a \cup a' \in X$ then $y \frown\!\!\!\!\smile y' \ [\text{mod } Y]$; and
(2) if $a \cup a' \in X$ and $y = y'$ then $a = a'$.

<u>Theorem 5.1.13</u>: (Girard, Lafont & Taylor [1989])
Let X and Y be coherent spaces.
Then
$$X \Rightarrow Y = \{ Tr(F) \mid F : X \to Y \text{ is stable} \}.$$

<u>Proof:</u>
By Lemmas 5.1.10 and 5.1.11. ■

The intention is that encoding a stable function by its trace corresponds to λ-abstraction and the formula (APP) defines the application of a function. Verification that the coherent semantics developed thus far is sufficient to interpret the positive $\{\Rightarrow, \wedge, t\}$ fragment of intuitionistic propositional calculus, and hence gives a model of typed λ-calculus, comes from the following result.

<u>Theorem 5.1.14</u>: (Lafont [1988a])
The category **St**. of coherent spaces, with stable functions as its morphisms, is cartesian closed.

<u>Outline of proof</u>:
We will not give all the gory details.

Clearly, T is the terminal object in **St**. For each X, there is only one map $F: X \to T$, given by $F(a) = \emptyset$ for all $a \in X$, and this F is stable.

To ensure that $\&$ is a product, we need projections. Define $P_0 : X \& Y \to X$ by $P_0(\{0\} \times a \cup \{1\} \times b) = a$, and $P_1 : X \& Y \to Y$ by $P_1(\{0\} \times a \cup \{1\} \times b) = b$. (Recall that each object $c \in X \& Y$ admits a unique decomposition.) By mere inspection, P_0 and P_1 are stable functions.

Now let $G_0 : Z \to X$ and $G_1 : Z \to Y$ be stable functions. We claim there is a unique stable function $F: Z \to X \& Y$ such that the following diagram commutes.

$$\begin{tikzcd} & Z \arrow[dl, "G_0"'] \arrow[d, dashed, "F"] \arrow[dr, "G_1"] & \\ X & X \& Y \arrow[l, "P_0"] \arrow[r, "P_1"'] & Y \end{tikzcd}$$

We define a set $f \subseteq Z_{fin} \times |X \& Y|$ by

$$f = \{ (c,(0,x)) \mid (c,x) \in Tr(G_0) \} \cup \{ (c,(1,y)) \mid (c,y) \in Tr(G_1) \}$$

We write $(i,w) \in |X \& Y|$, i.e. $i \in \{0,1\}$ and $w \in |X| \cup |Y|$.
Let $(c,(i,w)), (c',(i',w')) \in f$.

(1) Suppose $c \cup c' \in Z$. If $i = i'$ then $(c,w), (c',w') \in Tr(G_i)$ and hence $(i,w) \frown\!\!\smile (i,w')$ [mod $X\&Y$]. If $i \neq i'$ then we have $(i,w) \frown\!\!\smile (i',w')$ [mod $X\&Y$] automatically.

(2) Suppose $c \cup c' \in Z$ and $(i,w) = (i',w')$. Then $(c,w), (c',w) \in Tr(G_i)$ and hence $c = c'$.

Hence f is the trace of the stable function $F : Z \to X\&Y$ such that the diagram in question commutes.

By Theorem 5.1.13, the map

$$Tr : \quad Hom_{st}(X,Y) \longrightarrow (X \Rightarrow Y)$$

is a bijection. By putting a suitable ordering on $Hom_{st}(X,Y)$ (see Lafont [1988a], Exercise 6) it can be shown that Tr is an isomorphism between $Hom_{st}(X,Y)$ and $X \Rightarrow Y$ considered as partial orders. So $\Rightarrow$ is the internal hom on **St**. To establish closure, we have to exhibit a bijection

$$Hom_{st}(X\&Y, Z) \cong Hom_{st}(X, Y \Rightarrow Z)$$

natural in X and Z. A canonical isomorphism

$$(X\&Y) \Rightarrow Z \approx X \Rightarrow (Y \Rightarrow Z)$$

will suffice.

$$|(X \& Y) \Rightarrow Z| = (X \& Y)_{fin} \times |Z|.$$

Note that $c \in (X\&Y)_{fin}$ iff $c = \{0\} \times a \cup \{1\} \times b$ for some (uniquely determined) $a \in X_{fin}$ and $b \in Y_{fin}$.

$$|X \Rightarrow (Y \Rightarrow Z)| = X_{fin} \times |Y \Rightarrow Z| = X_{fin} \times (Y_{fin} \times |Z|).$$

It is readily verified that the map

$$(c, z) \longmapsto (a, (b, z))$$

is a graph isomorphism and hence induces the required canonical isomorphism of coherent spaces. ■

It can be shown that the category **Cont** of coherent spaces with continuous functions as its morphisms is <u>not</u> cartesian closed. One supposes that there is an 'exponential' coherent space Y^X such that

$$\mathrm{Hom}_{\mathbf{cont}}(X, Y) \cong Y^X$$

and derives a contradiction. A sketch of the proof is given in Lafont [1988a], (Exercise 2).

Note that the additive conjunction $\oplus$ is <u>not</u> a co-product on **St**. The injections $J_0 : X \to X \oplus Y$ and $J_1 : Y \to X \oplus Y$ defined by $J_0(a) = \{0\} \times a$ and $J_1(b) = \{1\} \times b$ are stable, and every object $c \in X \oplus Y$ can be written as $J_0(a)$ for some $a \in X$ or $J_1(b)$ for some $b \in Y$. The expression is unique, <u>except</u> in the case of $\emptyset$; we have $\emptyset = J_0(\emptyset) = J_1(\emptyset)$. This makes it impossible to define a function $F : X \oplus Y \to Z$ case-wise by

$$F(J_0(a)) = G_0(a), \quad F(J_1(b)) = G_1(b)$$

from two stable functions $G_0 : X \to Z$ and $G_1 : Y \to Z$. The problem is that $G_0(\emptyset)$ has no good reason to be equal to $G_1(\emptyset)$; see Girard, Lafont and Taylor [1989], Chapter 12.

5·2 Linearization: decomposing intuitionistic implication

We have the coherent space $X \Rightarrow Y$, where

$|X \Rightarrow Y| \overset{df}{=} X_{fin} \times |Y|$, and

$(a, y) \supset (a', y')$ [mod $X \Rightarrow Y$]

iff (1) if $a \cup a' \in X$ then $y \supset y'$ [mod Y]; and

(2) if $a \cup a' \in X$ and $y = y'$ then $a = a'$.

Such a coherent space <u>begs</u> to be decomposed into simpler parts. Girard called coherent space semantics 'disturbing'; the disturbance comes from the realization that intuitionistic implication is not primitive.

<u>Definition 5·2·0</u>:
Let X be a coherent space.
The coherent space $!X$ is defined as follows:

$|!X| \overset{df}{=} X_{fin}$ and $a \supset a'$ [mod $!X$] iff $a \cup a' \in X$.

<u>Definition 5·2·1</u>:
Let X and Y be coherent spaces.
The coherent space $X \multimap Y$ is defined as follows:

$|X \multimap Y| \overset{df}{=} |X| \times |Y|$,

$(x,y) \supset (x',y')$ [mod $X \multimap Y$]

iff (1) if $x \supset x'$ [mod X] then $y \supset y'$ [mod Y];

(2) if $x \supset x'$ [mod X] and $y = y'$ then $x = x'$.

In the presence of (1), (2) is equivalent to

(2') if $x \frown x'$ [mod X] then $y \frown y'$ [mod Y].

Evidently, $X \Rightarrow Y = \,!X \multimap Y$.

<u>Exercise 5.2.2:</u>

Fill in the blank:

Stable functions are to '$\Rightarrow$' as ______ functions are to '$\multimap$'.

<u>Definition 5.2.3:</u>

Let X and Y be coherent spaces.

A stable function $F : X \to Y$ is called <u>linear</u> iff F satisfies the following condition:

(II) linearity: if $S \subseteq X$ is linked then $F(\bigcup S) = \bigcup\{F(a) \mid a \in S\}$.

So linear functions preserve all the unions there are. By taking $S = \emptyset$ in (II), we get (V'): $F(\emptyset) = \emptyset$. Note that there is nothing to rule out $F(a) = \emptyset$ where $a \neq \emptyset$ (eg. the maps $F : X \to T$) so (V') is weaker than (V) in 5.0.4. The linearity condition (II) implies continuity (II') and monotonicity (I), so in view of our earlier discussion (Exercise 5.1.9), we have the following equivalence:

$F : X \to Y$ is linear

iff for all linked subfamilies $S \subseteq X$,

(II) $F(\bigcup S) = \bigcup\{F(a) \mid a \in S\}$, and

(III'') $F(\bigcap S) = \bigcap\{F(a) \mid a \in S\}$, provided S is non-empty.

Lemma 5·2·4: (Girard, Lafont and Taylor [1989])
Let $F: X \to Y$ be stable.

F is linear

iff $Tr(F) = \{ (\{x\}, y) \in X_{fin} \times |Y| \mid y \in F(\{x\}) \}$

Proof:
Suppose $F: X \to Y$ is linear and for some $y \in |Y|$, $(a, y) \in Tr(F)$ but a is not a singleton. Suppose $a = \emptyset$. then $y \in F(\emptyset) \neq \emptyset$, contradicting linearity. So assume $a \neq \emptyset$. then for any a' such that $\emptyset \subseteq a' \subseteq a$ with $a' \neq \emptyset$ and $a' \neq a$, we must have $y \notin F(a')$, since a' is minimal. Now $a \cup a' = a$ so $a \cup a' \in X$. Hence we have $F(a \cup a') = F(a) \neq F(a) \cup F(a')$, contradicting linearity.

Conversely, suppose $F: X \to Y$ is stable and $Tr(F) = \{ (\{x\}, y) \in X_{fin} \times |Y| \mid y \in F(\{x\}) \}$. Let $S \subseteq X$ be any linked subfamily. By monotonicity, we have $\bigcup \{ F(a) \mid a \in S \} \subseteq F(\bigcup S)$. Let $y \in F(\bigcup S)$. then there is a unique $x \in \bigcup S$ such that $y \in F(\{x\})$. Now $x \in a$ for some $a \in S$, hence $y \in F(a) \subseteq \bigcup \{ F(a) \mid a \in S \}$. ∎

Now if we know that a function F is linear, we can safely discard the singleton symbols in $Tr(F)$.

Definition 5·2·5:
Let $F: X \to Y$ be linear.
The linear trace of F, denoted $Trlin(F)$, is defined as follows:

$$Trlin(F) \stackrel{df}{=} \{ (x, y) \in |X| \times |Y| \mid y \in F(\{x\}) \}$$

Lemma 5·2·6: (Girard, Lafont & Taylor [1989])
Let $F: X \to Y$ be linear.
Then $Trlin(F)$ has the property that, for all $(x,y), (x',y') \in Trlin(F)$,

(1) if $x \frown x'$ [mod X] then $y \frown y'$ [mod Y], and
(2) if $x \frown x'$ [mod X] and $y = y'$ then $x = x'$.

Proof:
Recalling that $\{x\} \cup \{x'\} = \{x, x'\} \in X$ iff $x \frown x'$ [mod X], the result follows immediately from Lemma 5·1·10. ∎

Lemma 5·2·7: (Girard, Lafont & Taylor [1989])
Let X and Y be coherent spaces.
If $f \subseteq |X| \times |Y|$ is such that for all $(x,y), (x',y') \in f$,

(1) if $x \frown x'$ [mod X] then $y \frown y'$ [mod Y], and
(2) if $x \frown x'$ [mod X] and $y = y'$ then $x = x'$,

then there is a unique linear function $F: X \to Y$ defined by

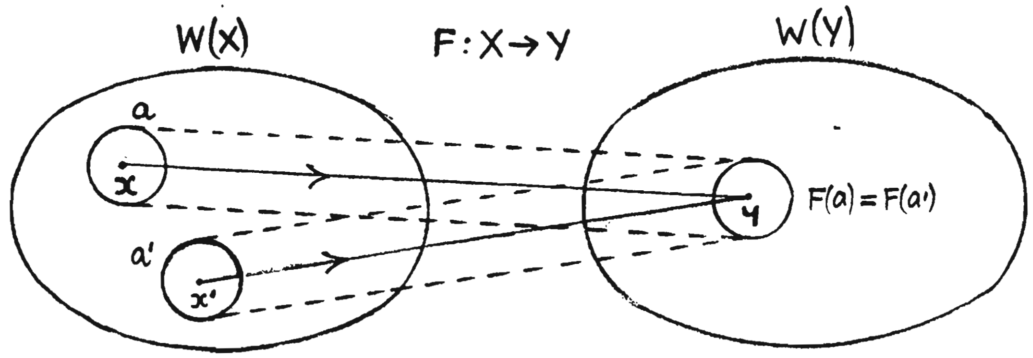
(LIN-APP) $\qquad F(a) = \{ y \in |Y| \mid \exists x \in a ((x,y) \in f) \}$

Proof:
Analogous to the proof of Lemma 5·1·11. The only extra item to check is the linearity condition. Let $S \subseteq X$ be linked. We have $\bigcup \{ F(a) \mid a \in S \} \subseteq F(\bigcup S)$ by the monotonicity of F. Let $y \in F(\bigcup S)$. Then there is an $x \in \bigcup S$ such that $(x,y) \in f$. Hence $y \in F(\{x\})$. Now $x \in a$ for some $a \in S$, hence $y \in F(a) \subseteq \bigcup \{ F(a) \mid a \in S \}$. ∎

Theorem 5.2.8: (Girard, Lafont and Taylor [1989])
Let X and Y be coherent spaces.
Then
$$X \multimap Y = \{ \mathrm{Trlin}(F) \mid F : X \to Y \text{ is linear} \}.$$

Proof: by Lemmas 5.2.6 and 5.2.7. ∎

When $F : X \to Y$ is linear then, given $a \in X$ and $y \in F(a)$, there is a unique $x \in a$ such that $y \in F(\{x\})$. Note, however, that linear functions need not preserve singletons: we can have $y \in F(\{x\})$ and $y' \in F(\{x\})$, provided $y \frown y'$ [mod Y] (condition (1)). So linear functions do not in general give rise to graph homomorphisms on the webs.
Condition (2) is like a local injectivity property: if $y \in F(\{x\})$ and $y \in F(\{x'\})$ and $x \neq x'$ then $x \smile x'$ [mod X].



Lemma 5.2.9: (Girard [1987])
Let X and Y be coherent spaces.
We have the following canonical isomorphisms:

$$X \multimap Y \approx Y^{\perp} \multimap X^{\perp},$$
$$\mathbb{1} \multimap X \approx X, \qquad X \multimap \perp \approx X^{\perp}.$$

Proof:

(i) The map $(x,y) \mapsto (y,x)$ gives a graph isomorphism $W(X \multimap Y) \cong W(Y^{\perp} \multimap X^{\perp})$.

(ii) The maps $(@,x) \mapsto x$ and $(x,@) \mapsto x$ give graph isomorphisms $W(\mathbb{1} \multimap X) \cong W(X)$ and $W(X \multimap \perp) \cong W(X^{\perp})$ respectively; explicitly

$$(@,x) \frown\!\!\!\smile (@,x') \; [\text{mod } \mathbb{1} \multimap X]$$

iff (1) if $@ \frown\!\!\!\smile @ \; [\text{mod } \mathbb{1}]$ then $x \frown\!\!\!\smile x' \; [\text{mod } X]$, and

(2) if $x \asymp x' \; [\text{mod } X]$ then $@ \asymp @ \; [\text{mod } \mathbb{1}]$,

iff $\quad x \frown\!\!\!\smile x' \; [\text{mod } X]$. ∎

Recall the other component of intuitionistic implication decomposed: coherence spaces $!X$ where $|!X| \stackrel{df}{=} X_{fin}$ and $a \frown\!\!\!\smile a' \; [\text{mod } !X]$ iff $a \cup a' \in X$. The objects of $!X$ are <u>linked</u> subfamilies $S \subseteq X_{fin}$, i.e. for all $a, a' \in S$, $a \cup a' \in X$. For each object $a \in X$, define

$$!a \stackrel{df}{=} \{ a_0 \in X_{fin} \mid a_0 \subseteq a \}.$$

So $!a \in !X$. This construction defines a function $F: X \to !X$ given by $F(a) = !a$. Note that F is stable, but <u>not</u> linear; a quick computation reveals that $Tr(F) = \{ (a_0, a_0) \mid a_0 \in X_{fin} \}$.

We have a general procedure for turning stable functions into linear ones, and vice-versa.

<u>Lemma 5.2.10</u>: (Girard, Lafont & Taylor [1989])
If $F: X \to Y$ is stable
then there is a unique linear function $Lin(F): !X \to Y$ defined by the equation $Trlin(Lin(F)) = Tr(F)$.

Proof:

We show that $\mathrm{Lin}(F)(!a) = F(a)$.

Let $y \in F(a)$. Then there is a unique finite $a_0 \subseteq a$ such that $(a_0, y) \in Tr(F) = Trlin(\mathrm{Lin}(F))$. Hence $y \in \mathrm{Lin}(F)(\{a_0\})$. Since $\{a_0\} \subseteq\ !a$, we have $y \in \mathrm{Lin}(F)(!a)$ by monotonicity. The argument that $y \in \mathrm{Lin}(F)(!a)$ implies $y \in F(a)$ is similar. ■

Corollary 5.2.11: (Girard, Lafont & Taylor [1989])

If $G : !X \to Y$ is linear

then there is a unique stable function $\mathrm{Delin}(G) : X \to Y$

defined by $\mathrm{Delin}(G)(a) = G(!a)$ and

satisfying the equation $Tr(\mathrm{Delin}(G)) = Trlin(G)$.

Proof:

The operations Lin and Delin are mutual inverses. ■

Let **Lin** denote the category of coherent spaces with linear functions as its morphisms. Technically, the previous two results say that the functor $! : \mathbf{Lin} \to \mathbf{Lin}$ is the left adjoint to the forgetful functor from **Lin** into **St**. Moreover, ! is a comonad (or cotriple): there are families of linear functions $E_X : !X \to X$ and $D_X : !X \to !!X$ that do the sorts of things they are supposed to do. The functor ! has other pleasant properties which we'll say a little more about later.

Of course, there is the dual of ! : the functor ? is defined so as to ensure that we have identities

$$(!X)^{\perp} = ?X^{\perp} \quad \text{and} \quad (?X)^{\perp} = !X^{\perp}.$$

Definition 5.2.11:
Let X be a coherent space.
The coherent spaces $!X$ and $?X$ are defined as follows:

$$|!X| \stackrel{\text{df}}{=} X_{fin} \quad \text{and} \quad a \frown a' \,[\text{mod}\, !X] \text{ iff } a \cup a' \in X$$
$$|?X| \stackrel{\text{df}}{=} (X^{\perp})_{fin} \quad \text{and} \quad a \frown a' \,[\text{mod}\, ?X] \text{ iff } a \cup a' \notin X^{\perp}$$

(The definition of $!X$ is repeated for comparison purposes.)

Observe that $a \supset a' \,[\text{mod}\,(?X)^{\perp}]$ iff $a \asymp a' \,[\text{mod}\, ?X]$ iff $a \cup a' \in X^{\perp}$ iff $a \supset a' \,[\text{mod}\, !X^{\perp}]$. Similar computations confirm the other de Morgan identity.

Fact 5.2.12: (Lafont [1988a])
The category **Lin** is Cartesian and co-cartesian. The product is $\&$, as in **St**; the projections P_0 and P_1 are linear. The co-product is $\oplus$; the problem which prevents $\oplus$ being a co-product in **St** is now fixed because $G(\emptyset) = \emptyset$ for all linear functions G. $\mathbf{Emp} = \mathbf{T} = \mathbf{0}$ is both terminal and initial.

Using the co-product $\oplus$ in **Lin**, we can define a co-product structure on the category **St** by performing a 'linearization'. For coherent spaces X and Y, define

$$X \vee Y \stackrel{\text{df}}{=} !X \oplus !Y$$

So $|X \vee Y| = \{0\} \times X_{fin} \cup \{1\} \times Y_{fin}$ and

$(0, a) \supset (0, a') \,[\text{mod}\, X \vee Y]$ iff $a \cup a' \in X$,
$(1, b) \supset (1, b') \,[\text{mod}\, X \vee Y]$ iff $b \cup b' \in Y$, and
$(0, a) \smile (1, b) \,[\text{mod}\, X \vee Y]$ for all $a \in X_{fin}$ and $b \in Y_{fin}$.

The injections $K_0 : X \to X \vee Y$ and $K_1 : Y \to X \vee Y$ given by $K_0(a) = \{0\} \times !a$ and $K_1(b) = \{1\} \times !b$ are stable. Given stable functions $G_0 : X \to Z$ and $G_1 : Y \to Z$, we can define $F : X \vee Y \to Z$ casewise:

for $S \in !X$, $\quad F(\{0\} \times S) = Lin(G_0)(S)$, and
for $T \in !Y$, $\quad F(\{1\} \times T) = Lin(G_1)(T)$.

In particular, $\quad F(\emptyset) = Lin(G_0)(\emptyset) = Lin(G_1)(\emptyset) = \emptyset$

F is linear, and hence stable. And finally, the initial object in **St** is $\mathbb{O} = \mathbf{Emp}$, as in **Lin**.

<u>Fact 5.2.13:</u> (Lafont [1988a])

$$Trlin : Hom_{\mathbf{Lin}}(X, Y) \xrightarrow{\cong} (X \multimap Y)$$

By Theorem 5.2.8, we know that Trlin is a bijection; the verification that it is an isomorphism of partial orders is similar to that required for $\Rightarrow$.

The category **Lin** is not, however, Cartesian <u>closed</u>; we <u>don't</u> have

$$(X \& Y) \multimap Z \approx X \multimap (Y \multimap Z)$$

What closure there is, is with respect to the <u>monoidal</u> structure on **Lin**.

<u>Definition 5.2.14:</u>

Let X and Y be coherent spaces.
The coherent spaces $X \otimes Y$ and $X \wp Y$ are as follows:

$|X \otimes Y| \stackrel{df}{=} |X \wp Y| \stackrel{df}{=} |X| \times |Y|$;

$(x, y) \coh (x', y')$ [mod $X \otimes Y$] iff $x \coh x'$ [mod X] and $y \coh y'$ [mod Y];

$(x, y) \frown (x', y')$ [mod $X \wp Y$] iff $x \frown x'$ [mod X] or $y \frown y'$ [mod Y].

<u>Fact 5.2.15</u>: (Lafont [1988a])

The operation $\otimes$ defines on **Lin** the structure of a <u>symmetric monoidal category</u>, with $\mathbb{1}$ as the unit.

What this means is that $\otimes$ is a bifunctor and there are canonical (natural) isomorphisms

$$X\otimes \mathbb{1} \approx X \quad X\otimes Y \approx Y\otimes X \quad (X\otimes Y)\otimes Z \approx X\otimes(Y\otimes Z).$$

satisfying the Mac Lane - Kelly equations (see Mac Lane [1971]).

<u>Fact 5.2.16</u>: (Lafont [1988a])

The category **Lin** is a <u>closed</u> symmetric monoidal category; i.e. their is a natural bijection

$$\mathrm{Hom}_{\mathbf{Lin}}(X\otimes Y, Z) \cong \mathrm{Hom}_{\mathbf{Lin}}(X, Y \multimap Z);$$

Which means

$$(X\otimes Y)\multimap Z \approx X\multimap(Y\multimap Z).$$

<u>Fact 5.2.17</u>: (Seely [1989])

The category **Lin** is a <u>$*$-autonomous category</u> (in the sense of Barr [1979]), which means it is a closed symmetric monoidal category together with an <u>involution</u> $(-)^{\perp}: \mathbf{Lin}^{op} \to \mathbf{Lin}$, isomorphisms $X\multimap Y \to Y^{\perp}\multimap X^{\perp}$ and isomorphisms $X \to X^{\perp\perp}$.

Following Seely [1989], we have

<u>Definition 5.2.18</u>:

A <u>linear category</u> is a $*$-autonomous category with finite products.

Note that if a $*$-autonomous category has a product then it has a coproduct by de Morgan duality.

Not unexpectedly, **Lin** is a linear category. The category $\mathbf{Vect}_K$ of finite dimensional vector spaces over a field K, with linear maps as its morphisms, is also a linear category. The duality operator $(-)^*$ is the involution, the monoidal structure is given by the tensor product $\otimes$ and the coproduct is the direct sum $\oplus$. Unfortunately, $\mathbf{Vect}_K$ is not a terribly good categorical model of propositional linear logic: in $\mathbf{Vect}_K$ we have

$$(V \oplus W)^* \cong V^* \oplus W^* \qquad (V \otimes W)^* \cong V^* \otimes W^*.$$

So in $\mathbf{Vect}_K$, $\oplus$ and $\&$ are collapsed into one, and likewise for $\otimes$ and $⅋$. Recent work by Lafont, cited in Martí-Oliet and Meseguer [1989], seeks to generalize the category $\mathbf{Vect}_K$. Lafont defines a category $\mathbf{Games}_K$, for any set K, and shows that **Lin** is isomorphic to a full subcategory of $\mathbf{Games}_{\{0,1\}}$.

Fact 5·2·19: (Seely [1989])
The category **Lin** together with the comonad $! : \mathbf{Lin} \to \mathbf{Lin}$ is such that

(i) for each X of **Lin**, $!X$ is a comonoid with respect to the monoidal structure;

(ii) there are natural isomorphisms $!X \otimes !Y \approx !(X \& Y)$ and $\mathbb{1} \approx !T$, and all the appropriate diagrams commute.

Following Seely [1989], any linear category with a comonad satisfying (i) and (ii) above (with the details suitably filled in) is called a <u>Girard category</u>.

Seely takes the (catagorical) essence of Girard's translation of intuitionistic logic into linear logic to be the following

<u>Proposition 5.2.20</u>: (Seely [1989])
If G,! is a Girard category then the Kleisli category K(G) with respect to ! is Cartesian closed. ∎

In particular, **St** is the Kleisli category of **Lin,!**. Seely notes that in general, K(G) does not have co-products. **St** is a special case because **Lin** is a subcategory of **St**.

A much more detailed discussion of the categorical interpretation of linear logic is to be found in Seely [1989]. See also Marti-Oliet and Meseguer [1989] and Lafont [1988a].

The general procedure in categorical logic is to associate, under the Lambek-Lawvere correspondance, morphisms of the category in question with equivalence classes of proofs in a given logical system, the equivalence classes being given by the defining equations of the category. In the case of linear categories, a rather long list of equations is required: see Seely [1989] and Marti-Oliet and Meseguer [1989];

a presentation in terms of categorical combinators is given in Lafont [1988b].

Girard takes a different course. In the next sub-section we see a direct construction of a semantic object for each proof in the sequent calculus **LL!**. The equivalence classes of proofs determined by this construction are of importance in the normalization (cut-elimination) process for the system of proof nets dealt with in Section 6.

5.3 Proofs as objects in coherent spaces.

Fix a countable collection of coherent spaces (excluding Sgl and Emp) and a bijective mapping of that collection onto the set of propositional letters of $\mathcal{L}_!$, the language of modal linear logic. Assign the coherent space Sgl to both the constants $\mathbb{1}$ and $\perp$, and the coherent space Emp to $\top$ and $\mathbb{0}$. The duals of propositional letters and all compound formulae built from $\otimes$, $⅋$, $\&$, $\oplus$, ! and ? will have assigned to them the appropriate coherent space formed from the semantic operations $(-)^\perp$, $\otimes$, $⅋$, $\&$, $\oplus$, ! and ?. Henceforth, we identify each formula of $\mathcal{L}_!$ with its coherent space.

If Δ is a sequence of formulae $A_1,\ldots,A_n$ then $\Delta = A_1 ⅋ \ldots ⅋ A_n$ as a coherent space. Hence

$$|\Delta| = |A_1| \times \ldots \times |A_n|.$$

We write $\underset{\sim}{z} \in |\Delta|$ where $\underset{\sim}{z} = (z_1, \ldots, z_n)$ and $z_i \in |A_i|$ for $i = 1, \ldots, n$. From the definition of the operation $⅋$ on coherent spaces (Definition 5·2·14), we have

$$\underset{\sim}{z} \frown \underset{\sim}{z}' \ [\mathrm{mod}\ \Delta] \quad \text{iff} \quad z_i \frown z_i' \ [\mathrm{mod}\ A_i] \quad \text{for some } i \in \{1, \ldots, n\},$$

and $\underset{\sim}{z} \supset \underset{\sim}{z}' \ [\mathrm{mod}\ \Delta]$ iff $\underset{\sim}{z} = \underset{\sim}{z}'$ or $\underset{\sim}{z} \frown \underset{\sim}{z}' \ [\mathrm{mod}\ \Delta]$.

We shall define by induction a (unique) object $\pi^* \in \Delta$ for each proof π in **LL!** of $\vdash \Delta$. That π^* <u>represents</u> the proof π should become clear from the construction. As an example, we'll be able to show that

if π_0 is a proof of $\vdash A$,
π_1 is a proof of $\vdash A \multimap B$ (i.e. $\vdash A^\perp ⅋ B$),
and $\pi_1^* = \mathrm{Trlin}(F)$ where $F : A \to B$ is linear
then $F(\pi_0^*) = \pi^*$ where π is the proof obtained from π_0 and π_1 by applying (CUT).

<u>Theorem 5·3·0</u>: (Girard [1987])
If π is a proof of $\vdash \Delta$ in **LL!**
then there is a unique object $\pi^* \in \Delta$ which represents π.

<u>Proof</u>:
The object π^* is defined by induction on the proof π of $\vdash \Delta$. In each case, it will be obvious that $\pi^* \subseteq |\Delta|$; what has to be verified is that for all $\underset{\sim}{z} \in \pi^*$ and $\underset{\sim}{z}' \in \pi^*$, $\underset{\sim}{z} \supset \underset{\sim}{z}' \ [\mathrm{mod}\ \Delta]$. We use commas to denote the concatenation of sequences and omit

outermost parentheses where appropriate.

(i) π is an instance of the identity axiom scheme, say
$\vdash A, A^{\perp}$.
Define $\pi^* \stackrel{\mathrm{df}}{=} \{(x,x) \mid x \in |A|\}$.
Recall that for all $x \in |A|$ and $x' \in |A|$ with $x \neq x'$, we have either $x \frown x'$ [mod A] or $x \frown x'$ [mod $A^{\perp}$].
Hence for all (x,x) and $(x',x') \in \pi^*$, $(x,x) \supset (x',x')$ [mod $A \otimes A^{\perp}$].

(ii) π is obtained from π_0 by an application of (EXCH):

$$\frac{\vdash \Gamma}{\vdash \sigma(\Gamma)}\ (\mathrm{EXCH})$$

where σ is a permutation of Γ.
Define $\pi^* \stackrel{\mathrm{df}}{=} \{\sigma(\underset{\sim}{z}) \mid \underset{\sim}{z} \in \pi_0^*\}$.
Assuming π_0^* is coherent, so is π^*.

<u>The additives:</u>

(iii) π is an instance of the axiom scheme for T, say
$\vdash T, \Gamma$.
Define $\pi^* \stackrel{\mathrm{df}}{=} \emptyset$, since $|T| \times |\Gamma| = \emptyset \times |\Gamma| = \emptyset$.

(iv) π is obtained from π_0 and π_1 by the rule (&):

$$\frac{\vdash A, \Gamma \qquad \vdash B, \Gamma}{\vdash A \& B, \Gamma}\ (\&)$$

Define $\pi^* \stackrel{\mathrm{df}}{=} \{(0,x), \underset{\sim}{z_0} \mid x, \underset{\sim}{z_0} \in \pi_0^*\} \cup \{(1,y), \underset{\sim}{z_1} \mid y, \underset{\sim}{z_1} \in \pi_1^*\}$.

Now $(0,x), \underset{\sim}{z_0} \supset (0,x'), \underset{\sim}{z_0'}$ [mod $A \& B, \Gamma$] since by hypothesis, we have $x, \underset{\sim}{z_0} \supset x', \underset{\sim}{z_0'}$ [mod A, Γ]; likewise for pairs of elements of π^* obtained from π_1^*. Since $(0,x) \frown (1,y)$ [mod $A \& B$] for all $x \in |A|$ and $y \in |B|$, we have $(0,x), \underset{\sim}{z_0} \frown (1,y), \underset{\sim}{z_1}$ [mod $A \& B, \Gamma$].

(v) π is obtained from π_0 by the rule (FST$\oplus$):

$$\frac{\vdash A, \Gamma}{\vdash A \oplus B, \Gamma}\ (\mathrm{FST}\oplus)$$

Define $\pi^* \overset{\mathrm{df}}{=} \{ (0,x), \underset{\sim}{z} \mid x, \underset{\sim}{z} \in \pi_0^* \}$.
The coherence of π^* follows immediately from the coherence of π_0^*.

(vi) π is obtained from π_1 by the rule (SND$\oplus$):

$$\frac{\vdash B, \Gamma}{\vdash A \oplus B, \Gamma}\ (\mathrm{SND}\oplus)$$

Define $\pi^* \overset{\mathrm{df}}{=} \{ (1,y), \underset{\sim}{z} \mid y, \underset{\sim}{z} \in \pi_1^* \}$.

<u>The multiplicatives:</u>

(vii) π is the axiom $\vdash \mathbb{1}$.
Define $\pi^* \overset{\mathrm{df}}{=} \{@\}$.

(viii) π is obtained from π_0 by the rule ($\perp$):

$$\frac{\vdash \Gamma}{\vdash \perp, \Gamma}\ (\perp)$$

Define $\pi^* \overset{\mathrm{df}}{=} \{ @, \underset{\sim}{z} \mid \underset{\sim}{z} \in \pi_0^* \}$.

(ix) π is obtained from π_0 and π_1 by the rule ($\otimes$):

$$\frac{\vdash A, \Gamma_0 \qquad\qquad \vdash B, \Gamma_1}{\vdash A \otimes B, \Gamma_0, \Gamma_1}\ (\otimes)$$

Define $\pi^* \overset{\mathrm{df}}{=} \{ (x,y), \underset{\sim}{z_0}, \underset{\sim}{z_1} \mid x, \underset{\sim}{z_0} \in \pi_0^* \text{ and } y, \underset{\sim}{z_1} \in \pi_1^* \}$

Let $\underset{\sim}{w} = (x,y), \underset{\sim}{z_0}, \underset{\sim}{z_1}$ and $\underset{\sim}{w'} = (x',y'), \underset{\sim}{z_0'}, \underset{\sim}{z_1'}$.
By hypothesis, we have $\quad x, \underset{\sim}{z_0} \supset x', \underset{\sim}{z_0'}$ [mod A, Γ]
and $\quad y, \underset{\sim}{z_1} \supset y', \underset{\sim}{z_1'}$ [mod B, Γ].
Let Δ be an abbreviation for $A \otimes B, \Gamma_0, \Gamma_1$.

We argue by cases.

Case(1): $x, \underset{\sim}{z_0} = x', \underset{\sim}{z_0'}$ and $y, \underset{\sim}{z_1} = y', \underset{\sim}{z_1'}$. Then $\underset{\sim}{w} = \underset{\sim}{w}'$.

Case(2): $x, \underset{\sim}{z_0} \frown x', \underset{\sim}{z_0'}$ [mod A, Γ_0] and $y, \underset{\sim}{z_1} = y', \underset{\sim}{z_1'}$.

Now either $\underset{\sim}{z_0} \frown \underset{\sim}{z_0'}$ [mod Γ_0], in which case $\underset{\sim}{w} \frown \underset{\sim}{w}'$ [mod Δ], or else $x \frown x'$ [mod A]. Since $y = y'$, we have $(x,y) \frown (x',y')$ [mod $A \otimes B$], hence $\underset{\sim}{w} \frown \underset{\sim}{w}'$ [mod Δ].

Case (3): $x, \underset{\sim}{z_0} = x', \underset{\sim}{z_0'}$ and $y, \underset{\sim}{z_1} \frown y', \underset{\sim}{z_1'}$ [mod B, Γ_1].

The argument is symmetric with case (2).

Case (4): $x, \underset{\sim}{z_0} \frown x', \underset{\sim}{z_0'}$ [mod A, Γ_0] and $y, \underset{\sim}{z_1} \frown y', \underset{\sim}{z_1'}$ [mod B, Γ_1].

Then <u>either</u> $x \frown x'$ [mod A] and $y \frown y'$ [mod B],

<u>or</u> $\underset{\sim}{z_0} \frown \underset{\sim}{z_0'}$ [mod Γ_0] <u>or</u> $\underset{\sim}{z_1} \frown \underset{\sim}{z_1'}$ [mod Γ_1];

in all cases, we have $\underset{\sim}{w} \frown \underset{\sim}{w}'$ [mod Δ].

(x) Π is obtained from Π_0 by the rule ($⅋$):

$$\frac{\vdash A, B, \Gamma}{\vdash A ⅋ B, \Gamma}\ (⅋)$$

Define $\Pi^* \overset{\text{df}}{=} \Pi_0^*$.

<u>The exponentials:</u>

(xi) Π is obtained from Π_0 by the rule (Th?):

$$\frac{\vdash \Gamma}{\vdash ?A, \Gamma}\ (Th?)$$

Define $\Pi^* \overset{\text{df}}{=} \{ \emptyset, \underset{\sim}{z} \mid \underset{\sim}{z} \in \Pi_0^* \}$.

Coherence is immediate: $\emptyset, \underset{\sim}{z} \frown \emptyset, \underset{\sim}{z}'$ [mod $?A, \Gamma$] iff $\underset{\sim}{z} \frown \underset{\sim}{z}'$ [mod Γ].

(xii) Π is obtained from Π_0 by the rule (C?):

$$\frac{\vdash ?A, ?A, \Gamma}{\vdash ?A, \Gamma}\ (C?)$$

Define $\Pi^* \overset{\text{df}}{=} \{ a \cup b, \underset{\sim}{z} \mid a, b, \underset{\sim}{z} \in \Pi_0^*$ and $a \cup b \in A^\perp \}$

Let $a \cup b, \underset{\sim}{z}$ and $a' \cup b', \underset{\sim}{z}' \in \Pi^*$. By hypothesis, we have $a, b, \underset{\sim}{z} \frown a', b', \underset{\sim}{z}'$ [mod $?A, ?A, \Gamma$] and $a \cup b \in A^\perp$ and $a' \cup b' \in A^\perp$. Hence either (1) $a, b, \underset{\sim}{z} = a', b', \underset{\sim}{z}$ or (2) $\underset{\sim}{z} \frown \underset{\sim}{z}'$ [mod Γ] or (3) $a \frown a'$ [mod $?A$] or (4) $b \frown b'$ [mod $?A$]. In cases (1) and (2), we have $a \cup b, \underset{\sim}{z} \frown a' \cup b', \underset{\sim}{z}'$ [mod $?A, \Gamma$]. Assume either (3) or (4) obtains. Then either $a \cup a' \notin A^\perp$ or $b \cup b' \notin A^\perp$. Hence $(a \cup b) \cup (a' \cup b') \notin A^\perp$, for otherwise we would have $a \cup a' \in A^\perp$ and $b \cup b' \in A^\perp$ by down closure. Hence $(a \cup b) \frown (a' \cup b')$ [mod $?A$] and so $a \cup b, \underset{\sim}{z} \frown a' \cup b', \underset{\sim}{z}'$ [mod $?A, \Gamma$].

(xiii) Π is obtained from Π_0 by the rule $(D?)$:

$$\frac{\vdash A, \Gamma}{\vdash ?A, \Gamma}\,(D?)$$

Define $\Pi^* \stackrel{df}{=} \{ \{x\}, \underset{\sim}{z} \mid x, \underset{\sim}{z} \in \Pi_0^* \}$

Let $\{x\}, \underset{\sim}{z}$ and $\{x'\}, \underset{\sim}{z}' \in \Pi^*$. By hypothesis, we have $x, \underset{\sim}{z} \frown x', \underset{\sim}{z}'$ [mod A, Γ]. Hence either (1) $x, \underset{\sim}{z} = x', \underset{\sim}{z}'$ or (2) $\underset{\sim}{z} \frown \underset{\sim}{z}'$ [mod Γ] or (3) $x \frown x'$ [mod A]. In cases (1) and (2), we have $\{x\}, \underset{\sim}{z} \frown \{x'\}, \underset{\sim}{z}'$ [mod $?A, \Gamma$]. Assume (3) obtains. Then $x \smile x'$ [mod $A^\perp$] hence $\{x, x'\} \notin A^\perp$, and so $\{x\} \frown \{x'\}$ [mod $?A$]. Hence $\{x\}, \underset{\sim}{z} \frown \{x'\}, \underset{\sim}{z}'$ [mod $?A, \Gamma$].

(xiv) Π is obtained from Π_0 by the rule $(!)$:

$$\frac{\vdash A, ?B_1, \ldots, ?B_k}{\vdash !A, ?B_1, \ldots, ?B_k}\,(!)$$

Define Π^* to be the set of all sequences of the form $\{x_1, \ldots, x_n\}, \underset{\sim}{z}_1 \cup \ldots \cup \underset{\sim}{z}_n$ such that

(a) $n \geq 1$;

(b) $\{x_1, \ldots, x_n\} \in A$;

(c) for $i = 1, \ldots, n$, $x_i, \underset{\sim}{z}_i \in \Pi_0^*$, where each $\underset{\sim}{z}_i$ is of the form $(b_{i1}, \ldots, b_{ik})$ and $b_{ij} \in (B_j^\perp)_{fin}$ for $j = 1, \ldots, k$;

(d) for $j=1,\dots,k$, $b_{1j} \cup \dots \cup b_{nj} \in B_j^{\perp}$.
We write $\underset{\sim}{z}_1 \cup \dots \cup \underset{\sim}{z}_n \in \Gamma^{\perp}$ for short.

We may assume the $x_1,\dots,x_n$ are distinct: it can be shown that $x_1 = x_2$ implies $\underset{\sim}{z}_1 = \underset{\sim}{z}_2$, so the repetition does not add anything and a size $(n-1)$ sequence would do just as well.

Now let $\underset{\sim}{t} = \{x_1,\dots,x_n\}, \underset{\sim}{z}_1 \cup \dots \cup \underset{\sim}{z}_n$ and $\underset{\sim}{u} = \{y_1,\dots,y_m\}, \underset{\sim}{w}_1 \cup \dots \cup \underset{\sim}{w}_m$ be elements of Π^*.

We argue by cases.

Case (1): $\underset{\sim}{t} = \underset{\sim}{u}$. Then $\underset{\sim}{t} \frown \underset{\sim}{u}$ [mod $!A, ?\Gamma$].

Case (2): $\underset{\sim}{t} \neq \underset{\sim}{u}$ and $\{x_1,\dots,x_n\} \cup \{y_1,\dots,y_m\} \in A$. Then $\{x_1,\dots,x_n\} \frown \{y_1,\dots,y_m\}$ [mod $!A$] hence $\underset{\sim}{t} \frown \underset{\sim}{u}$ [mod $!A, ?\Gamma$].

Case (3): $\underset{\sim}{t} \neq \underset{\sim}{u}$ and $\{x_1,\dots,x_n\} \cup \{y_1,\dots,y_m\} \notin A$. Then there must be an x_i and a y_j such that $\{x_i, y_j\} \notin A$, hence $x_i \smile y_j$ [mod A]. But since $x_i, \underset{\sim}{z}_i \in \Pi_0^*$ and $y_j, \underset{\sim}{w}_j \in \Pi_0^*$, we have $x_j, \underset{\sim}{z}_i \frown y_j, \underset{\sim}{w}_j$ [mod $A, ?\Gamma$]. Hence $\underset{\sim}{z}_i \frown \underset{\sim}{w}_j$ [mod $?\Gamma$]. This in fact implies that $\underset{\sim}{z}_1 \cup \dots \cup \underset{\sim}{z}_n \frown \underset{\sim}{w}_1 \cup \dots \cup \underset{\sim}{w}_m$ [mod $?\Gamma$]. Hence $\underset{\sim}{t} \frown \underset{\sim}{u}$ [mod $!A, ?\Gamma$].

We have not forgotten the (CUT) rule. We have left it until last because the definition of Π^* in this case involves an unbounded existential quantifier; in all the other cases, the definition of Π^* uses only elementary set-theoretic operations applied to Π_0^* and Π_1^*, where Π_0, Π_1 are subproofs.

(xv) Π is obtained from Π_0 and Π_1 by the rule (CUT):

$$\frac{\vdash A, \Gamma_0 \qquad \vdash A^{\perp}, \Gamma_1}{\vdash \Gamma_0, \Gamma_1}\ (\mathrm{CUT})$$

Define $\Pi^* \stackrel{\mathrm{df}}{=} \{\underset{\sim}{z}_0, \underset{\sim}{z}_1 \mid \exists x \in |A| \ (x, \underset{\sim}{z}_0 \in \Pi_0^* \text{ and } x, \underset{\sim}{z}_1 \in \Pi_1^*)\}$.

Suppose $\underset{\sim}{z}_0, \underset{\sim}{z}_1 \in \Pi^*$ with witness $x \in |A|$ and $\underset{\sim}{w}_0, \underset{\sim}{w}_1 \in \Pi^*$ with witness $y \in |A|$. By hypothesis, we have $x, \underset{\sim}{z}_0 \frown y, \underset{\sim}{w}_0$ [mod A, Γ_0] and $x, \underset{\sim}{z}_1 \frown y, \underset{\sim}{w}_1$ [mod $A^\perp, \Gamma_1$]. Now either (1) $x \asymp y$ [mod A] or (2) $x \asymp y$ [mod $A^\perp$]. If case (1) holds, we must have $\underset{\sim}{z}_0 \frown \underset{\sim}{w}_0$ [mod Γ_0], and if case (2) holds, we have $\underset{\sim}{z}_1 \frown \underset{\sim}{w}_1$ [mod Γ_1]. Either way, we get $\underset{\sim}{z}_0, \underset{\sim}{z}_1 \frown \underset{\sim}{w}_0, \underset{\sim}{w}_1$ [mod Γ_0, Γ_1].

A consolation is that the existential quantifier has <u>uniqueness</u> built in; cf. the existential quantifier in the formula (APP) by which a linear (or stable) function is recovered from its trace.

Suppose $x, \underset{\sim}{z}_0 \in \Pi_0^*$ and $y, \underset{\sim}{z}_0 \in \Pi_0^*$ and $x, \underset{\sim}{z}_1 \in \Pi_1^*$ and $y, \underset{\sim}{z}_1 \in \Pi_1^*$. Then $x, \underset{\sim}{z}_0 \frown y, \underset{\sim}{z}_0$ [mod A, Γ_0] and $x, \underset{\sim}{z}_1 \frown y, \underset{\sim}{z}_1$ [mod $A^\perp, \Gamma_1$]. The first implies that either $x = y$ or $x \frown y$ [mod A]; the second implies that either $x = y$ or $x \frown y$ [mod $A^\perp$]. Since we can't have both $x \frown y$ [mod A] <u>and</u> $x \frown y$ [mod $A^\perp$], we must have $x = y$.

This completes the construction. ■

Now we verify our earlier claim. Suppose Π_0 is a proof of $\vdash A$, Π_1 is a proof of $\vdash A \multimap B$ and $\Pi_1^* = \mathrm{Trlin}(F)$ where $F : A \to B$ is linear. Now both as formulae and as coherent spaces, $A \multimap B = A^\perp \parr B$. We may assume the proof Π_1 of $\vdash A^\perp \parr B$ is obtained from a proof Π_2 of $\vdash A^\perp, B$ by the rule ($\parr$). Then $\Pi_2^* = \Pi_1^* = \mathrm{Trlin}(F)$. Hence

$$F(\pi_0^*) = \{ y \in |B| \mid \exists x \in \pi_0^* \, ((x,y) \in Trlin(F)) \}$$
$$= \{ y \in |B| \mid \exists x \in |A| \, (x \in \pi_0^* \text{ and } (x,y) \in \pi_2^*) \}$$

Let π be the proof of $\vdash B$ obtained from the proof π_0 of $\vdash A$ and the proof π_2 of $\vdash A^\perp, B$ by (CUT). Then $\pi^* = F(\pi_0^*)$.

This is all in accordance with Heyting's ideal: the proof π_1 of $\vdash A \multimap B$ is, in an appropriate sense, a function which takes a proof π_0 of $\vdash A$ to a proof '$F(\pi_0)$', i.e. π, of $\vdash B$.

Observation 5·3·1:

We say that two proofs π_0 and π_1 of a sequent $\vdash \Delta$ differ only by their order of rules iff (i) π_0 and π_1 have the same occurrences of instances of axioms schemes; and (ii) for all rules (R) of **LL!** other than (EXCH), (R) is applied in π_0 with principal formula A and premis formulae B and C (or premis formula B) iff (R) is applied in π_1 with the same principal and premis formulae.

If π_0 and π_1 are two proofs of $\vdash \Delta$ which differ only by their order of rules, then $\pi_0^* = \pi_1^*$.

This observation gives us some information about the equivalence relation

$$\pi_0 \sim \pi_1 \quad \text{iff} \quad \pi_0^* = \pi_1^*$$

defined for proofs π_0 and π_1 in **LL!** of a given sequent $\vdash \Delta$.

When else do two proofs Π_0 and Π_1 of $\vdash \Delta$ correspond to the same semantic object?

Consider the following two configurations of proofs.

(1)

$$\cfrac{\cfrac{\vdash A^\perp, A}{[\mu_0]\vdash A^\perp \wp A}(\wp) \qquad \cfrac{\begin{array}{c}\Pi_0\\ \vdash A, \Delta_0\end{array} \qquad \begin{array}{c}\Pi_1\\ \vdash A^\perp, \Delta_1\end{array}}{[\mu_1]\vdash A\otimes A^\perp, \Delta_0, \Delta_1}(\otimes)}{[\mu]\vdash \Delta_0, \Delta_1}(\mathrm{CUT})$$

(2)

$$\cfrac{\begin{array}{c}\Pi_0\\ \vdash A, \Delta_0\end{array} \qquad \begin{array}{c}\Pi_1\\ \vdash A^\perp, \Delta_1\end{array}}{[\Pi]\vdash \Delta_0, \Delta_1}(\mathrm{CUT})$$

The proof Π of $\vdash \Delta_0, \Delta_1$ is obtained from the proof μ of $\vdash \Delta_0, \Delta_1$ by 'pushing the cut upwards'; this is one of a number of possible conversions in the procedure for eliminating cuts. Now compute the semantics:

$$\Pi^* = \{ \tilde{z}_0, \tilde{z}_1 \mid \exists x \in |A| \, (x, \tilde{z}_0 \in \Pi_0^* \text{ and } x, \tilde{z}_1 \in \Pi_1^*) \}$$

$$\mu_0^* = \{ (u,u) \mid u \in |A| \}.$$

$$\mu_1^* = \{ (u,v), \tilde{w}_0, \tilde{w}_1 \mid u, \tilde{w}_0 \in \Pi_0^* \text{ and } v, \tilde{w}_1 \in \Pi_1^* \}$$

$$\begin{aligned}
\mu^* &= \{ \tilde{w}_0, \tilde{w}_1 \mid \exists (u,v) \in |A|\times|A| \, ((u,v) \in \mu_0^* \text{ and } (u,v), \tilde{w}_0, \tilde{w}_1 \in \mu_1^*) \} \\
&= \{ \tilde{w}_0, \tilde{w}_1 \mid \exists u \in |A| \, ((u,u) \in \mu_0^* \text{ and } (u,u), \tilde{w}_0, \tilde{w}_1 \in \mu_1^*) \} \\
&= \{ \tilde{w}_0, \tilde{w}_1 \mid \exists u \in |A| \, (u, \tilde{w}_0 \in \Pi_0^* \text{ and } u, \tilde{w}_1 \in \Pi_1^*) \} \\
&= \Pi^*
\end{aligned}$$

This is not a coincidence.

The system of proof nets for linear logic, which is set out in the next section, is something of a hybrid of sequent calculi and natural deduction systems. Its rules are structurally similar to those of **LL!**, and by an analogous construction, we can define a semantic object β^* for each proof net β in the system of proof nets **PNI!**. A key feature of the normalization (cut elimination) procedure for **PNI!** is that if β is obtained from β_0 by a sequence of one or more conversions, then $\beta_0^* = \beta^*$. Moreover the map N, which sends each proof π in **LL!** of $\vdash A_1, \ldots, A_n$ to a (unique) proof net $N(\pi)$ with conclusions $A_1, \ldots, A_n$, is surjective. In addition, if $N(\pi) = \beta$ then $\pi^* = \beta^*$. So we can start with a proof π_0 of $\vdash \Delta$ in **LL!**, then take $\beta_0 = N(\pi_0)$ and apply any sequence of conversions to β_0 to get a normal (cut free) proof net β_0 (guaranteed by the Strong Normalization Theorem for **PNI!**). By surjectivity, there is a proof π of $\vdash \Delta$ in **LL!** such that $\beta = N(\pi)$; since β is cut-free, so is π. Then we have

$$\pi_0^* = \beta_0^* = \beta^* = \pi^* .$$

The eager reader, tantalized by this advertisement for Section 6, may wish to proceed forthwith in search of the joys of proof nets. But hold on; there is something more we can say about the objects $\pi^* \in \Delta$, where π is a proof of $\vdash \Delta$: they are big. If X is a coherent space, an object $c \in X$ is maximal iff

$$\forall x \in |X| \left(\text{if } \forall y \in c\, (x \supset y\ [\mathrm{mod}\ X]) \text{ then } x \in c \right);$$

equivalently, for all $a \in X$, if $c \subseteq a$ then $a = c$.

Theorem 5.3.2:

If π is a cut-free proof of $\vdash \Delta$ in **LL** then $\pi^* \in \Delta$ is maximal.

Proof:

By induction on the proof π of $\vdash \Delta$

(i) π is an instance of the identity axiom scheme, say $\vdash A, A^\perp$.

$\pi^* = \{ (x,x) \mid x \in |A| \}$.

Let $(y,z) \in |A| \times |A|$ and suppose that for all $x \in |A|$, $(x,x) \supset (y,z)$ [mod $A, A^\perp$]. Take $x = y$. Then $y \supset z$ [mod $A^\perp$]. Take $x = z$. Then $z \supset y$ [mod A]. Hence $y = z$ and $(y,y) \in \pi^*$.

(ii) π is obtained from π_0 by the rule (EXCH).

$\pi^* = \{ \sigma(\underset{\sim}{z}) \mid \underset{\sim}{z} \in \pi_0^* \}$, for some permutation σ.

The maximality of π^* follows immediately from that of π_0^*.

The additives:

(iii) π is an instance of the axiom scheme for $\top$, say $\vdash \top, \Gamma$.

$\pi^* = \emptyset$, and $|\top \mathbin{\&} \Gamma| = \emptyset$.

(iv) π is obtained from a proof π_0 of $\vdash A, \Gamma$ and a proof π_1 of $\vdash B, \Gamma$ by the rule ($\&$).

$\pi^* = \{ (0,x), \underset{\sim}{z_0} \mid x, \underset{\sim}{z_0} \in \pi_0^* \} \cup \{ (1,y), \underset{\sim}{z_1} \mid y, \underset{\sim}{z_1} \in \pi_1^* \}$.

Let $(i,v), \underset{\sim}{w} \in |A \& B, \Gamma|$ be such that

(0) for all $x, \underset{\sim}{z_0} \in \pi_0^*$, $(i,v), \underset{\sim}{w} \supset (0,x), \underset{\sim}{z_0}$ [mod $A \& B, \Gamma$], and

(1) for all $y, \underset{\sim}{z_1} \in \pi_1^*$, $(i,v), \underset{\sim}{w} \supset (1,y), \underset{\sim}{z_1}$ [mod $A \& B, \Gamma$].

Suppose $i = 0$, hence $v \in |A|$. Then (0) implies that for all $x, \underset{\sim}{z_0} \in \pi_0^*$, $v, \underset{\sim}{w} \supset x, \underset{\sim}{z_0}$ [mod A, Γ]. By hypothesis, π_0^*

is maximal. So $v, \underset{\sim}{w} \in \Pi_0^*$ and hence $(0,v), \underset{\sim}{w} \in \Pi^*$. Likewise, if $i=1$ and hence $v \in |B|$, (1) implies that $v, \underset{\sim}{w} \in \Pi_1^*$ and so $(1,v), \underset{\sim}{w} \in \Pi^*$.

(v) Π is obtained from a proof Π_0 of $\vdash A, \Gamma$ by the rule (FST$\oplus$).

$$\Pi^* = \{ (0,x), \underset{\sim}{z} \mid x, \underset{\sim}{z} \in \Pi_0^* \}$$

Let $(i,v), \underset{\sim}{w} \in |A \oplus B, \Gamma|$ be such that for all $x, \underset{\sim}{z} \in \Pi_0^*$, $(i,v), \underset{\sim}{w} \frown\!\!\!\!\smile (0,x), \underset{\sim}{z}$ [mod $A \oplus B, \Gamma$]. If $i=0$ then we have $v, \underset{\sim}{w} \frown\!\!\!\!\smile x, \underset{\sim}{z}$ [mod, A, Γ] for all $x, \underset{\sim}{z} \in \Pi_0^*$. Since Π_0^* is maximal, $v, \underset{\sim}{w} \in \Pi_0^*$ and hence $(0,v), \underset{\sim}{w} \in \Pi^*$. If $i=1$ then, since $(1,v) \smile (0,x)$ [mod $A \oplus B$], we must have $\underset{\sim}{w} \frown \underset{\sim}{z}$ [mod Γ] for all $\underset{\sim}{z}$ for which there is an $x \in |A|$ such that $x, \underset{\sim}{z} \in \Pi_0^*$. But now by choosing any $y \in |A|$ such that for all $x, \underset{\sim}{z} \in \Pi_0^*$, $y \neq x$, we can create an element $y, \underset{\sim}{w} \in |A, \Gamma|$ which is coherent with every $x, \underset{\sim}{z} \in \Pi_0^*$ but not in Π_0^*; contradiction. So the case $i=1$ is not possible.

(vi) Π is obtained from a proof Π_1 of $\vdash B, \Gamma$ by the rule (SND$\oplus$).

$$\Pi^* = \{ (1,y), \underset{\sim}{z} \mid y, \underset{\sim}{z} \in \Pi_1^* \}.$$

The argument is symmetric with (v).

<u>The multiplicatives:</u>

(vii) Π is the axiom $\vdash \mathbb{1}$. $\Pi^* = \{@\}$ and $|\mathbb{1}| = \{@\}$.

(viii) Π is obtained from a proof Π_0 of $\vdash \Gamma$ by the rule ($\perp$).

$$\Pi^* = \{ @, \underset{\sim}{z} \mid \underset{\sim}{z} \in \Pi_0^* \}.$$

The maximality of Π^* follows immediately from that of Π_0^*.

(ix) π is obtained from a proof π_0 of $\vdash A, \Gamma_0$ and a proof π_1 of $\vdash B, \Gamma_1$ by the rule $(\otimes)$.

$\pi^* = \{ (x,y), \tilde{z}_0, \tilde{z}_1 \mid x, \tilde{z}_0 \in \pi_0^* \text{ and } y, \tilde{z}_1 \in \pi_1^* \}$.

Let $(u,v), \tilde{w}_0, \tilde{w}_1 \in |A \otimes B, \Gamma_0, \Gamma_1|$ be such that for all $(x,y), \tilde{z}_0, \tilde{z}_1 \in \pi^*$, we have $(u,v), \tilde{w}_0, \tilde{w}_1 \mathrel{\overset{\frown}{\smile}} (x,y), \tilde{z}_0, \tilde{z}_1$ [mod Δ], where Δ is short for $A \otimes B, \Gamma_0, \Gamma_1$. We argue by cases.

Case (1): $u, \tilde{w}_0 \in \pi_0^*$ and $v, \tilde{w}_1 \in \pi_1^*$. Then $(u,v), \tilde{w}_0, \tilde{w}_1 \in \pi^*$.

Case (2): $u, \tilde{w}_0 \notin \pi_0^*$. Since π_0^* is maximal, there is some $x, \tilde{z}_0 \in \pi_0^*$ such that $u, \tilde{w}_0 \smile x, \tilde{z}_0$ [mod $A; \Gamma_0$]. Hence $u \mathrel{\overset{\smile}{\frown}} x$ [mod A] and $\tilde{w}_0 \mathrel{\overset{\smile}{\frown}} \tilde{z}_0$ [mod Γ_0] but not both $u = x$ and $\tilde{w}_0 = \tilde{z}_0$. Hence for all $y, \tilde{z}_1 \in \pi_1^*$, we have
(a) $(u,v), \tilde{w}_0, \tilde{w}_1 \neq (x,y), \tilde{z}_0, \tilde{z}_1$; and (b) $(u,v) \mathrel{\overset{\smile}{\frown}} (x,y)$ [mod $A \otimes B$] and (c) $\tilde{w}_0 \mathrel{\overset{\smile}{\frown}} \tilde{z}_0$ [mod Γ_0]. Then for all $y, \tilde{z}_1 \in \pi_1^*$, we must have $\tilde{w}_1 \frown \tilde{z}_1$ [mod Γ_1].

Case (2·1): $v, \tilde{w}_1 \notin \pi_1^*$. Then since π_1^* is maximal, there exists a $y, \tilde{z}_1 \in \pi_1^*$ such that $v, \tilde{w}_1 \mathrel{\overset{\smile}{\frown}} y, \tilde{z}_1$ [mod B, Γ_1]. Hence we have a $y, \tilde{z}_1 \in \pi_1^*$ such that $\tilde{w}_1 \mathrel{\overset{\smile}{\frown}} \tilde{z}_1$ [mod Γ_1], contradicting the conclusion of (2).

Case (2·2): $v, \tilde{w}_1 \in \pi_1^*$. Then by the conclusion of (2), we have $\tilde{w}_1 \frown \tilde{w}_1$ [mod Γ_1] ; contradiction.

∎

Taking on faith the advertised result that semantic objects remain constant under the elimination of cuts, we have the immediate

<u>Corollary 5·3·3:</u>

If π is any proof in **LL** of $\vdash \Delta$ then $\pi^* \in \Delta$ is maximal. ∎

Those with less faith may demand a direct proof that the rule (CUT) preserves maximality. The author has laboured long and hard on this one, without success.

The four modal rules in **LL!** are another story. It is relatively easy to show that modal thinning (Th?) and modal contraction (C?) preserve maximality of semantic objects but (D?) and (!) are rather more tricky.

<u>Exercise 5.3.4:</u>

Either prove or find a counterexample to the following propositions.

(i) If π is a proof of $\vdash ?A, \Gamma$ obtained from a proof π_0 of $\vdash A, \Gamma$ by the rule (D?) and $\pi_0^* \in A \parr \Gamma$ is maximal then $\pi^* \in ?A \parr \Gamma$ is maximal.

(ii) If π is a proof of $\vdash !A, ?B_1, \ldots, ?B_K$ obtained from a proof π_0 of $\vdash A, ?B_1, \ldots, ?B_K$ by the rule (!) and $\pi_0^* \in A \parr ?B_1 \parr \ldots \parr ?B_K$ is maximal then $\pi^* \in !A \parr ?B_1 \parr \ldots \parr ?B_K$ is maximal.

<u>Note</u>: (ii) does hold in the case when π is a proof of $\vdash !A$ obtained from a proof π_0 of $\vdash A$ by (!); in that case, $\pi^* = !\pi_0^* = \{ a \in A_{fin} \mid a \subseteq \pi_0^* \}$.

6. Proof nets and normalization

Girard's system of proof nets is motivated by the desire for a system in which the process of reducing proofs to normal form is reasonably neat and simple. Since linear logic has an involutive negation, normalization in a natural deduction system is going to involve messiness similar to that which arises in classical natural deduction systems. (For a Prawitz-style natural deduction system for linear logic, see Avron [1988]). Proof nets are graphical constructions which are like sequent calculus proofs in that they have multiple conclusions and, moreover, each of the sequent calculus rules is directly mimicked in the system of proof nets; in particular, a normal proof net is one which does not contain any instance of the analogue of the cut rule. (For earlier work on graphical proof systems for multiple conclusion logics, see Shoesmith and Smiley [1978].) On the other hand, the system of proof nets **PN1!** is a quotient of the sequent calculus **LL!** in the same way that the intuitionistic natural deduction system **NJ** is a quotient of the sequent calculus **LJ**: sequent calculus proofs which differ only by the order of rules are identified. So, in a sense, proof nets are the real proof objects.

With regard to nomenclature, the system we call **PN1!** is called **PN1** in Girard [1987]; the system we call **PN1**, which captures all of propositional linear logic, doesn't have a name in Girard [1987]. Girard goes on to consider **PN2**, the system with propositional quantifiers; we don't deal with **PN2**. We will work through (and fill in the details for) most of the material on proof nets in Girard [1987] up to, but not including, the proof of the Strong Normalization theorem. Primed by this guide, interested readers should be able to tackle that one on their own.

6.0 Tram trips and PNO

Following Girard, we start by developing a system of proof nets **PNO** which will match the pure multiplicative sequent calculus **LLM** (consisting of the identity axiom scheme and the rules (EXCH), (CUT), ($\otimes$) and ($\parr$)).

Definition 6.0.0:

A proof structure is an object consisting of consisting of occurrences of formulae in $\mathcal{L}_0$ (the $\{\otimes, \parr\}$ fragment) and links between these occurrences of formulae. The links are of the following kinds:

(i) axiom link: $\overline{A \qquad A^{\perp}}$ where A is a literal,

(ii) CUT link: $\dfrac{A \qquad A^{\perp}}{\text{CUT}}$

(iii) $\otimes$ link: $\dfrac{A \qquad B}{A \otimes B}$

(iv) $\parr$ link: $\dfrac{A \qquad B}{A \parr B}$

An axiom link has no premises and two conclusions. With respect to the other kinds of links, occurrences of formula above the line are premises of the link, and an occurrence of a formula below the line is the conclusion of the link. The symbol 'CUT' is not a formula (so CUT links have two premises and no conclusion). Both axiom links and CUT links are considered symmetric, i.e. A and $A^{\perp}$ can be interchanged.

We also require that

(1) every occurrence of a formula in the structure is the conclusion of exactly one link; and

(2) every occurrence of a formula in the structure is the premis of at most one link.

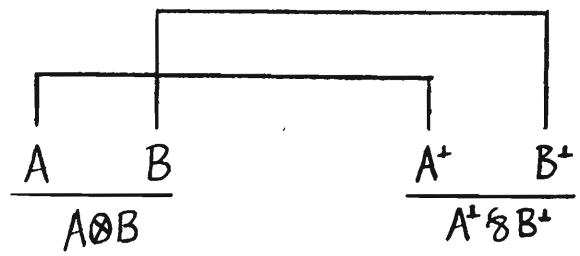
An occurrence of a formula in a proof structure which is not the premis of any link is called <u>terminal</u>.
A link in a proof structure is called a <u>terminal link</u> of that proof structure iff either its conclusion (or conclusions) is (are) terminal, or else it is a CUT link.

To be precise, we should define an occurrence of a formula as an ordered pair (A, i) where A is a formula and i is a positive integer. And, technically, we should define binary relations $AX((A,i),(A^{\perp},j))$ and $CUT((A,i),(A^{\perp},j))$ and ternary relations $\otimes((A,i),(B,j),(A\otimes B,k))$ and $⅋((A,i),(B,j),(A⅋B,k))$, but that would be needless precision. We shall be content with graphical representations and where there is no risk of ambiguity, speak of formulae rather than formula occurrences.

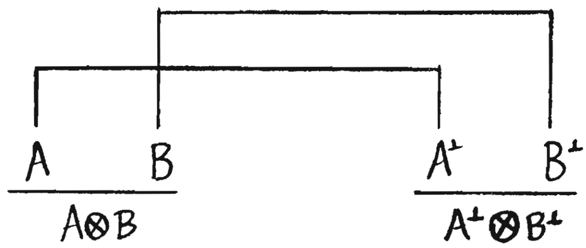
Examples 6.0.1:

The following diagrams represent proof structures.

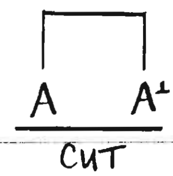
(a)



(b)



(c)

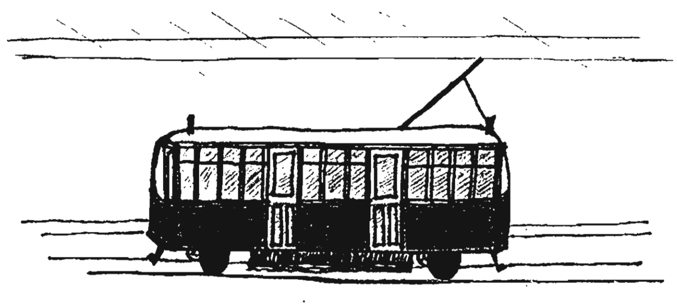


Definition 6.0.2:

A proof structure with terminals $A_1, \ldots, A_n$ is correct iff the sequent $\vdash A_1, \ldots, A_n$ is provable in **LLM**.

Clearly, example (a) above represents a correct proof structure while examples (b) and (c) do not (the empty sequent is not provable). So we need a criterion by which we can distinguish the correct proof structures from the incorrect. Noting the graphical similarity of examples (a) and (b), the criterion must be such that

$\otimes$ and $\mathbin{\rotatebox[origin=c]{180}{\&}}$ links can be clearly differentiated. Girard calls his criterion the <u>long trip condition</u>. For pedagogical purposes, we elaborate on the theme of travel; specifically, tram travel.



<u>Definition 6·0·3</u>:

Each proof structure determines a network of <u>tram tracks.</u> With each formula occurrence A in a proof structure, we associate two <u>tram stops</u>: the left hand side tram stop, from which one catches north-bound ($\uparrow$) trams, is denoted $A^\wedge$, and the right hand side tram stop, from which one catches south-bound ($\downarrow$) trams, is denoted $A^\vee$.

The layout of track in the network is such that every <u>trip</u> is a <u>round trip</u>; when a tram stops at, say, $A^\wedge$, then for some positive integer k, the k^{th} stop to which the tram travels after leaving $A^\wedge$ will be $A^\wedge$ again.

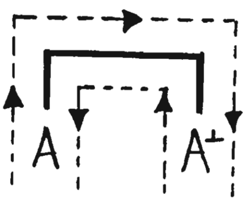
Let S be the collection of all tram stops in the network and let p be the number of formula occurrences in the corresponding proof structure, so the cardinality of S is $2p$. A <u>trip</u> in the network is a bijective function $t: S_0 \longrightarrow \mathbb{Z}/k\mathbb{Z}$, where $S_0 \subseteq S$ (so $k \leq 2p$), subject to some further conditions set out below. We say two trips $t : S_0 \longrightarrow \mathbb{Z}/k\mathbb{Z}$ and $t' : S_0 \longrightarrow \mathbb{Z}/k\mathbb{Z}$ are <u>equivalent</u> iff for all tram stops $\Sigma \in S_0$,

$$t'(\Sigma) \equiv t(\Sigma) + r \quad [\mathrm{mod}\ k]$$

for some $k \in \{0, 1, \ldots, k-1\}$. Otherwise put, two trips are equivalent when they define the same cyclic ordering (modulo k) on S_0, but differ in the choice of initial tram stop. Two trips are <u>distinct</u> iff they are not equivalent.

We define simultaneously the network of tram tracks for a proof structure and the possible trips through that network by reference to the links and terminal formula occurrences contained in the given proof structure. The definition is component-wise.

(1) <u>axiom links</u>:
Tram tracks in the vicinity of an axiom link are as follows.



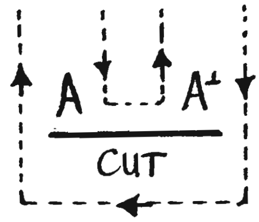
The tracks are such that every trip t satisfies

(i) $t(A_\vee) = t(A^{\perp}{}^{\wedge}) + 1$, and

(ii) $t(A^{\perp}_{\vee}) = t(A^{\wedge}) + 1$.

(2) CUT links:

Tram tracks in the vicinity of a CUT link are as follows.



The tracks are such that every trip t satisfies

(i) $t(A^{\wedge}) = t(A^{\perp}{}_{\vee}) + 1$, and

(ii) $t(A^{\perp\wedge}) = t(A_{\vee}) + 1$.

(3) terminal formula occurrences:

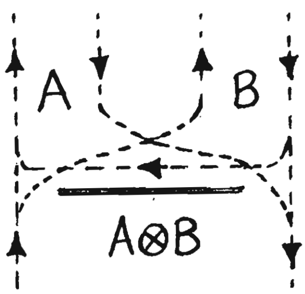
Tram tracks in the vicinity of terminal formula occurrences are as follows.

The track is such that every trip t satisfies

$t(A^{\wedge}) = t(A_{\vee}) + 1$.

(4) ⊗ links:

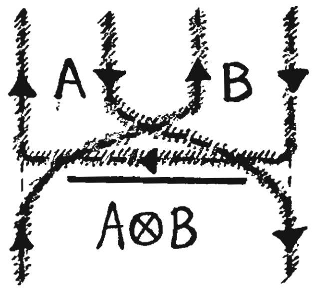
Tram tracks in the vicinity of ⊗ links are as follows.



Associated with each $\otimes$ link is a switch with two positions, "L" and "R".

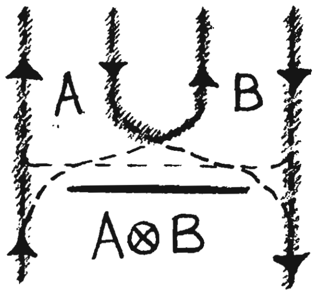
When the switch is on "L", trips t satisfy the following conditions:

(i) $t(A^\wedge) = t(B_\vee) + 1$;
(ii) $t(B^\wedge) = t(A\otimes B^\wedge) + 1$;
(iii) $t(A\otimes B_\vee) = t(A_\vee) + 1$.

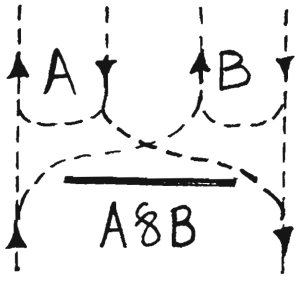


When the switch is on "R", trips t satisfy the following conditions:

(i) $t(A^\wedge) = t(A\otimes B^\wedge) + 1$;
(ii) $t(B^\wedge) = t(A_\vee) + 1$;
(iii) $t(A\otimes B_\vee) = t(B_\vee) + 1$.



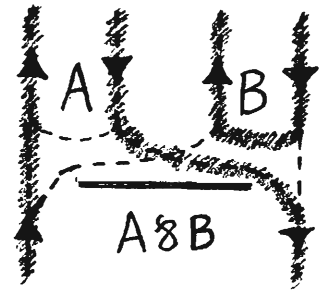
(5) <u>⅋ links:</u>
Tram tracks in the vicinity of ⅋ links are as follows.



Associated with each $\parr$ link is a switch with two positions, "L" and "R".

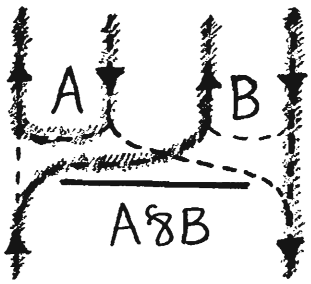
When the switch is on "L", trips t satisfy the following conditions:

(i) $t(A^{\wedge}) = t(A \parr B^{\wedge}) + 1$;
(ii) $t(B^{\wedge}) = t(B_{\vee}) + 1$;
(iii) $t(A \parr B_{\vee}) = t(A_{\vee}) + 1$.



When the switch is on "R", trips t satisfy the following conditions:

(i) $t(A^{\wedge}) = t(A_{\vee}) + 1$;
(ii) $t(B^{\wedge}) = t(A \parr B^{\wedge}) + 1$;
(iii) $t(A \parr B_{\vee}) = t(B_{\vee}) + 1$.



In view of the above specifications, each trip t in the given tram network / proof structure is uniquely determined by the choice of tramstop Σ such that $t(\Sigma) = 0$ and the settings of all the $\otimes$ and $\parr$ switches in the network. Given a tramstop $\Sigma \in S$ and a configuration of $\otimes$ and $\parr$ switches, let $k \leq 2p$ be the smallest positive integer such that $t(\Sigma) = k$ and let $S_0 \subseteq S$ be the collection of all tram stops visited in the course of the trip. In this case, t is a bijection $t : S_0 \to \mathbb{Z}/k\mathbb{Z}$ (and all the identity symbols in the above specifications are to be reinterpreted as congruence modulo k).

Let $t : S_0 \to \mathbb{Z}/k\mathbb{Z}$ be any trip in the given tram network / proof structure. t is a <u>long trip</u> iff $k = 2p$; equivalently, iff $S_0 = S$. Otherwise, t is a <u>short trip</u>.

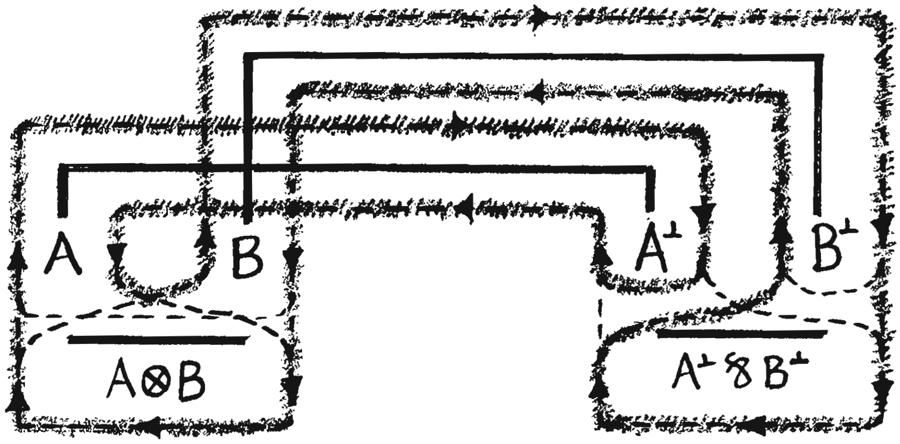
(End of Definition 6.0.3.)

Observe that if a proof structure contains n $\otimes$ or $⅋$ links then, for any given tram stop Σ_i in the corresponding tram network, there are 2^n <u>distinct</u> trips t such that $\Sigma_i \in \mathrm{dom}(t)$.

<u>Examples 6.0.4:</u>

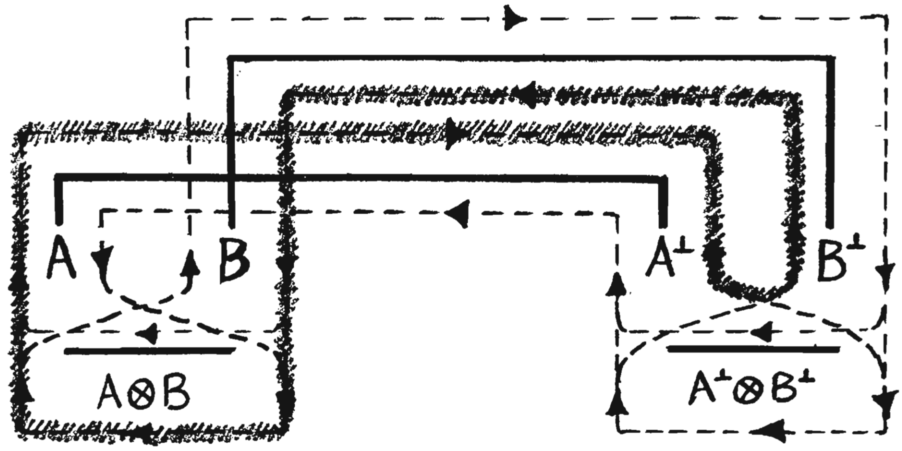
Recall the proof structures represented in 6.0.1. We draw them again, now enhanced with tram tracks, and take a few trips.

(a)



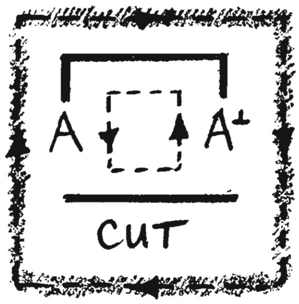
The shaded track represents the trips with both the $\otimes$ switch and the $⅋$ switch set on "R"; the twelve equivalent trips (one for each possible initial tram stop) are long trips. The reader is invited to verify that the other three configurations of switch settings also give rise to long trips.

(b)



The shaded track corresponds to the trip starting from, say, $A^{\wedge}$ with both ⊗ switches set on "R" (and to the other five equivalent trips). So we have a short trip in an incorrect proof structure.

(c)



As expected, we also get a short trip in this proof structure.

<u>Definition 6.0.5:</u>

A proof structure is called a <u>proof net</u> iff every trip in the tram network determined by that proof structure is a long trip. Let PNO denote the collection of all proof nets built out of axiom links, CUT links, ⊗ links and ⅋ links.

Of course, we can't yet claim that a proof structure is correct iff it is a proof net; the rest of 6.0 will be devoted to establishing this result. Since a proof structure with n switches give rise to 2^n distinct trips (which include a given tram stop), the long trip criterion is not a feasible method of checking correctness. In practice, we can always work with proof structures that come directly (by the method set out below) from sequent calculus proofs, or that come from correct proof structures by means of transitions which preserve correctness. Indeed, it is easy to inductively define a collection of correct proof structures (which will turn out to be identical to **PNO**) every element of which comes from a proof in **LLM**. To prove, rather than obtain by definitional theft, that **PNO** is what we want it to be, we need an abstract property like the long trip criterion.

On the practical side of things, some improvement has been made by Danos and Regnier [1989]. By working with an alternative graphical representation of proof structures, they show how correctness can be verified by checking at most 2^m cases, where **m** is the number of ⅋ links in the given structure. In that paper, Danos and Regnier also develop a generalized multiplicative connective.

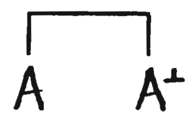
<u>Theorem 6·0·6</u>: (Girard [1987])

If π is a proof of $\vdash A_1, \ldots, A_n$ in **LLM** then we can naturally associate with π a proof net $N(\pi)$ in **PNO** whose terminal formula occurrences are exactly $A_1, \ldots, A_n$.

<u>Proof</u>:

$N(\pi)$ is defined by induction on the proof π.

(i) π is an instance $\vdash A, A^\perp$ of the identity axiom scheme. Obviously, $N(\pi)$ is the proof structure



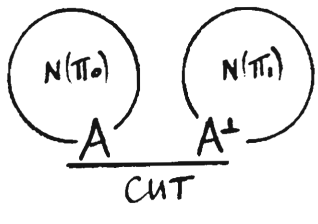
which is a proof net: all trips are of the form $\ldots, A^\wedge, A^\perp{}_\vee, A^{\perp\wedge}, A_\vee, A^\wedge, \ldots$, which are long trips.

(ii) π is obtained from π_0 by the rule (EXCH). Set $N(\pi) = N(\pi_0)$.

(iii) π is obtained from π_0 and π_1 by the rule (CUT):

$$\frac{\vdash A, \Delta_0 \qquad \vdash A^\perp, \Delta_1}{\vdash \Delta_0, \Delta_1}\ (\mathrm{CUT})$$

By the induction hypothesis, we have proof nets $N(\pi_0)$ and $N(\pi_1)$ which have as their terminals A and all the formula occurrences in Δ_0, and $A^\perp$ and all of Δ_1, respectively. We construct a proof structure $N(\pi)$ as follows:



The set of terminals of $N(\pi)$ is $\Delta_0 \cup \Delta_1$ (considering Δ_0 and Δ_1 as sets of formula occurrences rather than sequences of formulae). Suppose there are p formula occurrences in $N(\pi_0)$ and q formula occurrences in $N(\pi_1)$. Arbitrarily select positions for all the switches in $N(\pi_0)$ and $N(\pi_1)$. Let t_0 be the resulting trip in $N(\pi_0)$ starting at $A^{\wedge}$ and let t_1 be the trip in $N(\pi_1)$ starting at $A^{\perp\wedge}$; both t_0 and t_1 are long trips. Let t be the trip in $N(\pi)$, starting at $A^{\wedge}$, determined by the given configuration of switches. Then t is such that

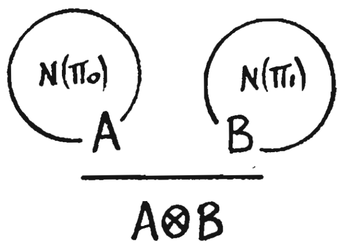
$$t(\Sigma_0) = t_0(\Sigma_0) \text{ for all tram stops } \Sigma_0 \text{ in } N(\pi_0), \text{ and}$$
$$t(\Sigma_1) = 2p + t_1(\Sigma_1) \text{ for all tram stops } \Sigma_1 \text{ in } N(\pi_1).$$

In particular, $t(A^{\perp}{}_{\vee}) = 2p+2q-1$, and after $A^{\perp}{}_{\vee}$ the tram must return to $A^{\wedge}$. Hence t is a long trip. Since the switch settings were arbitrary, $N(\pi)$ is a proof net.

(iv) π is obtained from π_0 and π_1 by the rule $(\otimes)$:

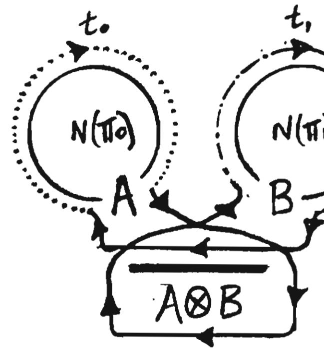
$$\frac{\vdash A, \Delta_0 \qquad \vdash B, \Delta_1}{\vdash A\otimes B, \Delta_0, \Delta_1}\,(\otimes)$$

From proof nets $N(\pi_0)$ and $N(\pi_1)$ whose sets of terminals are $\{A\} \cup \Delta_0$ and $\{B\} \cup \Delta_1$ respectively, construct a proof structure $N(\pi)$, with terminals $\{A\otimes B\} \cup \Delta_0 \cup \Delta_1$ as follows:

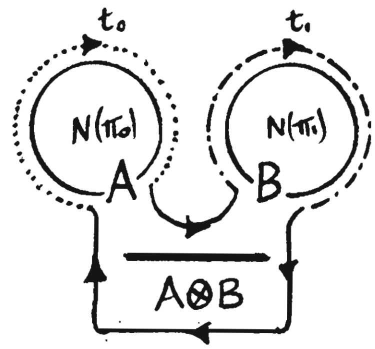


Arbitrarily select positions for all the switches in $N(\pi_0)$ and $N(\pi_1)$. Let t_0 be the resulting (long) trip in $N(\pi_0)$ starting at $A^{\wedge}$ and let t_1 be the resulting (long) trip in $N(\Pi_1)$ starting at $B^\wedge$. For the given configuration of switches in $N(\Pi_0)$ and $N(\Pi_1)$, there are two possible trips in $N(\Pi)$ starting at $A^\wedge$: one for each of the two positions of the final $\otimes$ switch.

If the switch is on "L", the tram follows the route of t_0 until it gets to $A_\vee$, then goes to $A\otimes B_\vee$, $A\otimes B^\wedge$ and then $B^\wedge$. Then it follows the route of t_1 until it gets to $B_\vee$ and then goes back to $A^\wedge$. Graphically, the situation is as follows:



If the switch is on "R", then the trip is as follows:

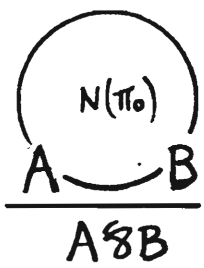


By inspection, both trips are long. Hence $N(\Pi)$ is a proof net.

(v) Π is obtained from Π_0 by the rule ($\wp$):

$$\frac{\vdash A, B, \Delta}{\vdash A \wp B, \Delta}\ (\wp)$$

From the proof net $N(\pi_0)$ whose set of terminals is $\{A, B\} \cup \Delta_0$, construct a proof structure $N(\pi)$ with terminals $\{A ⅋ B\} \cup \Delta_0$ as follows:



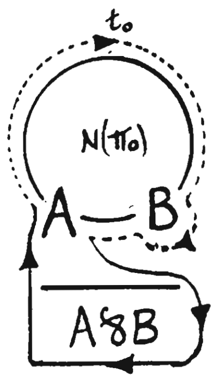
Arbitrarily select positions for all the switches in $N(\pi_0)$ and let t_0 be the resulting (long) trip in $N(\pi_0)$ starting at $A^\wedge$. For the given configuration of switches in $N(\pi_0)$, there are trips in $N(\pi)$ starting at $A^\wedge$.

If the final ⅋ switch is on "L", the tram starts at $A^\wedge$ following the route of t_0, gets to $B_\vee$ and loops around to $B^\wedge$ as it does on t_0, and continues on to $A_\vee$. Then it goes down to $A⅋B_\vee$, around to $A⅋B^\wedge$ and back to $A^\wedge$.

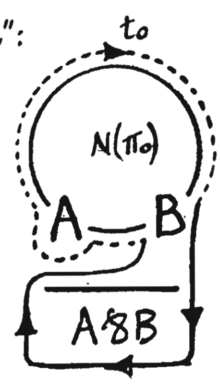
If the final ⅋ switch is on "R", the tram follows the route of t_0 until it get to $B_\vee$, then goes down to $A⅋B_\vee$, around to $A⅋B^\wedge$ and up to $B^\wedge$. From $B^\wedge$ onwards to $A_\vee$, the tram resumes the course of t_0. After $A_\vee$, it loops back to $A^\wedge$, as it does on t_0.

Graphically, the two cases are as follows:

"L":



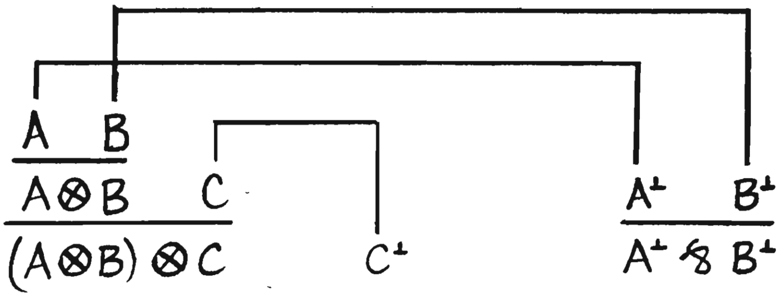
"R":



In both cases we have long trips. Hence $N(\pi_0)$ is a proof net. ■

Proposition 6·0·7: (Girard [1987])
If π_0 and π_1 are two proofs of $\vdash \Delta$ in **LLM** which differ only by their order of rules
then $N(\pi_0) = N(\pi_1)$. ■

The proof of 6·0·7 is just an elaboration of the fact that sequent calculus proofs proceed sequentially, adding one new connective at a time, while proof nets are built up in a parallel fashion. As an illustration, the proof net



is the image under the map $N :$ **LLM** $\longrightarrow$ **PNO** of both of the following proofs of $\vdash (A\otimes B)\otimes C,\ A^\perp \parr B^\perp,\ C^\perp$.

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

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

To establish that every proof net in **PNO** is a correct proof structure, we must show that the map $N: \mathbf{LLM} \to \mathbf{PNO}$ is surjective. This result requires a rather delicate argument.

<u>Theorem 6.0.8</u>: (Girard [1987])
The map $N: \mathbf{LLM} \to \mathbf{PNO}$ is surjective.

<u>Proof</u>:
Let β be a proof net in **PNO** and let $A_1, \ldots, A_n$ be a list of the terminal formula occurrences of β. We prove, by induction on the number of links in β, that there is a proof π in **LLM** of $\vdash \sigma(A_1, \ldots, A_n)$, for some permutation σ, such that $\beta = N(\pi)$.

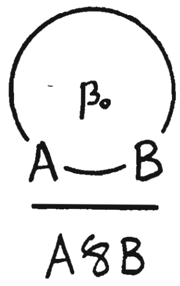
Suppose β has exactly one link. Then β must be of the form

in which case, take π to be the instance $\vdash A, A^{\perp}$ of the Identity axiom scheme.

Suppose β has more than one link. Now β cannot consist of two or more non-connected axiom links since all trips in such proof structures are short.

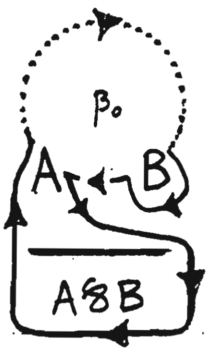
So β must contain either a CUT link or else a terminal $\otimes$ or $\parr$ link.

Case (i): β has at least one terminal $\parr$ link. We draw β as follows:



Here, β_0 is the proof structure obtained from the proof net β by removing the $\parr$ link (so A and B are terminal in β_0). We claim that β_0 is a proof net. Arbitrarily select positions for all the switches in β_0 and suppose the additional $\parr$ switch in β is on "L". In β we have a long trip of the form

$$A^\wedge, \ldots, B_\vee, B^\wedge, ---, A_\vee, A \parr B_\vee, A \parr B^\wedge, A^\wedge.$$



This shows that the trip in β_0 of the form

$$A^\wedge, \ldots, B_\vee, B^\wedge, ---, A_\vee, A^\wedge$$

is a long trip. Since the positioning of switches was arbitrary, β_0 is a proof net.

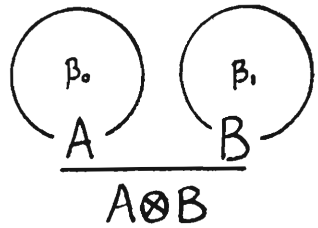
Since β_0 has one less link than β, the induction hypothesis gives us a proof Π_0 of $\vdash A, B, \Gamma$. (where Γ is a sequence of all the terminals of β_0 other than A and B) such that $\beta_0 = N(\Pi_0)$. Then we can take Π to be the proof

$$\dfrac{\begin{array}{c}\Pi_0 \\ \vdash A, B, \Gamma\end{array}}{\vdash A \invamp B, \Gamma}\ (\invamp)$$

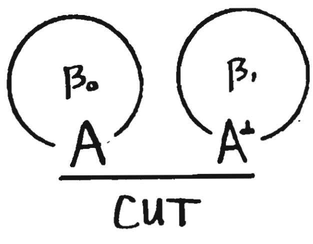
and clearly, $\beta = N(\Pi)$.

Case (ii): β has no terminal $\invamp$ links. Then β must contain at least one CUT link or at least one terminal $\otimes$ link. Notice that CUT links and terminal $\otimes$ links are structurally similar: if we made a terminal $\otimes$ link out of premises A and $A^\perp$, and stipulated that all tram trips are to run express (not stopping) through the tram stops $(A \otimes A^\perp)^\vee$ and $(A \otimes A^\perp)^\wedge$ then the result would be the same as if we made a CUT link out of A and $A^\perp$.

We say a terminal $\otimes$ link in a proof net β splits iff there are sub-proof nets β_0 and β_1 of β such that every formula occurrence in β other than the conclusion of the $\otimes$ link is in exactly one of β_0 and β_1, and the only link between β_0 and β_1 is the $\otimes$ link in question.



Likewise, we say a CUT link in a proof net β <u>splits</u> iff there are sub-proof nets β_0 and β_1 of β such that every formula occurrence in β is in exactly one of β_0 and β_1, and the only link between β_0 and β_1 is the CUT link in question.



To complete the proof of the surjectivity of the map N, we need the following, by no means obvious, result.

<u>Theorem 6·0·9</u>: the Splitting Theorem (Girard [1987])

If β is a proof net in **PNO** with more than one link but no terminal $\otimes$ links,

then there is either a CUT link in β which splits or else a terminal $\otimes$ link in β which splits. □

For now, we take the Splitting Theorem on faith. Suppose we have a CUT link in β, with premises A and $A^\perp$, which splits. Applying the induction hypothesis to β_0 and β_1, we obtain proofs π_0 and π_1 in **LLM** of $\vdash A, \Gamma_0$ and $\vdash A^\perp, \Gamma_1$, respectively, such that $\beta_0 = N(\pi_0)$ and $\beta_1 = N(\pi_1)$. Then take π to be the proof

$$\frac{\overset{\pi_0}{\vdash A, \Gamma_0} \qquad \overset{\pi_1}{\vdash A^\perp, \Gamma_1}}{\vdash \Gamma_0, \Gamma_1}\ (\mathrm{CUT})$$

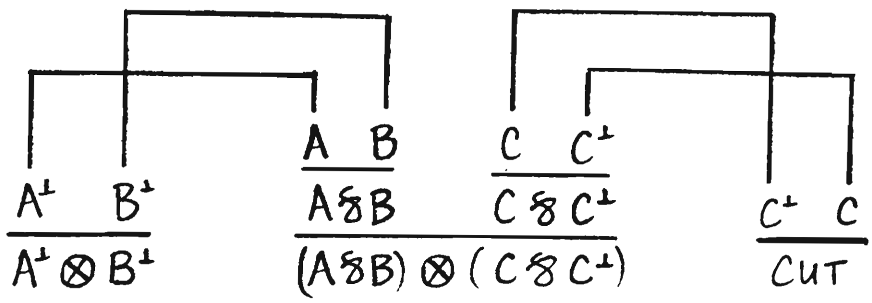
Clearly, $\beta = N(\pi)$.

Similarly, if there is a terminal $\otimes$ link in β which splits, then by applying the induction hypothesis to β_0 and β_1, we readily obtain the desired proof π in **LLM** such that $N(\pi) = \beta$. ■

Observation 6.0.10:

Let β be a proof net in **PNO** and fix an ordering, say $A_1, \ldots, A_n$, on the terminal formula occurrences of β. By the surjectivity of the map $N : \mathbf{LLM} \longrightarrow \mathbf{PNO}$, there is a proof π_0 in **LLM** of $\vdash \sigma(A_1, \ldots, A_n)$, for some permutation σ, such that $\beta = N(\pi_0)$. Now apply the exchange rule to π_0 to obtain a proof π of $\vdash A_1, \ldots, A_n$. We can now define an object $\beta^* \in A_1 \mathbin{⅋} \ldots \mathbin{⅋} A_n$ (identifying formulae with coherent spaces) by simply putting $\beta^* = \pi^*$. To ensure that β^* is well-defined, we have to verify that whenever $N(\pi_0) = N(\pi_1)$, $\pi_1^* = \{ \tau(\underset{\sim}{z}) \mid \underset{\sim}{z} \in \pi_0^* \}$ for some permutation τ. We omit the verification.

If it were the case that in any proof net without terminal ⅋ links, <u>every</u> CUT link and terminal $\otimes$ link splits, then the Splitting Theorem would be trivial. But this is not the case. For example, consider the following proof net.



The central $\otimes$ link splits but neither the CUT link nor the other $\otimes$ link are splittable. Note also that the hypothesis 'without terminal ⅋ links' is necessary: look again at the proof net labelled (a) in Examples 6·0·1.

We will set out the main lines of argument in the proof of the Splitting Theorem, but omit some of the details.

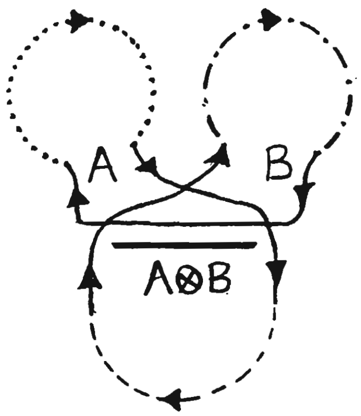
<u>Lemma 6·0·11:</u>
Let β be a proof net, let $\frac{A \quad B}{A\otimes B}$ be a $\otimes$ link in β and let t be any (necessarily long) trip in β.
If the given $\otimes$ switch is on "L" then the trip t is of the form

$$A^{\wedge}, \ldots, A_{\vee}, A\otimes B_{\vee}, \text{----}, A\otimes B^{\wedge}, B^{\wedge}, \text{-.-.-}, B_{\vee}, A^{\wedge}$$

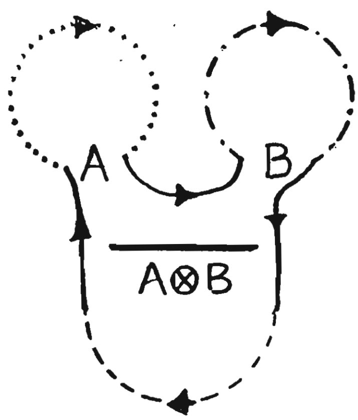
and if the given $\otimes$ switch is on "R" then the trip t is of the form

$$A^{\wedge}, \ldots, A_{\vee}, B^{\wedge}, \text{-.-.-}, B_{\vee}, A\otimes B_{\vee}, \text{----}, A\otimes B^{\wedge}, A^{\wedge}.$$

Graphically, the trips are as follows.



Switch on "L"



Switch on "R"

Proof:

Suppose the $\otimes$ switch is on "L". Assume, for a contradiction, that the next tram stop in the $\otimes$ link to which the tram travels after $A\otimes B_v$ is not $A\otimes B^{\wedge}$. The only other points of entry to the $\otimes$ link are A_v and B_v. We can eliminate A_v, for otherwise we would have a short trip

$$A_v, A\otimes B_v, \text{---.---.--}, A_v.$$

So suppose the next stop in the $\otimes$ link after $A\otimes B_v$ is B_v. The the trip must be of the form

$$A_v, A\otimes B_v, \text{---.-----}, B_v, A^{\wedge}, \text{...---...}, A\otimes B^{\wedge}, B^{\wedge}, \text{--..--..-}, A_v$$

By then when the $\otimes$ switch is on "R" we can piece together a short trip

$$B_v, A\otimes B_v, \text{---.-----.---}, B_v.$$

The argument is similar when we start with the $\otimes$ switch on "R". ■

Using a similar sort of argument, we can also characterize the general pattern of trips through $\parr$ links.

Lemma 6.0.12:

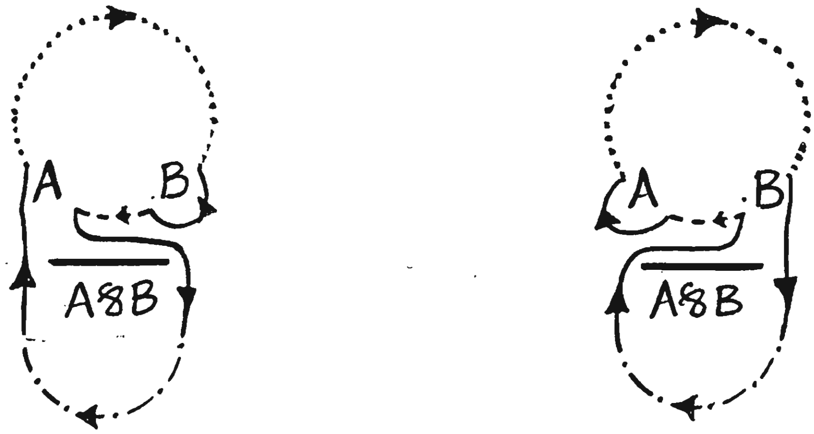
Let β be a proof net, let $\dfrac{A \quad B}{A\parr B}$ be a $\parr$ link in β and let t be any (long) trip in β.
If the given $\parr$ switch is on "L", then the trip t is of the form

$$A^{\wedge}, \ldots, B_v, B^{\wedge}, \text{----}, A_v, A\parr B_v, \text{-.-.-}, A\parr B^{\wedge}, A^{\wedge}$$

and if the given ⅋ switch is on "R" then the trip t is of the form

$A^{\wedge}, \ldots, B_{\vee}, A⅋B_{\vee}, \ldots, A⅋B^{\wedge}, B^{\wedge}, \ldots, A_{\vee}, A^{\wedge}$.

Graphically, the trips are as follows.



Switch on "L" Switch on "R" ■

Definition 6.0.13:

Let β be a proof net in **PNO**, let A be any formula occurrence in β which is a premis of a link, and let t be any (long) trip in β. The interval denoted $[A^{\wedge}, A_{\vee}]_t$ is the collection of all tram stops between $A^{\wedge}$ and $A_{\vee}$ on the trip t, together with $A^{\wedge}$ and $A_{\vee}$. $[A^{\wedge}, A_{\vee}]_t$ is ordered in terms of the trip t. When A is a formula occurrence in β which is the conclusion of a link, the interval $[A_{\vee}, A^{\wedge}]_t$ is defined similarly.

Corollary 6.0.14:

If $\frac{A \quad B}{A \otimes B}$ is any $\otimes$ link in a proof net β then for each trip t in β, the intervals $[A^{\wedge}, A_{\vee}]_t$, $[B^{\wedge}, B_{\vee}]_t$ and $[A\otimes B_{\vee}, A\otimes B^{\wedge}]_t$ are pair-wise disjoint and their union is the collection of all tramstops in β. ■

Corollary 6.0.15:

If $\frac{A \quad A^{\perp}}{\text{CUT}}$ is any CUT link in a proof net β then for each trip t in β, $[A^{\wedge}, A_{\vee}]_t \cap [A^{\perp\wedge}, A^{\perp}{}_{\vee}]_t = \emptyset$. and $[A^{\wedge}, A_{\vee}]_t \cup [A^{\perp\wedge}, A^{\perp}{}_{\vee}]_t$ contains every tramstop in β. ∎

Definition 6.0.16:

Let β be a proof net and let A be either a premis of a $\otimes$ link in β or a premis of a CUT link in β. We define

$$(A^{\wedge}, A_{\vee})_t \overset{\text{df}}{=} \{ C \mid C^{\wedge} \in [A^{\wedge}, A_{\vee}]_t \text{ and } C_{\vee} \in [A^{\wedge}, A_{\vee}]_t \}$$

that is, the collection of all formula occurrences in β both of whose tram stops are in the interval $[A^{\wedge}, A_{\vee}]_t$.

We define the <u>empire</u> of A, denoted eA, as follows:

$$eA \overset{\text{df}}{=} \{ C \mid \text{for all trips } t \text{ in } \beta,\ C \in (A^{\wedge}, A_{\vee})_t \}$$

So eA is the intersection of all the $(A^{\wedge}, A_{\vee})_t$; trivially, $A \in eA$.

Corollary 6.0.17:

If $\frac{A \quad B}{A \otimes B}$ is any $\otimes$ link in a proof net β then $eA \cap eB = \emptyset$. ∎

Corollary 6.0.18:

If $\frac{A \quad A^{\perp}}{\text{CUT}}$ is any CUT link in a proof net β then $eA \cap eA^{\perp} = \emptyset$. ∎

Lemma 6.0.18: (Girard [1987])

Let $\frac{A \quad B}{A \otimes B}$ be any $\otimes$ link in a proof net β.

(i) If C is linked to $C^{\perp}$ in β by an axiom link $\overline{C \quad C^{\perp}}$
then $C \in eA$ iff $C^{\perp} \in eA$.

(ii) If C is linked to $C^{\perp}$ in β by a CUT link $\frac{C \quad C^{\perp}}{CUT}$
then $C \in eA$ iff $C^{\perp} \in eA$.

(iii) If $\frac{C \quad D}{C \otimes D}$ is any $\otimes$ link in β distinct from $\frac{A \quad B}{A \otimes B}$
then $C \in eA$ iff $C \otimes D \in eA$, and
$D \in eA$ iff $C \otimes D \in eA$.

(iv) If $\frac{C \quad D}{C \,\&\, D}$ is any $\&$ link in β
then $C \in eA$ and $D \in eA$ iff $C \,\&\, D \in eA$.

(v) If C is an hereditary premis of A in β
then $C \in eA$.

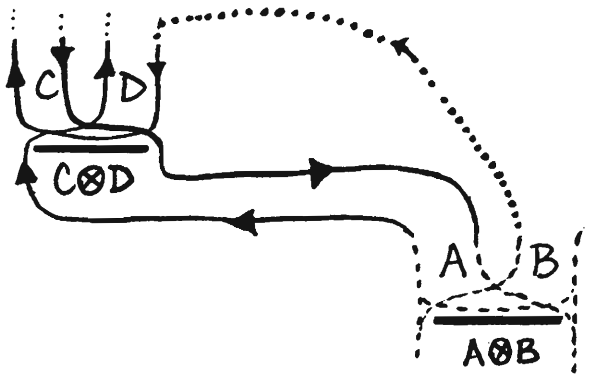
Proof:

(V) is a consequence of (i)—(iv).

(i) and (ii) are immediate: in the first case we have $t(C_\vee) = t(C^{\perp\wedge}) + 1$ and $t(C^{\perp}_{\vee}) = t(C^{\wedge}) + 1$ for all trips t in β; in the second case we have $t(C^{\wedge}) = t(C^{\perp}_{\vee}) + 1$ and $t(C^{\perp\wedge}) = t(C_\vee) + 1$ for all trips t in β.

The proofs of (iii) and (iv) involve teasing out the consequences of the general pattern of trips through $\otimes$ and $\&$ links (Lemmas 6.0.11 and 6.0.12). As an illustration, we give the proof of the second part of (iii): if $C \otimes D \in eA$ then $C \in eA$ and $D \in eA$.

If $C \otimes D \in eA$ then for all trips t in β, $C \otimes D^{\wedge} \in [A^{\wedge}, A_{\vee}]_t$ and $C \otimes D_{\vee} \in [A^{\wedge}, A_{\vee}]_t$. Let t be a trip in β such that the $\frac{C \quad D}{C\otimes D}$ switch is on "L".



Then $C_v \in [A^\wedge, A_v]_t$ and $D^\wedge \in [A^\wedge, A_v]_t$. Now suppose that $D_v \notin [A^\wedge, A_v]_t$. Then either $D_v \in [B^\wedge, B_v]_t$ or else $D_v \in [A\otimes B_v, A\otimes B^\wedge]_t$. Assume the former and consider the sequence of tramstops $B^\wedge, \ldots, D_v$ on the trip t. By changing the $C\otimes D$ switch to "R" and setting the $A\otimes B$ switch on "R" also, we can piece together a short trip t' of the form

$$A_v,\ B^\wedge, \ldots,\ D_v,\ C\otimes D_v,\ \underline{\quad\quad},\ A_v.$$

Hence $D_v \notin [B^\wedge, B_v]_t$. For similar reasons, $D_v \notin [A\otimes B_v, A\otimes B^\wedge]_t$. So we must have $D_v \in [A^\wedge, A_v]_t$ for all trips t in β with the $C\otimes D$ switch on "L", and for all such trips t, $t(C^\wedge) = t(D_v) + 1$. Hence $D \in (A^\wedge, A_v)_t$ and $C \in (A^\wedge, A_v)_t$ for all trips t with the $C\otimes D$ switch on "L".

For trips in β with the $C\otimes D$ switch on "R", repeat the above argument with C and D exchanged. ■

<u>Corollary 6.0.19</u>:

Let $\frac{A \quad A^\perp}{CUT}$ be any CUT link in a proof net β.

(i) If C is linked to $C^\perp$ in β by an axiom link $\overline{C \quad C^\perp}$ then $C \in eA$ iff $C^\perp \in eA$.

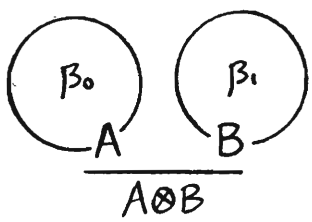
(ii) If $\dfrac{C \quad C^{\perp}}{\text{CUT}}$ is a CUT link in β distinct from $\dfrac{A \quad A^{\perp}}{\text{CUT}}$
then $C \in eA$ iff $C^{\perp} \in eA$.

(iii) If $\dfrac{C \quad D}{C \otimes D}$ is a $\otimes$ link in β
then $C \in eA$ iff $C \otimes D \in eA$, and
$D \in eA$ iff $C \otimes D \in eA$.

(iv) If $\dfrac{C \quad D}{C \parr D}$ is a $\parr$ link in β
then $C \in eA$ and $D \in eA$ iff $C \parr D \in eA$.

(v) If C is an hereditary premis of A in β
then $C \in eA$. ∎

Let $\dfrac{A \quad B}{A \otimes B}$ be a terminal $\otimes$ link in a proof net β. The empires eA and eB are our candidates for the underlying sets of disjoint sub-proof nets β_0 and β_1 such that β is split as follows:



Now if eA contains any part (premis or conclusion) of either an axiom link, a CUT link or a $\otimes$ link other than $\dfrac{A \quad B}{A \otimes B}$ then all the formula occurrences in that link are in eA. The only problem cases are $\parr$ links in β where one premis is in eA and the other premis is in eB so the conclusion is in neither.

<u>Theorem 6.0.20</u>: the Trip Theorem (Girard [1987]).
Let A be a premis of either a CUT link or a $\otimes$ link in a proof net β. Then there is a trip t in β such that

$$eA = (A^{\wedge}, A_{\vee})_t$$

Proof:

Recall that for all trips t in β, $eA \subseteq (A^\wedge, A_\vee)_t$. The theorem asserts the existence of a trip which realizes eA.

The trip t in β is defined as follows. For each $\parr$ link $\frac{C \quad D}{C \parr D}$ such that exactly one premis is in eA (so $C \parr D \notin eA$), if $C \in eA$ then set that $\parr$ switch to "R", and if $D \in eA$ then set that $\parr$ switch to "L".

All other switches in β are set arbitrarily.

Now suppose $E \in (A^\wedge, A_\vee)_t$ but $E \notin eA$. Since $A \in eA$, our supposition means that at some stage after $A^\wedge$ in the interval $[A^\wedge, A_\vee]_t$, we travel from a tramstop of a formula $F \in eA$ to, say, $E_\vee$. So either $t(E_\vee) = t(F^\wedge)+1$ or $t(E_\vee) = t(F_\vee)+1$. What can the link between E and F be? F cannot be $E^\perp$, linked to E by either an axiom link or a CUT link, because in both cases we have $E^\perp \in eA$ iff $E \in eA$. Likewise, F cannot be any part of a $\otimes$ link of which E is a part and F cannot be the conclusion of a $\parr$ link of which E is a premis. The only remaining possibility is that F is a premis of a $\parr$ link of which E is the conclusion, say E is $F \parr G$. But then $G \notin eA$ for otherwise $E \in eA$. So we have exactly one premis of a $\parr$ link in eA. The trip t is defined so that after $F_\vee$ we turn back to $F^\wedge$, never getting to the conclusion $F \parr G = E$. Hence $E \notin (A^\wedge, A_\vee)_t$. ■

Definition 6.0.20:

If β is any proof net then $|\beta|$ is the collection of all formula occurrences in β.

Corollary 6.0.21:

Let $\frac{A \quad B}{A \otimes B}$ be any terminal $\otimes$ link in a proof net β. $|\beta| = eA \cup eB \cup \{A \otimes B\}$ iff there is no $\wp$ link $\frac{C \quad D}{C \wp D}$ in β such that <u>either</u> $C \in eA$ and $D \in eB$ <u>or</u> $C \in eB$ and $D \in eA$.

Proof:

Suppose there is a $\wp$ link $\frac{C \quad D}{C \wp D}$ in β with one premis in each of eA and eB. Then $C \wp D \notin eA$ and $C \wp D \notin eB$, hence $|\beta| \neq eA \cup eB \cup \{A \otimes B\}$.

Conversely, suppose there are no $\wp$ links in β with one premis in each of eA and eB. Then there are no constraints on trips satisfying the Trip Theorem so for <u>all</u> trips t in β, $eA = (A^\wedge, A_\vee)_t$ and $eB = (B^\wedge, B_\vee)_t$. The remaining two tram stops in β are $A \otimes B_\vee$ and $A \otimes B^\wedge$, hence $|\beta| = eA \cup eB \cup \{A \otimes B\}$. ■

Corollary 6.0.22:

Let $\frac{A \quad A^\perp}{\text{CUT}}$ be any CUT link in a proof net β. $|\beta| = eA \cup eA^\perp$ iff there are no $\wp$ links in β with one premis in each of eA and $eA^\perp$. ■

Note that <u>terminal</u> $\wp$ links can give rise to the 'one premis each way' phenomenon (see Examples 6.0.1 (a)) but not all instances of the phenomenon come from terminal $\wp$ links.

Lemma 6.0.22:

If $\frac{A \quad B}{A \otimes B}$ is a terminal $\otimes$ link in a proof net β such that $|\beta| = eA \cup eB \cup \{A \otimes B\}$,
then the proof structures β_0 and β_1 obtained from β by restriction to eA and eB respectively are proof nets.

Proof:

The hypothesis implies that for each trip t in β, $eA = (A^{\wedge}, A_{\vee})_t$ and $eB = (B^{\wedge}, B_{\vee})_t$. Moreover, for all formula occurrences $C \in |\beta|$, $C^{\wedge} \in [A^{\wedge}, A_{\vee}]_t$ iff $C_{\vee} \in [A^{\wedge}, A_{\vee}]_t$, and likewise for $[B^{\wedge}, B_{\vee}]_t$. Let t_0 be any trip in β_0 starting at $A^{\wedge}$. Then t_0 must follow the course of an interval $[A^{\wedge}, A_{\vee}]_t$, for some trip t in β, and then loop back to $A^{\wedge}$ (since A is terminal in eA). Hence t_0 is a long trip. Likewise, all trips t_1 in β_1 are long trips. ■

Corollary 6.0.23:

If $\frac{A \quad A^{\perp}}{CUT}$ is a CUT link in a proof net β such that $|\beta| = eA \cup eA^{\perp}$,
then the proof structures β_0 and β_1 obtained from β by restriction to eA and $eA^{\perp}$ respectively are proof nets. ■

Now we are almost ready to prove the Splitting Theorem; we need one more preparatory lemma.

Lemma 6·0·24: (Girard [1987])
Let A be a premis of either a $\otimes$ link or a CUT link in a proof net β.
If $\frac{C \quad D}{C\otimes D}$ is a $\otimes$ link in β such that $C\otimes D$ is an hereditary premis of A
then $eC \cup eD \subseteq eA$.

Proof:
Let t be a trip in β such that $eA = (A^\wedge, A_\vee)_t$ and the $C\otimes D$ switch is on "L". Then the interval $[A^\wedge, A_\vee]_t$ is of the form

$$A^\wedge, \ldots, C\otimes D^\wedge, D^\wedge, \ldots, D_\vee, C^\wedge, \ldots, C_\vee, C\otimes D_\vee, \ldots, A_\vee$$

Hence $eD \subseteq (D^\wedge, D_\vee)_t \subseteq (A^\wedge, A_\vee)_t = eA$ and likewise, $eC \subseteq eA$. ■

Proof of theorem 6·0·9 (the Splitting theorem)
Let β be a proof net with more than one link but no terminal ⅋ links. Survey the collection of all $\otimes$ links $\frac{A \quad B}{A\otimes B}$ and CUT links $\frac{A \quad A^\perp}{\text{CUT}}$ in β, and choose one such that $eA \cup eH$ is maximal with respect to inclusion, where H is either B or $A^\perp$ depending on the case.

If a $\otimes$ link $\frac{A \quad B}{A\otimes B}$ has been chosen, then we claim $A\otimes B$ is terminal in β. Suppose otherwise. Then there must be either a terminal $\otimes$ link $\frac{C \quad D}{C\otimes D}$ or else a CUT link $\frac{C \quad C^\perp}{\text{CUT}}$ such that $A\otimes B$ is an hereditary premis of, say, C. By Lemma 6·0·24, we have $eA \cup eB \subseteq eC$, Hence $eA \cup eB \subseteq eC \cup eD$ or $eA \cup eB \subseteq eC \cup eC^\perp$, contradicting the assumption of maximality.

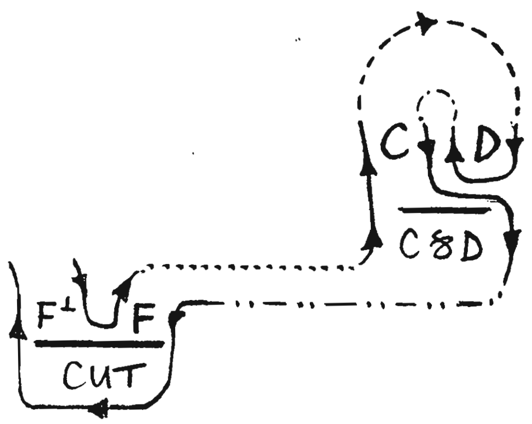
If a CUT link $\frac{A \quad A^{\perp}}{CUT}$ has been chosen, then it is necessarily a terminal link of β.

Assume a $\otimes$ link has been chosen; the argument for a CUT link with $eA \cup eA^{\perp}$ maximal can be extracted from what follows.

Now suppose that $eA \cup eB \cup \{A \otimes B\} \neq |\beta|$. Then, by Lemma 6.0.21, there is a $\parr$ link $\frac{C \quad D}{C \parr D}$ such that either $C \in eA$ and $D \in eB$ or else $C \in eB$ and $D \in eA$. Now $C \parr D$ must be an hereditary premis of one of the premises of either a CUT link or a terminal $\otimes$ link. For definiteness, let $C \parr D$ be an hereditary premis of F in $\frac{F^{\perp} \quad F}{CUT}$. By Corollary 6.0.19, we have $C \parr D \in eF$, $C \in eF$ and $D \in eF$. So this $\parr$ link puts no constraint on trips satisfying the Trip Theorem with respect to eF.

Suppose $C \in eA$ and $D \in eB$. Now we can choose a trip t in β such that $eF = (F^{\wedge}, F_{\vee})_t$ and $eB = (B^{\wedge}, B_{\vee})_t$; in particular, the $C \parr D$ switch is on "L". By Lemma 6.0.12, the interval $[F^{\wedge}, F_{\vee}]_t$ is of the form

$$F^{\wedge}, \dots, C \parr D^{\wedge}, C^{\wedge}, \dots, D_{\vee}, D^{\wedge}, \dots, C_{\vee}, C \parr D_{\vee}, \dots, F_{\vee}.$$



The we must have $B^{\wedge}$ between $C^{\wedge}$ and $D_{\vee}$, and $B_{\vee}$ between $D^{\wedge}$ and $C_{\vee}$. Hence $eB = (B^{\wedge}, B_{\vee})_t \subseteq (F^{\wedge}, F_{\vee})_t = eF$.

By interchanging C and D we get $eA \subseteq eF$.
Hence $eA \cup eB \subseteq eF \cup eF^{\perp}$, contradicting maximality.

So we must have $e_A \cup e_B \cup \{A \otimes B\} = |\beta|$. And by Lemma 6·0·22, the $\otimes$ link $\frac{A \quad B}{A \otimes B}$ splits β, as required. ∎

6·1 Normalization in PNO

Normalization in **PNO** is quite quick and painless.

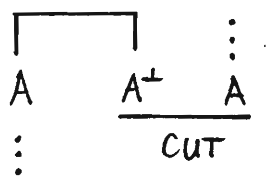
Definition 6·1·0:
Let β be a proof net in **PNO**.
We say β is normal iff β contains no CUT links.
β converts to a proof structure β', written $\beta \text{ con } \beta'$, when one of the following cases holds:

(i) axiom conversion (AC):
β' is obtained from β by replacing a configuration of the form

(ii) multiplicative symmetric conversion ($\otimes/\wp$ -SC):
β' is obtained from β by replacing a configuration of the form

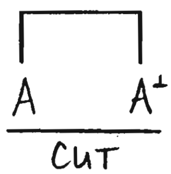
Observe that for any proof net β, there is a β' such that β con β' iff β contains at least one CUT link.

The axiom conversion scheme (AC) may appear too restrictive: We seem to have omitted from consideration configurations of the form



But recall that axiom links can only have <u>literals</u> as their conclusions (Definition 6·0·0). So whenever we have a CUT against the conclusion of an axiom link, the other premis of the CUT link must also be a literal.

We can also ignore configurations of the form



Since such proof structures are not proof nets ((c) in Examples 6·0·4).

<u>Definition 6·1·1:</u>
Let β be a proof net in PNO containing p formula occurrences. The size of β, $s(\beta) = p$.

We have yet to verify that when β is a proof net and β con β' then β' is a proof <u>net</u>.

Lemma 6·1·2:

If β is a proof net in **PNO** and β con β' then β' is a proof net with the same terminal formula occurrences as β and $s(\beta') < s(\beta)$.

Proof:

(i) Suppose β con β' by the axiom conversion scheme (AC). Each (long) trip in β is of the form

$$A^\wedge,\ \underline{A}^\perp{}_\vee,\ \underline{A}^\wedge,\ A^\perp{}_\vee,\ \ldots,\ A^{\perp\wedge},\ \underline{A}_\vee,\ \underline{A}^{\perp\wedge},\ A_\vee,\ ---,\ A^\wedge$$

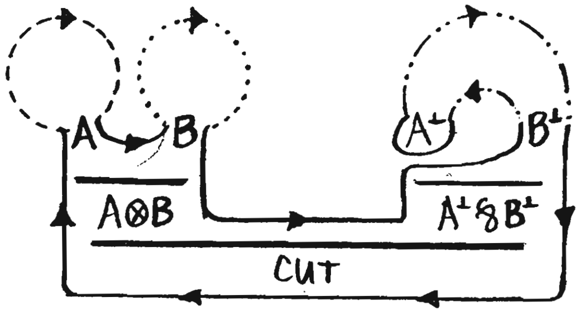
where $\underline{A}$ (respectively, $\underline{A}^\perp$) denotes the occurrence of the formula A ($A^\perp$) which is a premis of the CUT link under examination. By identifying the two occurrences of A and the two occurrences of $A^\perp$, we obtain a long trip in β' of the form

$$A^\wedge,\ A^\perp{}_\vee,\ \ldots,\ A^{\perp\wedge},\ A_\vee,\ ---,\ A^\wedge$$

But every trip in β' is of this form, so β' is a proof net. If $s(\beta) = p$ then $s(\beta') = p-2$.

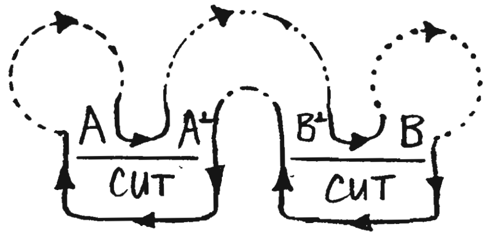
(ii) Suppose β con β' by the scheme ($\otimes/⅋ - sc$). Arbitrarily select positions for all the switches in β'. This induces a switch configuration for all the switches in β except for the switches for the $\otimes$ link and the ⅋ link removed by this conversion. Suppose both those switches are on "R". (the argument is similar for the other three combinations.) By Lemmas 6·0·11 and 6·0·12, the trip t in β starting at $A^\wedge$ is of the form

$$A^\wedge,\ ---,\ A_\vee,\ B^\wedge,\ \ldots,\ B_\vee,\ A\otimes B_\vee,\ (A^\perp ⅋ B^\perp)^\wedge,\ B^{\perp\wedge},\ ----,\ A^\perp{}_\vee,$$
$$A^{\perp\wedge},\ ---,\ B^\perp{}_\vee,\ (A^\perp ⅋ B^\perp)_\vee,\ A\otimes B^\wedge,\ A^\wedge$$



Hence the trip t' in β' determined by the given configuration of switches in β' must be of the form

$$A^\wedge, ---, A_v, A^{\perp\wedge}, -\cdot\cdot-\cdot\cdot-, B^\perp v, B^\wedge, \ldots, B_v, B^{\perp\wedge}, -\cdot-\cdot-, A^\perp v, A^\wedge$$



Since t is a long trip, so is t'. Hence β' is a proof net. If $s(\beta) = p$ then $s(\beta') = p-2$. ■

<u>Definition 6·1·3:</u>
Let β and β' be proof nets.
We say β <u>reduces</u> to β', denoted $\beta \rightsquigarrow \beta'$, if there is a sequence of conversions

$$\beta = \beta_0 \text{ con } \beta_1 \text{ con } \ldots \text{ con } \beta_{n-1} \text{ con } \beta_n = \beta'$$

from β to β'. (So the relation $\rightsquigarrow$ is the transitive closure of con.) Such a sequence of conversions is called a <u>reduction sequence</u> from β to β' of length n ($n \geq 0$; $n=0$ when $\beta = \beta'$). We use the notation $\beta \rightsquigarrow_n \beta'$ to indicate the existence of a reduction sequence from β to β' of length n.

A proof net β is <u>weakly normalizable</u> iff for some $n<\omega$ and some β' which is normal, $\beta \rightsquigarrow_n \beta'$.
In this case, we say β' is a <u>normal form</u> for β.
For each proof net β, define

$$L(\beta) \overset{df}{=} \sup\{n \mid \exists\beta' (\beta \rightsquigarrow_n \beta')\}.$$

A proof net β is <u>strongly normalizable</u> iff $L(\beta) < \omega$.

If every reduction sequence starting from a given proof net β is of bounded length, then every reduction sequence starting from β can be extended to one whose final term is normal. And conversely.

A proof net β may fail to be strongly normalizable if there is a sequence of conversions starting from β such that the conversions do not decrease the size of the proof nets involved; in particular, if there is a 'loop' $\beta \rightsquigarrow \beta' \rightsquigarrow \beta'' \rightsquigarrow \beta' \rightsquigarrow \beta'' \rightsquigarrow \ldots$ where β' and β'' are not normal. Such things do not happen in **PNO**.

<u>Proposition 6.1.4</u>: (Girard [1987])
The relation $\rightsquigarrow$ on **PNO** has the Church-Rosser property. That is, if $\beta \rightsquigarrow \beta_0$ and $\beta \rightsquigarrow \beta_1$ then there is some β' such that $\beta_0 \rightsquigarrow \beta'$ and $\beta_1 \rightsquigarrow \beta'$. ■

We omit the proof; it is fairly straightforeward but messy. If one contemplates for a moment the conversion schemes (AC) and ($\otimes/⅋$-SC) then one readily forms the belief that the order of any two conversions can be swapped without altering the final result.

<u>Theorem 6·1·5:</u> (Girard [1987])
Every proof net in **PNO** is strongly normalizable and has a unique normal form.

<u>Proof:</u>
Let β be a proof net in **PNO** and suppose $s(\beta)=p$. Suppose $\beta \rightsquigarrow_n \beta'$. By Lemma 6·1·2, $n < s(\beta)$. Hence $L(\beta) < s(\beta)$. If β' and β'' are two normal forms for β then by Proposition 6·1·4, $\beta' = \beta''$. ∎

In the last part of Section 5 we announced the result that if $\beta \rightsquigarrow \beta_0$ then $\beta^* = \beta_0^*$. We could verify this for **PNO** now: we would have to find a proof π in **LLM** such that $\beta = N(\pi)$, mimick the conversions in **LLM** to obtain a π_0 such that $\beta_0 = N(\pi_0)$ and then check that $\pi^* = \pi_0^*$ (cf. the discussion following Observation 5·3·1). We could, but we won't. The normalization of proof nets is a 'bottom-up' procedure: we push cuts upwards until we get to axiom links at the top, then get rid of the cuts altogether. Inductively defining π^* for a proof π, and derivatively, β^* for a proof net β, is a 'top-down' process. In Section 6·3, after we have developed the full system of proof nets **PN!** adequate for **LL!**, we shall present Girard's alternative 'bottom-up' characterization of β^*. Then in Section 6·4, where we set out the normalization procedure for **PN!**, we shall confirm that when $\beta \rightsquigarrow \beta_0$ then $\beta^* = \beta_0^*$.

6·2 Axiom boxes and PNT

Our task is to extend **PNO** so as to obtain systems of proof nets adequate for **LL** and **LL!**. Now a cheap way of extending a sequent calculus or a natural deduction system is by adding new axiom schemes. Can we do that with proof nets?

Definition 6·2·0:
A axiom box is a link of the form

$$\boxed{A_1 - A_2 - \cdots - A_n}$$

where $A_1, \ldots, A_n$ are formulae in the language $\mathcal{L}_!$ of modal linear logic, $n \geqslant 1$. $A_1, \ldots, A_n$ are the conclusions of such a link; there are no premises.
A proof$^+$ structure is an object consisting of occurrences of formulae of $\mathcal{L}_!$ and links between these occurrences of formulae. In addition to axiom links, CUT links, $\otimes$ links and $⅋$ links, we also allow axiom boxes to link formula occurrences. With each axiom box with n conclusions, $n \geqslant 1$, we associate a switch with $(n-1)!$ positions. Each position of the switch corresponds to an n-cycle σ in the permutation group S_n. When the switch is set at σ, tram trips t satisfy the following condition:

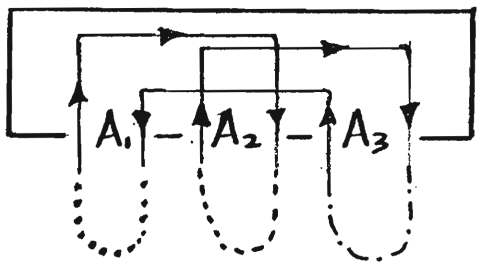
$$\text{for } i = 1, \ldots, n, \quad t(A_{\sigma(i)}\vee) = t(A_i\wedge) + 1$$

where $A_1, \ldots, A_n$ are the conclusions of the given axiom box.
A proof$^+$ net is a proof$^+$ structure which admits no short trips. Let **PNO$^+$** denote the collection of all proof$^+$ nets.

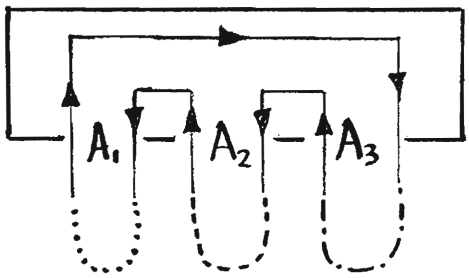
<u>Examples 6·2·1</u>:

(i) Axiom links $A \quad A^{\perp}$ are axiom boxes; the switch has <u>one</u> position.

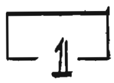
(ii) The switch associated with an axiom box with three conclusions has two positions: the 3-cycles (123) and (132). When $\sigma = (123)$, <u>long</u> trips are as follows.



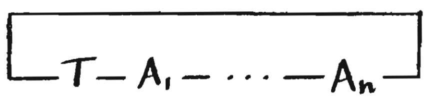
When $\sigma = (132)$, <u>long</u> trips are as follows.



(iii) We are particularly interested in the axiom box with one conclusion



and a switch with $0! = 1$ position, and axiom boxes of the form



which have a switch with $n!$ positions.

In our definition of proof$^+$ structures, we allow <u>any</u> formula of $\mathcal{L}_!$ to be a conclusion of an axiom box. So corresponding to **PNO$^+$**, we have the sequent calculus **LLM$^+$** which is obtained from **LLM** by adjoining infinitely many axioms, one for each sequence of formulae of $\mathcal{L}_!$.

<u>Theorem 6·2·2</u>: (Girard [1987])
If π is a proof of $\vdash A_1, \ldots, A_n$ in **LLM$^+$** then we can naturally associate with π a proof$^+$net $N^+(\pi)$ in **PNO$^+$** whose terminal formula occurrences are exactly $A_1, \ldots, A_n$

<u>Proof</u>:
Modify the proof of Theorem 6·0·6 in the obvious way. ■

<u>Theorem 6·2·3</u>: (Girard [1987])
The map N^+ : **LLM$^+$** $\rightarrow$ **PNO$^+$** is surjective.

<u>Proof</u> (sketch):
We have to show that the empires eA retain their nice properties (Lemma 6·0·18 and Corollary 6·0·19) when axiom boxes are admitted. In particular, we have to ensure that when A is a premis of either a CUT link or a $\otimes$ link in a proof net β in **PNO$^+$**, and C_i and C_j are two conclusions of an axiom box

$$\boxed{C_1 - \cdots - C_n}$$

in β, then $C_i \in eA$ iff $C_j \in eA$. This follows from the fact that any long trip t in β can be expressed as the disjoint union of the intervals $[C_{i\vee}, C_i^{\wedge}]_t$ for $i=1,\dots,n$. (Look again at (ii) in Examples 6.2.1.). Other than this, the rest of the results leading up and including the Splitting Theorem go through almost unchanged. ∎

Of course, the system **PNO$^+$** (and **LLM$^+$**) is not terribly interesting; its purpose is only to record the fact that axiom boxes work.

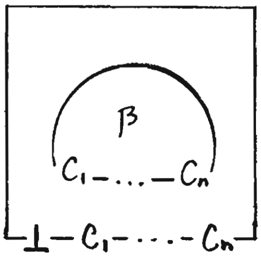
If one scrutinizes the inference rules of the sequent calculus **LL!** then, after a few moments reflection, one will notice that the rules (FST $\oplus$), (SND $\oplus$), (D?) and (C?) are easily mimicked as links. This is because these rules, like ($\otimes$), ($\&$) and (CUT), place no restriction on the parametric sequences (or 'contexts', as Girard calls them) occurring in the premis sequents, and whatever parametric sequences there are reappear without change in the conclusion sequent. Now we have just established that the axioms and axiom schemes of **LL!** can be mimicked as axiom boxes. So this leaves four inference rules to be accounted for. They pose two distinct sorts of problems:

I. the 'nothing to link on to' problem:
 the rules ($\perp$) and (Th?); and

II. the 'global constraint' problem:
 the rules ($\&$) and (!).

Girard deals with the four rules uniformly with a device called a <u>proof box</u>. A proof box is like an axiom box except that it has one or more proof nets <u>inside</u> it. Proof boxes are a source of complication when it comes to the normalization procedure. As Girard puts it, they are '... moments where we restore the sequent (i.e. the sequential!) structure. Their use is therefore a bridle to parallelism.' (Girard [1987], p.43) Proof boxes also make a mess of tram networks.

Girard's strategy for dealing with the rule ($\perp$) is as follows. From a proof net β with terminals $C_1, \ldots, C_n$, form a proof net β' with terminals $\perp, C_1, \ldots, C_n$ as illustrated:



To mimick the rule (Th?), replace '$\perp$' with '?A' where A is any formula of $\mathcal{L}$:

The problem with the rules ($\perp$) and (Th?) is that they 'create' a new formula out of nothing (which is just to say, they involve <u>thinning</u>) so there is no premis formula to 'link' on to. But with regard to parametric sequences, they make no demands and are perfectly conservative. We cannot 'tack on' a $\perp$ or a ?A at the bottom of a proof net (or structure) but we <u>can</u> use axiom boxes so that all our thinning business is done at the top. In what follows, we part company with Girard and abandon the use of proof boxes to mimick the rules ($\perp$) and (th?). (Girard [1987], p. 47, does remark that the proof boxes for thinning '... seem of very limited interest.')

Definition 6·2·4:

A new proof structure is an object consisting of occurrences of formulae of $\mathcal{L}_!$ and links between these occurrences of formulae. The links are of the following kinds:

(1) axiom boxes:

(1·1) generalized axiom link: $k+m+2$ conclusions; $k \geq 0, m \geq 0$.

$$\boxed{\perp - \cdots - \perp - ?A_1 - \cdots - ?A_m - C - C^\perp}$$

where k of the conclusions are occurrences of $\perp$, $A_1, \ldots, A_m$ are any formulae of $\mathcal{L}_!$ and C and $C^\perp$ are atomic formulae of $\mathcal{L}_!$.

(1·2) $\mathbb{1}$ axiom box: $m+1$ conclusions; $m \geq 0$.

$$\boxed{\mathbb{1} - ?A_1 - \cdots - ?A_m}$$

where $A_1, \ldots, A_m$ are any formulae of $\mathcal{L}_!$.

(1·3) $\top$ axiom box: $m+1$ conclusions; $m \geq 0$.

$$\boxed{\top - A_1 - \cdots - A_m}$$

where $A_1, \ldots, A_m$ are any formulae of $\mathcal{L}_!$.

(2) unary links:

(2.1) FST $\oplus$ link: $\dfrac{A}{A \oplus B}$

(2.2) SND $\oplus$ link: $\dfrac{B}{A \oplus B}$

(2.3) D? link: $\dfrac{A}{?A}$

(3) binary links:

(3.1) CUT link: $\dfrac{A \quad A^{\perp}}{CUT}$

(3.2) $\otimes$ link: $\dfrac{A \quad B}{A \otimes B}$

(3.3) $⅋$ link: $\dfrac{A \quad B}{A ⅋ B}$

(3.4) C? link: $\dfrac{?A \quad ?A}{?A}$

We also require that

(i) every occurrence of a formula in a new proof structure is the conclusion of exactly one link; and

(ii) every occurrence of a formula in a new proof structure is the premis of at most one link.

Definition 6.2.5:

Tram trips in a new proof structure are defined Component-wise.

(1) The scheduling of trips through axiom boxes is as specified in Definition 6.2.0.

(2) Tram tracks in the vicinity of a unary link are as follows.

The tracks are such that every trip t satisfies
(i) $t(A^{\wedge}) = t(C^{\wedge})+1$, and
(ii) $t(C_{\vee}) = t(A_{\vee})+1$.

(3) The scheduling of trips through CUT links, $\otimes$ links and ⅋ links is as specified in Definition 6·0·3. The scheduling of trips through C? links follows the same pattern as for ⅋ links.

A new proof structure is a <u>new proof net</u> iff it does not admit any short trips. Let **PNT** denote the collection of all new proof nets.

Now that we have got through the definitions, we can drop the modifier 'new'; until further notice, 'proof net' will mean an element of **PNT**. (The 'T' is for 'temporary' and also for 'trams'.) Let **LLT** denote the (admittedly unnatural) subsystem of **LL!** obtained from **LL!** by omitting the rules (&) and (!).

<u>Theorem 6·2·6:</u>
If π is a proof of $\vdash A_1, \ldots, A_n$ in **LLT**
then we can naturally associate with π a proof net $N(\pi)$ in **PNT** whose terminal formula occurrences are exactly $A_1, \ldots, A_n$.

<u>Proof</u>:

The only cases involving any novelty are those of the rules $(\perp)$ and $(Th?)$.

(i) Suppose π is obtained from π_0 by the rule $(\perp)$:

$$\frac{\vdash B_1, \dots, B_n}{\vdash \perp, B_1, \dots, B_n} (\perp)$$

Assume we have a proof net $\beta_0 = N(\pi_0)$ with terminals $B_1, \dots, B_n$. We construct a proof structure β from β_0 as follows.

If β_0 has a generalized axiom link

$$\perp^k - ?\Gamma - C - C^\perp$$

then replace that link with

$$\perp - \perp^k - ?\Gamma - C - C^\perp .$$

If β_0 has more than one generalized axiom link, choose the one that contains an hereditary premis of B_i for the <u>least</u> i (with respect to the ordering $B_1, \dots, B_n$).

Otherwise, if β_0 has a $\mathbb{1}$ axiom box

$$\mathbb{1} - ?\Gamma$$

then replace that box with the generalized axiom link

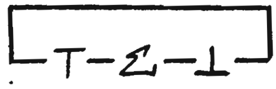
$$?\Gamma - \mathbb{1} - \perp .$$

(This is why we have atomic formulae of $\mathcal{L}$: rather than literals in the 'old axiom link' position.) If there is more than one $\mathbb{1}$ axiom box, choose as above.

Otherwise β_0 must contain a $\top$ axiom box, say

$$\top - \Sigma$$

If there is more than one $\top$ axiom box, choose as above. Replace that box with



Let t be any trip in the proof structure β obtained from β_0 by the above procedure. Then t is the same as some trip t_0 in β_0, except for the extra segment of t around the new terminal $\bot$. It is clear that t must be a long trip if t_0 is.

(ii) Suppose π is obtained from π_0 by the rule (Th?):

$$\frac{\vdash B_1, \ldots, B_n}{\vdash ?A, B_1, \ldots, B_n}\ (\mathrm{Th}?)$$

Assume we have a proof net $\beta_0 = N(\pi_0)$ with terminals $B_1, \ldots, B_n$. We construct a proof structure β from β_0 by 'inserting a $?A$', following a procedure analogous to the one described in (i). And as above, β will be a proof net. ■

<u>Theorem 6.2.7</u>:
The map N: **LLT** $\longrightarrow$ **PNT** is surjective.

<u>Proof</u> (sketch):
If β in **PNT** consists of an axiom box then choose any one of the equivalent-up-to-exchanges proofs in **LLT** of the appropriate sequent.
Suppose β contains more than one link. We can readily deal with the cases where β contains a terminal unary link or a terminal $\otimes$ or C? link. This leaves us with the hypothesis that all the

terminal links in β are either CUT links or $\otimes$ links. It is clear that if A is a premis of either a CUT link or $\otimes$ link then (i) the premis of a unary link is in eA iff the conclusion is, and (ii) the conclusion of a C? link is in eA iff <u>both</u> premises are. We have to modify the trip specified in the proof of the Trip Theorem (6.0.20) so as to deal with the case when exactly one premis of a C? link is in eA, in addition to the case when exactly one premis of a $\wp$ link is in eA. Provided we always allow for this new possibility, the proof of the Splitting Theorem goes through. ■

In the same way as was noted in Observation 6.0.10, we can define β^*, for β in **PNT**, in terms of π^*, where $\beta = \mathbf{N}(\pi)$.

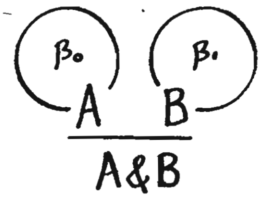
6.3 Proof boxes and PN!

The rules (&) and (!) of **LL!** both involve a <u>global</u> constraint which is antithetical to the spirit of localism inherent in proof nets as developed so far. For these rules, the use of proof boxes seems unavoidable.

In Chapter 6 of Girard [1987], some tentative (and inconclusive) suggestions are given regarding the avoidance of & proof boxes by working instead with families of proof structures called <u>slices</u>.

Another approach might be to have a binary link corresponding to the rule of adjunction used in Hilbert-style formulations of relevance logics (see Avron [1988]). It would be as follows:

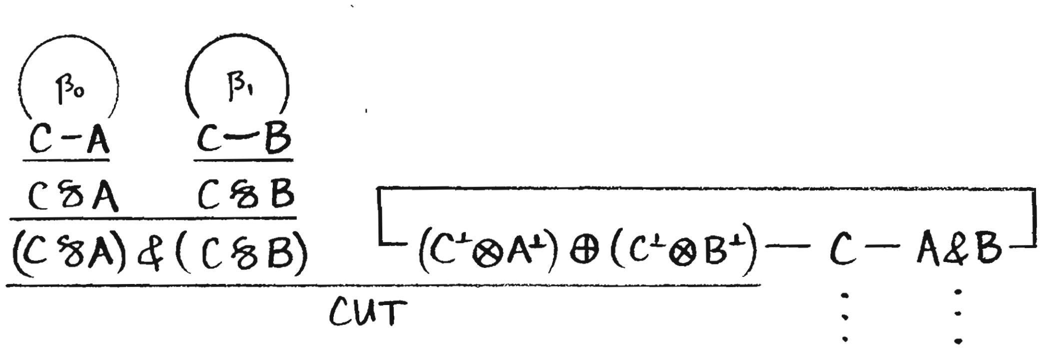
if β_0 and β_1 are proof nets with A and B, respectively, as their <u>sole</u> terminal formulae, then form a proof net as illustrated.



All other instances of the sequent calculus rule (&) would have to be captured using appropriate axiom boxes. Now in a Hilbert-style system, we make use of the axiom scheme

$$((C \multimap A) \& (C \multimap B)) \multimap (C \multimap (A \& B))$$

by deriving an instance of the antecedent using the rule of adjunction and then applying Modus Ponens. To do the same in the context of proof nets would involve <u>essential</u> and <u>ineliminable</u> CUT's against axiom boxes.

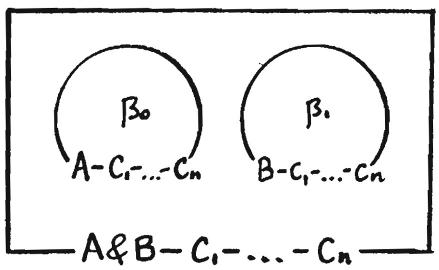


Finding the alternatives unsatisfactory, we resign ourselves to proof boxes.

<u>Definition 6.3.0:</u>
The system of proof nets **PNI!** is defined inductively as follows.

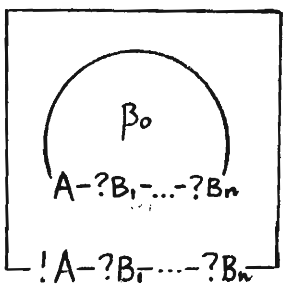
(i) If β is a proof net in **PNT** then β is a proof net in **PNI!**.

(ii) If β_0 and β_1 are proof nets in **PNI!** with terminal formulae $A, C_1, \ldots, C_n$ and $B, C_1, \ldots, C_n$ respectively then β is a proof net in **PNI!** with terminal formulae $A\&B, C_1, \ldots, C_n$, where β is as illustrated:



In this case, β is called an <u>&-proof box</u>.

(iii) If β_0 is a proof net in **PNI!** with terminal formulae $A, ?B_1, \ldots, ?B_n$ then β is a proof net in **PNI!** with terminal formulae $!A, ?B_1, \ldots, ?B_n$, where β is as illustrated:



In this case, β is called a <u>!-proof box</u>.

The system of proof nets **PNI** is obtained from **PNI!** by omitting clause (iii) above, disallowing D? links and C? links, setting $m=0$ in generalized axiom links and $\mathbb{1}$ axiom boxes (where m is the number of formulae of the form ?A) and restricting all links to occurrences of formulae of $\mathcal{L}$.

An &-or !-proof box in a proof net acts as an impermeable barrier between the proof nets or net inside and the rest of the proof net of which the box is a part. In the region of a proof net <u>outside</u> all of the proof boxes of the net, the concept of a trip still makes sense. From this perspective, the conclusions of proof boxes look and behave as if they were conclusions of axiom boxes, and all other links in the region behave as they do in **PNT**. Likewise, in the region of a proof net inside a proof box but outside any other proof box, the concept of a trip still makes sense. And an innermost region of a proof net in **PNI!**, i.e. a region no part of which is outside any proof box, is just a proof net in **PNT**. So we can have lots of <u>partial</u> trips in a proof net in **PNI!** but travelling from the inside of a proof box to the outside, or vice-versa, is impossible.

It is possible to give something like a long trip characterization of proof nets in **PNI!**: partial trips in each of the unconnected regions are long, relative to the region.

Theorem 6·3·1:

If π is a proof of $\vdash A_1, \ldots, A_n$ in **LL!**
then we can naturally associate with π a proof net $N(\pi)$ in **PNI!** whose terminal formula occurrences are exactly $A_1, \ldots, A_n$.

Proof:

If the last rule used in π is either (&) or (!) then the proof net $N(\pi)$ falls out of Definition 6·3·0. ■

Theorem 6·3·2:

The map N: **LL!** $\longrightarrow$ **PNI!** is surjective.

Proof (sketch):

If β is either an &-proof box or a !-proof box then the proof π such that $\beta = N(\pi)$ comes directly from the proofs or proof given by the induction hypothesis by either (&) or (!).

Again, we are reduced to the case where all the terminal links of β are either CUT links or $\otimes$ links. Now we can work just in the outermost region of β, considering all proof boxes which border the region as axiom boxes. Then proceed as in the proofs of the corresponding results for **PNO**$^+$ and **PNT**. ■

As before, we define β^* for β in **PNI!** in terms of π^*, where $\beta = N(\pi)$.

As we noted earlier, this 'top-down' inductive definition of β^* is less than optimal for use in the context of the normalization process. We now present Girard's alternative 'bottom-up' characterization of β^*, modified to suit our variant treatment of $(\perp)$ and (th?).

<u>Definition 6·3·3:</u>

Let β be a proof net in PN1! and fix an ordering, say $C_1, \ldots, C_n$, on the terminal formula occurrences of β.

A <u>basis for an experiment</u> in β is a sequence $\underset{\sim}{w} = (w_1, \ldots, w_n)$ such that $w_i \in |C_i|$ for $i = 1, \ldots, n$.

An <u>experiment</u> in β consists of the allocation of one or more elements $x \in |A|$, for each occurrence of a formula A in β, according to the following procedure.

(i) Arbitrarily select a basis $\underset{\sim}{w} \in |C_1 \mathbin{⅋} \ldots \mathbin{⅋} C_n|$.

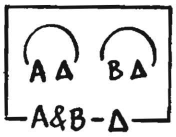
(ii) For each CUT link $\frac{A \quad A^\perp}{\mathrm{CUT}}$ in β, arbitrarily select an element $x \in |A| = |A^\perp|$; we consider this x to be allocated to both A and $A^\perp$.

(iii) If $\frac{A \quad B}{A \otimes B}$ is any $\otimes$ link in β and we have already allocated $z = (x, y) \in |A \otimes B|$, then allocate $x \in |A|$ and $y \in |B|$.

(iv) If $\frac{A \quad B}{A ⅋ B}$ is any ⅋ link in β and we have already allocated $z = (x, y) \in |A ⅋ B|$, then allocate $x \in |A|$ and $y \in |B|$.

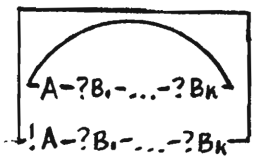
(v) If $\frac{A}{A \oplus B}$ is any FST $\oplus$ link in β and we have already allocated $z \in |A \oplus B|$, then if $z = (0, x)$, allocate $x \in |A|$ but if $z = (1, y)$ then <u>abandon</u> the experiment.

(vi) If $\frac{B}{A\oplus B}$ is any SND$\oplus$ link in β and we have already allocated $z \in |A\oplus B|$, then if $z=(1,y)$, allocate $y \in |B|$, but if $z=(0,x)$ then abandon the experiment.

(vii) If  is any &-proof box in β and we have already allocated $z \in |A\& B|$ and $\underset{\sim}{u} \in |\Delta|$, then if $z=(0,x)$, allocate $x \in |A|$ and $\underset{\sim}{u} \in |\Delta|$, and if $z=(1,y)$, allocate $y \in |B|$ and $\underset{\sim}{u} \in |\Delta|$.

(viii) If $\frac{A}{?A}$ is any D? link in β and we have already allocated $a \in |?A|$, then if $a=\{x\}$, allocate $x \in |A|$, but if a is not a singleton then abandon the experiment.

(ix) If $\frac{?A \quad ?A}{?A}$ is any C? link in β and we have already chosen $a \in |?A|$, then arbitrarily choose a decomposition $a = a' \cup a''$ and allocate $a' \in |?A|$ for the left premis and $a'' \in |?A|$ for the right premis.

(x) Let  be any !-proof box in β and suppose we have already allocated $a \in |!A|$ and $b_j \in |?B_j|$ for $j=1,\ldots,k$. Now $a=\{x_1,\ldots,x_m\}$ for some $m \geq 0$. For each $j=1,\ldots,k$, arbitrarily choose a decomposition $b_j = b_{1j} \cup \ldots \cup b_{mj}$. Then for each $i=1,\ldots,m$, allocate $x_i \in |A|$ and $\underset{\sim}{z}_i = (b_{i1},\ldots,b_{ik}) \in |?B_1,\ldots,?B_k|$.

In addition to the circumstances already specified, an experiment is to be abandoned if at any stage in the allocation process, we arrive at an occurrence of a formula A such that $|A| = \emptyset$; in particular, if the proof net contains either $\top$ or $\mathbb{O}$.

An experiment in β is <u>completed</u> when, for each occurrence of a formula A in β, at least one element $x \in |A|$ has been allocated. If an experiment is abandoned then it cannot be completed.

A completed experiment in β is <u>successful</u> iff (1) for each generalized axiom link in β,

$$\boxed{\perp^k - ?A_1 - \cdots - ?A_m - C - C^\perp}$$

if $(@, \ldots, @, a_1, \ldots, a_m, x, x')$ has been allocated then $a_i = \emptyset$ for $i = 1, \ldots, m$ and $x = x'$; and

(2) for each $\mathbb{1}$ axiom box in β,

$$\boxed{\mathbb{1} - ?A_1 - \cdots - ?A_m}$$

if $(@, a_1, \ldots, a_m)$ has been allocated then $a_i = \emptyset$ for $i = 1, \ldots, m$.

(End of definition 6.3.3)

<u>Theorem 6.3.4</u> : (Girard [1987])

Let β be a proof net in **PN1!** and let $C_1, \ldots, C_n$ be an ordered list of the terminal formula occurrences of β. Write $C_1, \ldots, C_n$ as Γ. Then

$$\beta^* = \{ \underset{\sim}{w} \in |\Gamma| \mid \underset{\sim}{w} \text{ is a basis for a successful experiment in } \beta \}.$$

<u>Proof</u> (sketch):

Suppose $\underset{\sim}{w} \in |\Gamma|$ is a basis for a successful experiment in β. This means that whenever β_0 is a generalized axiom link with conclusions $\perp^k, ?\Sigma, C, C^\perp$ and $\underset{\sim}{z} \in |\perp^k, ?\Sigma, C, C^\perp|$ is one of the sequences allocated on the basis of $\underset{\sim}{w}$, we have $\underset{\sim}{z} \in \beta_0^*$. And likewise whenever β_0 is a $\mathbb{1}$ axiom box. Since $\underset{\sim}{w}$ is a basis for a successful experiment in

β, there can be no $\top$ axiom boxes in β. So $\underset{\sim}{w}$ determines correct sequences for all the axiom boxes in β. By following the course of these sequences through the 'top-down' inductive definition of β^* (via the appropriate π^*, where $\beta = N(\pi)$) we see that $\underset{\sim}{w} \in \beta^*$.

Conversely, if $\underset{\sim}{w} \in \beta^*$ then it is immediate that $\underset{\sim}{w}$ is a basis for a successful experiment in β. Note that if $\underset{\sim}{w} \in \beta^*$ then $\beta^* \neq \emptyset$, hence β cannot contain any $\top$ axiom boxes. When β does contain a $\top$ axiom box, there are no successful experiments so the set of all bases for successful experiments in β is empty.

To ensure that we have identical <u>subgraphs</u> of the web $W(\Gamma)$ and not just identical <u>sets</u>, we have to establish that

$$\{ \underset{\sim}{w} \in |\Gamma| \mid \underset{\sim}{w} \text{ is a basis for a successful experiment in } \beta \}$$

is a <u>coherent</u> subset of $|\Gamma|$. The result is proved for proof nets β in **PNO** in Girard [1987] (Theorem 3·18). The difficulties are concentrated in the multiplicative subsystem; in comparison, the extension to **PN1!** is fairly straightforeward. ■

6.4 Normalization in PNI!

In what follows, we shall define a number (twelve, to be precise) of conversion schemes. We say β converts to β', written $\beta \text{ con } \beta'$, iff the transition from β to β' is an instance of one of these schemes. The definitions of the other terms appropriate to the discussion of normalization carry over from Section 6.1.

For all but one of the conversion schemes, the size of the resulting proof net is strictly smaller than the size of the original. The troublesome case is when one premis $!A$ of a CUT link is a conclusion of a ! proof box and the other premis $?A^{\perp}$ is the conclusion of a C? link; the required conversion produces an exponential growth in size.

Definition 6.4.0:

We say a proof net β in PNI! is built from boxes $\square_1, \ldots, \square_n$ and formula occurrences $A_1, \ldots, A_k$ by means of the unary and binary links iff (1) each $\square_i$, $i=1,\ldots,n$, is either an axiom box or a proof box which is not inside any other box, and $\square_1, \ldots, \square_n$ is an exhaustive list of all such boxes, and (2) each A_j, $j=1,\ldots,k$, is the conclusion of either a unary or a binary link and is not inside any proof box, and $A_1, \ldots, A_k$ is an exhaustive list of such formula occurrences. (So the conclusions of an outermost box are not counted.)

The size $s(\beta)$ of a proof net β is defined by induction on the build-up of β as follows:

(i) if β is built from boxes $\square_1,\ldots,\square_n$ and formula occurrences $A_1,\ldots,A_k$ by means of the unary and binary links, then

$$s(\beta) = s(\square_1)\cdot\ldots\cdot s(\square_n)\cdot 2^k.$$

(ii) if β is a (proof or axiom) box then the size of β is defined as follows:

- if β is a generalized axiom link with $k+m+2$ conclusions (as in Definition 6.2.4), then $s(\beta) = k+m+3$;
- if β is a $\mathbb{1}$ axiom box with $m+1$ conclusions (as in Definition 6.2.4) then $s(\beta) = m+2$;
- if β is a $\top$ axiom box with $m+1$ conclusions (as in Definition 6.2.4) then $s(\beta) = m+2$;
- if β is an &-proof box formed from proof nets β_0 and β_1 then $s(\beta) = s(\beta_0) + s(\beta_1) + 1$;
- if β is a !-proof box formed from a proof net β_0 then $s(\beta) = s(\beta_0) + 1$.

To distinguish between the different sorts of conclusions of an axiom or proof box, we say the <u>front door(s)</u> of a generalized axiom link, $\mathbb{1}$ axiom box and $\top$ axiom box are the atomic formulae C and $C^\perp$, $\mathbb{1}$ and $\top$ respectively; all the other conclusions of such boxes are called <u>side doors</u>. Likewise, the front door of an &-proof box (!-proof box) is $A\&B$ ($!A$) and all the other conclusions are called side doors of the box.

The conversion schemes are of three kinds.

(1) Generalized axiom conversion. This is performed any time we have a CUT link both premises of which are front doors of generalized axiom links. This is the analogue of the scheme (AC) defined in 6·1·0.

(2) Symmetric conversions. These cover cases where the premises of a CUT link come by dual links.

(3) Commutative conversions. These are required when one of the premises of a CUT link is a side door of either a T axiom box, an &-box or a !-box. (Side doors of generalized axiom links and $\mathbb{1}$ axiom boxes are dealt with in (2).)

The conversions required for the modal connectives are such that reduction in **PNI!** fails to have the Church-Rosser property. The property of preserving semantic objects, that is

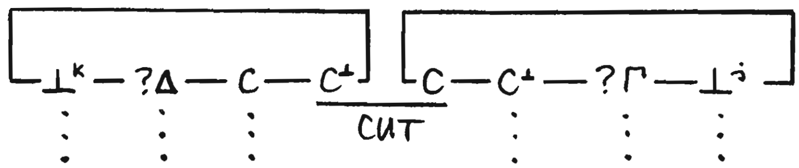
$$\text{if } \beta \rightsquigarrow \beta_0 \text{ then } \beta^* = \beta_0^*$$

is the (not to be scoffed at) consolation prize; a proof net β in **PNI!** may reduce to distinct normal forms β_0 and β_1 but since $\beta_0^* = \beta_1^*$, they do not differ too much.

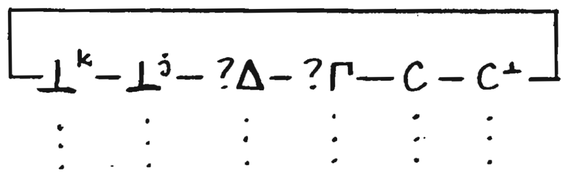
We will use the 'bottom-up' characterization of β^* to verify, for some but not all of the conversion schemes, that if β con β_0 then $\beta^* = \beta^*$. For the cases omitted, consult the original: Girard [1987], Chapter 4.

(1) Generalized axiom conversion (GAC):

β' is obtained from β by replacing a configuration of the form



by



if $\quad s(\beta) = x(k+m+3)(j+n+3)$
then $\quad s(\beta') = x(k+j+m+n+3)$.

We claim $\quad \beta^* = \beta'^*$.

This is proved by induction on the depth of nesting of boxes containing the CUT link in question.

Base case: $n=0$. So the CUT link is in the outermost region of β, i.e. it is not contained in any box. Let $\underset{\sim}{w}$ be any basis for a successful experiment in β. Suppose we have chosen $x \in |C|$ and $x \in |C^\perp|$ for the CUT link in β. Since the experiment succeeds on the basis of $\underset{\sim}{w}$, $\underset{\sim}{w}$ must force the allocation of $x \in |C|$ for C in the left axiom box and $x \in |C^\perp|$ for $C^\perp$ in the right axiom box, as well as ensuring that ϕ is assigned to each $?A_i$ in $?\Delta$ and to each $?B_j$ in $?\Gamma$. (Note that @ is always allocated to $\perp$ since $|\perp| = \{@\}$.) But in such a case, $\underset{\sim}{w}$ is also the basis of a successful experiment in β'. Hence $\beta^* \subseteq \beta'^*$. Conversely, suppose $\underset{\sim}{z}$ is a basis for a successful experiment in β'.

then $\underset{\sim}{z}$ must force the allocation of $x \in |C|$ and $x \in |C^\perp|$ as well as ensuring that all the $?A_i$ and $?B_j$ are assigned ϕ. Now with regard to the CUT link in β, we are free to choose $x \in |C|$ and $x \in |C^\perp|$ for the premises C and $C^\perp$. So $\underset{\sim}{z}$ is a basis for a successful experiment in β. Hence $\beta'^* \subseteq \beta^*$.

Induction step: $n>0$. So the conversion takes place within a box $\square$, and $\square$ is replaced by $\square'$. If $\square$ is not the innermost proof box containing the CUT then consider the box $\square_0$ of depth one fewer than the depth of $\square$. the conversion replaces $\square_0$ with $\square_0'$, and the induction hypothesis gives us $\square_0^* = (\square_0')^*$. Since the conversion takes place inside $\square_0$, it has no impact outside that box; in particular, the constituents of $\square$ other than $\square_0$ are the same as the constituents of $\square'$ other than $\square_0'$. Hence $\square^* = \square'^*$. If $\square$ is the innermost proof box containing the CUT then there is a proof net β_0 inside $\square$ such that the conversion replaces β_0 with β_0'. By the base case of the induction, $\beta_0^* = (\beta_0')^*$, and so $\square^* = \square'^*$. Now β' is built from $\square'$ in the same way that β is built from $\square$, so we must have $\beta^* = \beta'^*$.

The argument for the induction step given above applies generally to any conversion. So for the remaining conversions, we need only consider the base case of the induction, i.e. we may assume the conversion does not take place within a box.

The conversion scheme (GAC) deals with the case when both premises of a CUT link are front doors of a generalized axiom link. If exactly one premis of a CUT link is such a front door then, since it is an atomic formula, the only way in general that the dual atomic formula can occur is as a side door of a T axiom box. That class of cuts is dealt with in (3.1) below.

(2) Symmetric conversions

(2.1) Multiplicative symmetric conversion ($\otimes/\wp$-SC):

β' is obtained from β by replacing a configuration of the form

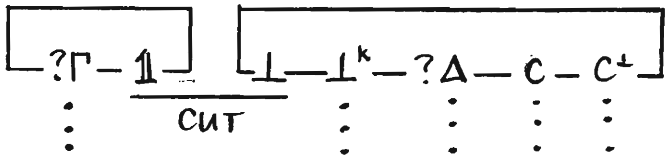
$$\dfrac{\dfrac{\begin{matrix}\vdots & \vdots\\ A & B\end{matrix}}{A\otimes B} \qquad \dfrac{\begin{matrix}\vdots & \vdots\\ A^{\perp} & B^{\perp}\end{matrix}}{A^{\perp}\wp B^{\perp}}}{\text{CUT}} \qquad \text{by} \qquad \dfrac{\begin{matrix}\vdots & \vdots\\ A & A^{\perp}\end{matrix}}{\text{CUT}} \quad \dfrac{\begin{matrix}\vdots & \vdots\\ B & B^{\perp}\end{matrix}}{\text{CUT}}$$

If $s(\beta) = x\cdot 2^6$ then $s(\beta') = x\cdot 2^4$.

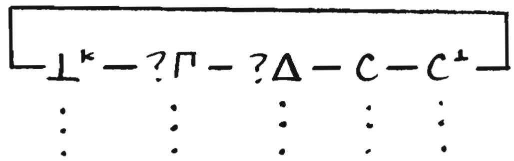
In any experiment in β, we have to select a pair $(x,y)\in|A\otimes B| = |A^{\perp}\wp B^{\perp}|$ then allocate $x\in|A|$ and $x\in|A^{\perp}|$, and $y\in|B|$ and $y\in|B^{\perp}|$. But this is indistinguishable from an experiment in β', where we select $x\in|A|=|A^{\perp}|$ and $y\in|B|=|B^{\perp}|$. Hence $\underset{\sim}{w}$ is a basis for a successful experiment in β iff it is a basis for a successful experiment in β'. Hence $\beta^* = \beta'^*$.

(2·2) Multiplicative unit conversion ($\mathbb{1}/\perp$ - sc)

β' is obtained from β by replacing a configuration of the form



by

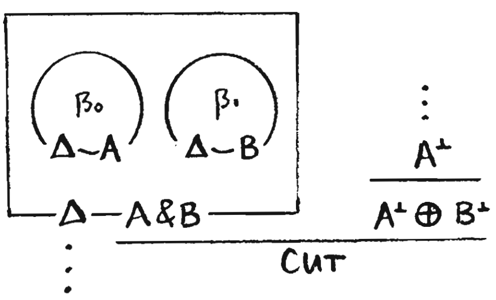


If $s(\beta) = x(n+2)((k+1)+m+3)$
then $s(\beta') = x(k+n+m+3)$

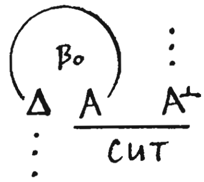
In β, we have to select $@ \in |\mathbb{1}| = |\perp|$ but this contributes nothing to the success or otherwise of an experiment. What matters is the allocation of elements $a_i \in |?A_i|$ in $?\Gamma$, $b_j \in |?B_j|$ in $?\Delta$, $x \in |C|$ and $x' \in |C^\perp|$, just as in an experiment in β'. Hence $\beta^* = \beta'^*$

(2·3) Additive symmetric conversion ($\&$ / FST$\oplus$ - sc)

β' is obtained from β by replacing a configuration of the form



by



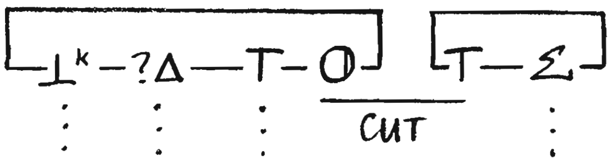
If $s(\beta) = (x+y+1)\cdot 2z$ then $s(\beta') = x \cdot z$

Suppose that in an experiment in β, we have $\underset{\sim}{z} \in |\Delta|$ and we have to choose an element in $|A \& B| = |A^{\perp} \oplus B^{\perp}|$. If we choose $(1, y) \in |A \& B|$ then, due to the FST $\oplus$ link, the experiment will not succeed. So in successful experiments in β, an element $(0, x) \in |A \& B|$ is chosen and $\underset{\sim}{z}, x$ is allocated to Δ, A and x is allocated to $A^{\perp}$. In an experiment in β' where $\underset{\sim}{z} \in |\Delta|$ is given, we have to choose an $x \in |A| = |A^{\perp}|$ then allocate $\underset{\sim}{z}, x$ to Δ, A and x to $A^{\perp}$. Hence $\beta^* = \beta'^*$.

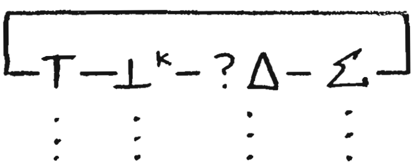
(2.4) Additive symmetric conversion ($\& / \text{SND} \oplus - \text{SC}$): the obvious modification of ($\& / \text{FST} \oplus - \text{SC}$).

(2.5) Additive unit conversion ($0 / \top - \text{SC}$):
Although there is no link specifically for 0, we allow constants as well as literals to be front doors of generalized axiom links.

β' is obtained from β by replacing a configuration of the form



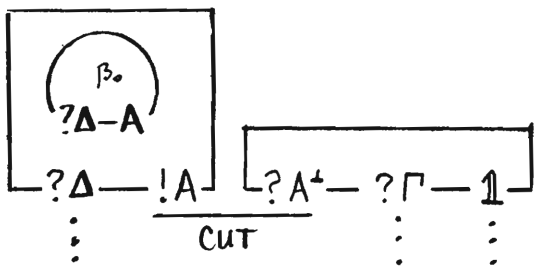
by



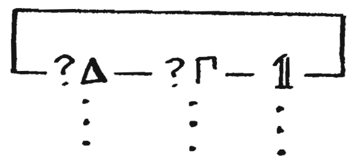
If $s(\beta) = x \cdot (k+m+3)(n+2)$ then $s(\beta') = x \cdot (k+m+n+2)$.
$\beta^* = \beta'^* = \emptyset$.

(2·6) Exponential symmetric conversion (! / Th? – SC):
This conversion is required whenever one premis of a CUT link is a side door ?A of either a generalized axiom link or a $\mathbb{1}$ axiom box. We state it for the latter.

β' is obtained from β by replacing a configuration of the form



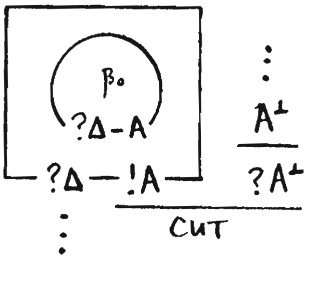
by



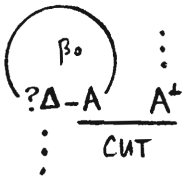
If $s(\beta) = x.(y+1)(m+3)$ then $s(\beta') = x.(n+m+2)$ for some $n \leq y$.

In an experiment in β, suppose we have $\underset{\sim}{b} \in |?\Delta|$ and we need to select an $a \in |!A| = |?A^{\perp}|$. For the experiment to succeed, we must choose $a = \emptyset$. But if $a = \emptyset$ then we must have $b_i = \emptyset$, $i = 1, \ldots, n$, where $\underset{\sim}{b} = (b_1, \ldots, b_n)$. This is what is required for a successful experiment in β'.

(2·7) Exponential symmetric conversion (! / D? – SC)
β' is obtained from β by replacing a configuration of the form



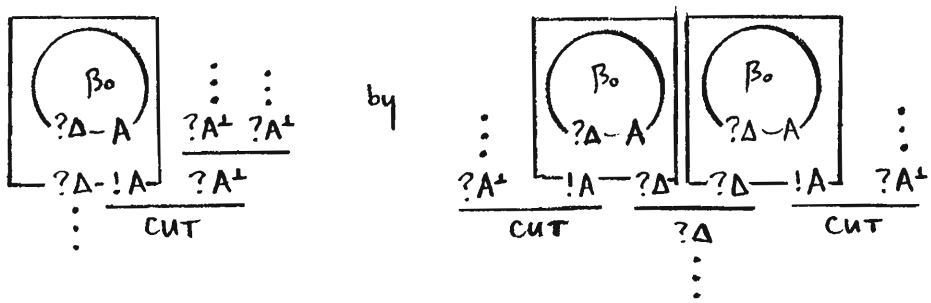
by



If $s(\beta) = (x+1).4z$ then $s(\beta') = x.2z$.

In an experiment in β, suppose we have $\underset{\sim}{b} \in |?\Delta|$ and we need to select an $a \in |!A| = |?A^{\perp}|$. Due to the D? link, the experiment will be abandoned unless $a = \{x\}$. Then we assign x to $A^{\perp}$ and $\underset{\sim}{b}.x$ to $?\Delta, A$. (Since a is a singleton, we don't have to choose a decomposition of $\underset{\sim}{b}$.) But this is what we do in any experiment in β'. Hence $\beta^* = \beta'^*$

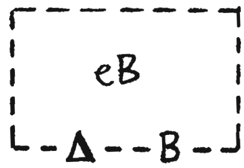
(2.8) Exponential symmetric conversion $(!/c? - sc)$:
β' is obtained from β by replacing a configuration of the form



The duplication of the !-proof box results in an exponential growth in size.
If $s(\beta) = (x+1).8z$
then $s(\beta') = (x+1)^2.4z.2^n$ where $n < x$ (n is the number of formula occurrences in $?\Delta$).

(3) Commutative conversions.
To deal with the cases when one of the premises of a CUT link is a side door of a $\top$ axiom box or an &-box, we need the concept of a ghost box.

Let $\frac{B \quad B^{\perp}}{\text{CUT}}$ be a CUT link, in a given proof net β, which is not inside any proof box. In this outer-most region of β, we can treat the conclusions of any proof box bordering the region as if they were the conclusions of an axiom box. So we can sensibly consider the empire eB of B. The <u>frontier</u> of eB consists of B together with the conclusions of β which belong to eB and the premises of $⅋$ links and $C?$ links such that the other premis is not in eB. Otherwise put, the frontier of eB consists of those formula occurrences in eB that become terminal when we consider eB as (the underlying set of) a proof net. List the frontier of eB as Δ, B. The <u>ghost box</u> of eB is an object of the form



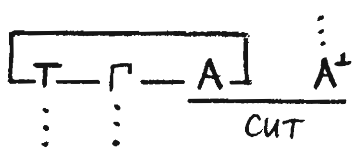
For the purposes of tram trips (within this outer-most region of β), Δ, B behave like the conclusions of an axiom box. The <u>materialization</u> of eB consists of replacing eB in β by the ghost box of eB.

<u>Proposition 6.4.1</u>: (Girard [1987])
If β is a proof net in **PN1!** and $\frac{B \quad B^{\perp}}{\text{CUT}}$ is a CUT link in β not inside any proof box then the proof structure obtained from the outer-most region of β by materializing eB and $eB^{\perp}$ does not admit any short-trips. ■

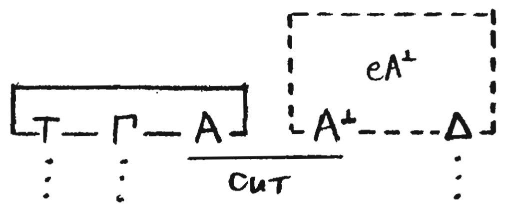
For the purposes of conversion, ghost boxes give us much needed information about a premis of a CUT link. The formula occurrences in the frontier of eB, other than B itself, are those which are both connected with B, in the sense that they lie in the interval $[B^\wedge, B_\vee]_t$ for each trip t, and are linked with the region outside eB.

(3.1) Zero commutation (T-cc)

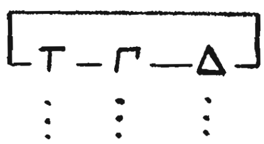
If β contains the configuration



then first materialize $eA^\perp$,



then create β' by replacing the above configuration by one of the form

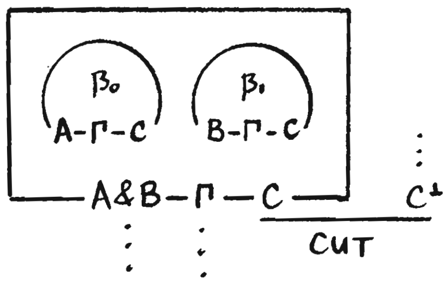


If $s(\beta) = (n+3)\cdot x \cdot y$ then $s(\beta') = (n+m+2)\cdot y$ where $m < x$.

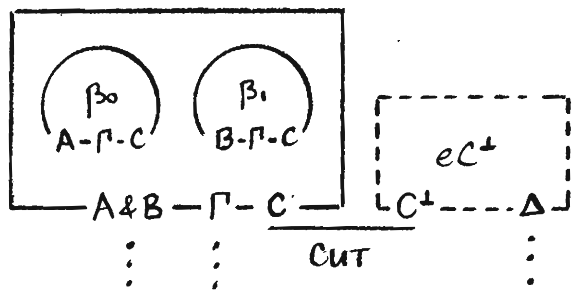
$\beta^* = \beta'^* = \emptyset$.

(3·2) Additive commutation ($\&$-CC):

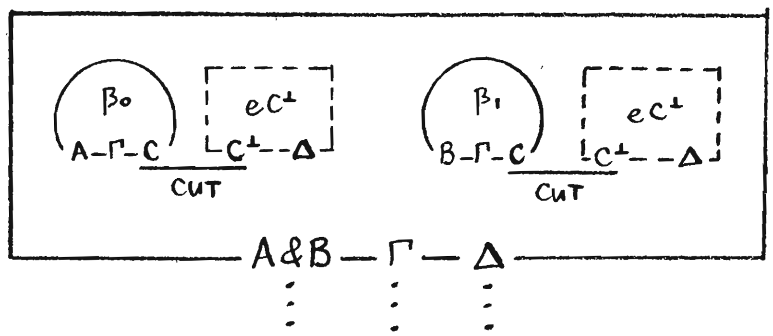
If β contains the configuration



then first materialize $eC^\perp$,



then create β' by replacing the above configuration by one of the form



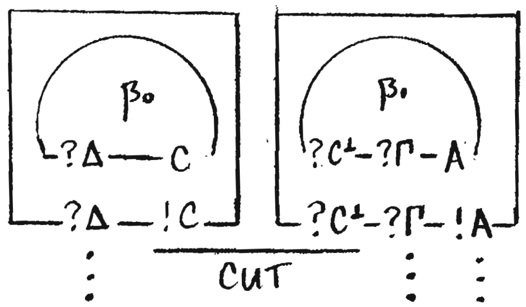
After performing this conversion, the ghost boxes may be erased.

If $s(\beta) = (x+y+1)\cdot z\cdot t$ then $s(\beta') = (xz+yz+1)\cdot t$

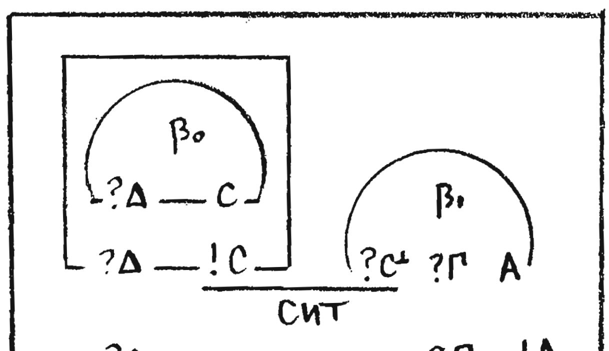
(3·3) Exponential commutation (!-CC)

In the case when one premis of a CUT link is a side door of a !-proof box, ghost boxes are of no help. If $?C^{\perp}$ is one premis of a CUT then the other is $!C$. If $!C$ is a side door of a T axiom box then use the scheme (T-CC), and if $!C$ is a side door of an &-proof box then use the scheme (&-CC). The only remaining possibility is that $!C$ is the front door of a !-proof box.

β' is obtained from β by replacing a configuration of the form

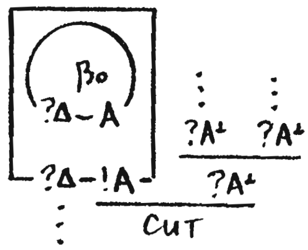


by



If $s(\beta) = (x+1)\cdot(y+1)\cdot z$ then $s(\beta') = ((x\cdot(y+1))+1)\cdot z$.

<u>Theorem 6.4.2</u>: The Small Normalization Theorem (Girard [1987])
If β is any proof net in **PN1!** which does not contain a configuration of the form



then β is strongly normalizable.

<u>Proof</u>:
If β does not contain the objectionable configuration then $L(\beta) < S(\beta)$. ■

For the proof of the Strong Normalization theorem for **PN2** (and **PN1!**), Girard adapts his technique of 'candidats de réductibilité' originally devised for the system **F**. The CR's are sets of proof nets which have an underlying structure similar to that of <u>facts</u> in the phase space semantics. Those readers still breathing are encouraged to first take a long walk and then, suitably refreshed, work through the remaining material on their own.

Appendix A: A guide to notation

	Girard [1987]	Seely [1989]	Avron [1988]	Relevance logics eg. Dunn [1986]
implication	$A \multimap B$	$A \multimap B$	$A \rightarrow B$	$A \rightarrow B$
negation	$A^{\perp}$	$\neg A$	$\sim A$	$\neg A$
times/fusion	$A \otimes B$	$A \otimes B$	$A \circ B$	$A \circ B$
	$\mathbb{1}$	I	t	t
par/fission	$A \parr B$	$A \odot B$	$A + B$	$A + B$ or $A \uplus B$
	$\perp$	$\emptyset$	f	f
with/and	$A \& B$	$A \times B$	$A \wedge B$	$A \wedge B$ or $A \& B$
	$\top$	1	$\top$	$\top$
plus/or	$A \oplus B$	$A + B$	$A \vee B$	$A \vee B$
	$\mathbb{0}$	0	F	F
"of course"/ necessity	$!A$	$!A$	$\Box A$	$\Box A$
"why not"/ possibility	$?A$	$?A$	$\Diamond A$	$\Diamond A$

Appendix B: Two sided sequent calculi

Let $\mathcal{L}_D$ be the collection of formulae generated from propositional letters and constants $\mathbb{1}, \perp, \top, \mathbb{0}$ by means of the unary connective $(-)^\perp$, the binary connectives $\otimes, \mathbin{⅋}, \multimap, \&$ and $\oplus$, and the unary connectives ! and ?.

The two-sided sequent calculus for propositional linear logic, **DLL**, consists of the axiom schemes:

$$(\text{identity}) \quad A \vdash A$$

$(R\mathbb{1}) \quad \vdash \mathbb{1}$ $\qquad$ $(L\perp) \quad \perp \vdash$

$(R\top) \quad \Gamma \vdash \top, \Delta$ $\qquad$ $(L\mathbb{0}) \quad \Gamma, \mathbb{0} \vdash \Delta$

$(R\,neg) \quad A \vdash A^{\perp\perp}$ $\qquad$ $(L\,neg) \quad A^{\perp\perp} \vdash A$

and the following rules of inference:

structural rules:

$$\frac{\Gamma \vdash \Delta}{\tau(\Gamma) \vdash \sigma(\Delta)}\,(\text{EXCH}) \qquad \frac{\Gamma_0 \vdash A, \Delta_0 \quad A, \Gamma_1 \vdash \Delta_1}{\Gamma_0, \Gamma_1 \vdash \Delta_0, \Delta_1}\,(\text{CUT})$$

where τ and σ are any permutations

negation rule:

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma, B^\perp \vdash A^\perp, \Delta}\,(\text{VAR})$$

additive rules:

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \& B \vdash \Delta}\,(L\&1) \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \& B \vdash \Delta}\,(L\&2)$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \& B, \Delta}\,(R\&) \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \oplus B \vdash \Delta}\,(L\oplus)$$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \oplus B, \Delta}\,(R\oplus 1) \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \oplus B, \Delta}\,(R\oplus 2)$$

multiplicative rules:

$$\frac{\Gamma \vdash \Delta}{\Gamma, \mathbb{1} \vdash \Delta}\ (L\mathbb{1}) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \bot, \Delta}\ (R\bot)$$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \otimes B \vdash \Delta}\ (L\otimes) \qquad \frac{\Gamma_0 \vdash A, \Delta_0 \quad \Gamma_1 \vdash B, \Delta_1}{\Gamma_0, \Gamma_1 \vdash A \otimes B, \Delta_0, \Delta_1}\ (R\otimes)$$

$$\frac{\Gamma_0, A \vdash \Delta_0 \quad \Gamma_1, B \vdash \Delta_1}{\Gamma_0, \Gamma_1, A \parr B \vdash \Delta_0, \Delta_1}\ (L\parr) \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \parr B, \Delta}\ (R\parr)$$

$$\frac{\Gamma_0 \vdash A, \Delta_0 \quad \Gamma_1, B \vdash \Delta_1}{\Gamma_0, \Gamma_1, A \multimap B \vdash \Delta_0, \Delta_1}\ (L\multimap) \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \multimap B, \Delta}\ (R\multimap)$$

The language for <u>intuitionistic linear logic</u> is as above, except that the constant $\bot$ and the binary connective $\parr$ are omitted. The sequent calculus for propositional intuitionistic linear logic is obtained from **DLL** by (i) omitting the axiom schemes $(L\bot)$, $(R\,neg)$ and $(L\,neg)$; (ii) omitting the inference rules (VAR), $(R\bot)$, $(L\parr)$ and $(R\parr)$; and (iii) stipulating that sequents contain at most one formula on the RHS.

The sequent calculus **DLL!** is obtained from **DLL** by adjoining the following inference rules:

$$\frac{\Gamma \vdash \Delta}{\Gamma, !A \vdash \Delta}\ (LTh!) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash ?A, \Delta}\ (RTh?)$$

$$\frac{\Gamma, !A, !A \vdash \Delta}{\Gamma, !A \vdash \Delta}\ (LC!) \qquad \frac{\Gamma \vdash ?A, ?A, \Delta}{\Gamma \vdash ?A, \Delta}\ (RC?)$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, !A \vdash \Delta}\,(LD!) \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash ?A, \Delta}\,(RD?)$$

$$\frac{!\Gamma, A \vdash ?\Delta}{!\Gamma, ?A \vdash ?\Delta}\,(L?) \qquad \frac{!\Gamma \vdash A, ?\Delta}{!\Gamma \vdash !A, ?\Delta}\,(R!)$$

Bibliography

Avron, A. [1988]
"The Semantics and Proof Theory of Linear Logic", Theoretical Computer Science, 57 (1988), 161-184.

Barr, M. [1979]
*- Autonomous Categories, Springer Lecture Notes in Mathematics 752, Berlin, 1979.

Belnap, N.D. [1982]
"Display Logic", Journal of Philosophical Logic, 11 (1982), 375-417.

Belnap, N.D. [1990]
"Linear Logic Displayed", Notre Dame Journal of Formal Logic, 31 (1990), 14-25.

Berry, G. [1978],
"Stable Models of Typed Lambda-Calculi", Proceedings of the 5th International Colloquium on Automata, Languages and Programming (ICALP), Udine, 1978.

Burris, S. and Sankappanavar, H.P. [1980],
A Course in Universal Algebra, Graduate Texts in Mathematics, Springer-Verlag, New York, 1980.

Danos, V. and Regnier, L. [1989],
"The Structure of Multiplicatives", Archive for Mathematical Logic, 28 (1989), 181-203.

Dunn, J.M. [1986]
"Relevance Logic and Entailment", in D. Gabbay and F. Guenther (eds), Handbook of Philosophical Logic, Vol. III, Reidel, Dordrecht, 1983; 117-224.

Gentzen, G. [1964,5]
"Investigations into Logical Deduction", trans. M.E. Szabo, American Philosophical Quarterly, 1 (1964), 288-306; 2 (1965), 204-218. Reprinted in M.E. Szabo, (ed), The Collected Works of Gerhard Gentzen, North Holland, Amsterdam, 1969; 68-131.

Girard, J.-Y. [1987]
"Linear Logic", Theoretical Computer Science, 50 (1987), 1-102.

Girard, J.-Y. [1989]
"Towards a Geometry of Interaction", in J.W. Gray and A. Ščedrov (eds), Categories in Computer Science and Logic, Proceedings of Summer Research Conference, Boulder, June 1987; Contemporary Mathematics Volume 92, American Mathematical Society, Providence, 1989; 69-108.

Girard, J.-Y. and Lafont, Y. [1987]
"Linear Logic and Lazy Computation", in TAPSOFT '87, Proceedings of the International Joint Conference on the Theory and Practice of Software Development (Pisa, Italy), Vol. 2, Springer Lecture Notes in Computer Science, 250.

Girard, J.-Y. with Lafont, Y. and Taylor, P. [1989], Proofs and Types, Cambridge Tracts in Theoretical Computer Science 7, CUP, Cambridge, 1989. (Translation and appendices by Lafont and Taylor.)

Girard, J.-Y., Scedrov, A. and Scott, P.J. [1990], "Bounded Linear Logic: a Modular Approach to Polynomial Time Computability" (extended abstract), in S.R. Buss and P.J. Scott (eds), Feasible Mathematics, Mathematical Sciences Institute Workshop, Ithaca, New York, June 1989; Progress in Computer Science and Applied Logic 9, Birkhäuser, 1990.

Lafont, Y. [1988a]. "Introduction to Linear Logic", Lecture Notes for the Summer School on Constructive Logics and Category Theory (Isle of Thorns, August 1988).

Lafont, Y. [1988b] "The Linear Abstract Machine," Theoretical Computer Science, 59 (1988), 157-180.

Lambek, J. and Scott, P.J. [1986] Introduction to Higher Order Categorical Logic, Cambridge Studies in Advanced Mathematics 7, CUP, 1986.

Mac Lane, S. [1971], Categories for the Working Mathematician, Graduate Texts in Mathematics, Springer-Verlag, New York.

Marti-Oliet, N. and Mesegeur, J. [1989]
"From Petri Nets to Linear Logic", in D.H. Pitt et al. (eds), Category Theory and Computer Science, Proceedings, Manchester, September 1989; Springer Lecture Notes in Computer Science, 389; 313-340.

Moschovakis, J.R. [1980],
"Kleene's Realizability and 'Divides' Notions for Formalized Intuitionistic Mathematics", in J. Barwise et. al (eds), The Kleene Symposium, North Holland, 1980; 167-179.

Schwichtenberg, H. [1977]
"Proof Theory: Some Applications of Cut-Elimination", in J. Barwise (ed.), Handbook of Mathematical Logic, North Holland, Amsterdam, 1977; 867-895.

Scott, D.S. [1982].
"Domains for Denotational Semantics", in M. Nielson and E.M. Schmidt (eds), Automata, Languages and Programming: International Colloquium, (ICALP), Proceedings, Aarhus, Denmark, 1982; Springer Lecture Notes in Computer Science 140; 577-613.

Seely, R.A.G. [1989]
"Linear Logic, *-Autonomous Categories and Cofree Algebras", in J.W. Gray and A. Sčedrov (eds), Categories in Computer Science and Logic, Proceedings of Summer Research Conference, Boulder, June 1987; Contemporary Mathematics Volume 92, American Mathematical Society, Providence, 1989; 371-382.

Shoesmith, D. J. and Smiley, T. J. [1978],
Multiple Conclusion Logic, CUP, Cambridge, 1978.

Thistlewaite, P.B., McRobbie, M.A. and Meyer, R.K. [1988],
Automated Theorem-Proving in Non-Classical Logics,
Pittman, London, 1988.