Introduction to linear logic and ludics, Part I

Pierre-Louis Curien (CNRS & Université Paris VII)*

June 12, 2004

Abstract

This two-parts paper offers a survey of linear logic and ludics, which were introduced by Girard in 1986 and 2001, respectively. Both theories revisit mathematical logic from first principles, with inspiration from and applications to computer science. The present part I covers an introduction to the connectives and proof rules of linear logic, to its decidability properties, and to its models. Part II will deal with proof nets, a graph-like representation of proofs which is one of the major innovations of linear logic, and will present an introduction to ludics.

Keywords: Cut-elimination (03F05), Linear logic (03F52), Logic in computer science (03B70), Interactive modes of computation (68Q10), Semantics (68Q55), Programming languages (68N15).

Prerequisites

We assume some basic knowledge of sequent calculus and natural deduction (see [11, 15]), of λ-calculus (the classical reference is [1], see also [17]), and of category theory (only in section 7, see [22]).

Warning

This paper is not trying to survey the whole and impressive body of works on linear logic since 17 years, but rather chooses a route that tries to highlight the deep originality of the subject. The bibliography is in consequence very partial (also reading the latter as a French word, wich means something like "personal", possibly biased).

1 Introduction

Linear logic arose from the semantic study of λ-calculus, specifically, the second-order typed λ-calculus, or system F (see [11]). Shortly after proposing the first denotational model of system F [9], Girard realized that in coherence spaces (to be introduced in section 7) the interpretation of type $A \to B$ decomposes naturally as $(!A) \multimap B$ (this will be detailed in section 6), and in almost no time a full-fledged new logic, with a totally innovative way of representing proofs and executing them, that is, of performing cut-elimination, was created. We tell this story here, not in the order in which it unfolded, but starting from so-called substructural considerations. We raise the question of what happens

*Laboratoire *Preuves, Programmes et Systèmes*, Case 7014, 2 place Jussieu, 75251 Paris Cedex 05, France, curien@pps.jussieu.fr.

when we remove some of the structural rules from sequent calculus, most importantly contraction. Substructural logics of various kinds have been considered much before the birth of linear logic, but what characterizes truly linear logic is not that aspect, but rather the controlled way in which the structural rules of weakening and contraction are reintroduced, by means of the new modality ! ("of course") (and its dual ? ("why not")). This, together with proof nets, constitutes the major breakthrough of linear logic.

Let us consider the implication in the absence of contraction. In λ-calculus, this corresponds to considering terms in which each variable occurs at most once. (Here we use the Curry-Howard correspondence between proofs and programs, see [11]). Consider thus the set of *affine* λ-terms built with the following constraints: x is an affine term, if M is an affine term then $\lambda x.M$ is an affine term, and if M, N are affine terms *with disjoint sets of free variables* then MN is an affine term. The key fact about affine terms is the following:

Affine terms normalize in linear time.

The reason is trivial: each β-reduction strictly decreases the size, keeping in mind that $P[x \leftarrow Q]$ is the result of the substitution of at most one occurrence of x with Q, so $P[x \leftarrow Q]$ is shorter by at least the two symbols of abstraction and application that have been absorbed by the reduction of $(\lambda x.P)Q$. Of course, this linearity is one of the reasons for the name Linear Logic.

In contrast, arbitrary λ-terms may take an exponential time and more to reach their normal form. For example, the reader may play with $\underline{m}\,\underline{n}$, where $\underline{n} = \lambda f x.f^n(x)$ (Church numerals, with $f^0(x) = x$ and $f^{n+1}(x) = f(f^n(x))$).

As another instance of the phenomenon of duplication, or of *multiple use* of a variable (or assumption), think of a constructive reading of $(\forall\, x\ \exists\, y\ x < y)$ from which one may wish to extract a program creating an infinite strictly increasing sequence of numbers. The program extracted from the formula will actually be a procedure to produce a $y > x$, when given an x, and it will be called in a loop. In linear logic, this formula would have to be written $!(\forall\, x\ \exists\, y\ x < y)$.

Rather than continuing a long introduction, we decide to enter in the subject proper, and we content ourselves with giving a plan of the sections to come. In section 2, we introduce so-called *multiplicative-addditive* linear logic, and we complete the description of (propositional) linear logic with the *exponentials* in section 3. We shall not consider quantifiers in this survey paper, in any case, they look very much as usual. Then, in section 4, we illustrate the expressivity of linear logic by sketching the proof that propositional linear logic is undecidable, a property that sharply distinguishes linear logic from classical and intuitionistic logics. The following three sections are concerned with the semantics of linear logic. We first discuss phase semantics, which is just a semantics of provability (section 5), then we introduce the coherence semantics, already alluded to (section 6), and finally we address the question of more general categorical definitions of models (section 7).

In part II, we shall go back to syntactic issues and introduce proof nets. In particular, we shall address the so-called correctness criteria: proof nets are elegant graph representations of proofs avoiding some useless sequentializations imposed by sequent calculus. Reconstructing the sequentializations and thus deciding whether a proof structure, that is, a would-be proof net, is actually a proof net, is a quite fascinating problem, and there are different equivalent characterizations, giving different insights into the geometry and the dynamics of proofs. The last sections (a polished form of [4]) are devoted to ludics, which while strongly inspired by linear logic takes a more radical view of proofs as interactive processes, evolving in *space* and time.

Here is a table of sources I have been using for writing this paper. The reader will be able to find more complete information and proofs by going to these references, as well as to the many others that he will find in their bibliographies or on the Web!

Part I		
	sections 2 and 3	[10, 12, 5] (slightly revisited here in the light of ludics)
	section 4	[21]
	sections 5 and 6	[10]
	section 7	[23] (which itself is a survey)
Part II		
	proof nets	[10, 8, 16]
	ludics	[13, 14]

2 Multiplicatives and additives

In sequent calculus, depending on presentations, you can see the left and right rules for, say, conjunction given in this format:

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

or in that format:

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2}$$

The two formats have been called *additive* and *multiplicative*, respectively, by Girard. We recall that a sequent $\Gamma \vdash \Delta$ is made of two multisets of formulas (that is, we work modulo the so-called exchange rule which says that $\Gamma \vdash \Delta$ entails any of its permutations – on the contrary, rejecting this rule leads to a complicated and still not very well-understood subject called non-commutative (linear) logic). The notation Γ_1, Γ_2 stands for the multiset union of Γ_1 and Γ_2.

Logicians did not bother about these different presentations, because they are equivalent. Yes, but modulo the contraction and weakening rules:

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

Let us show this, say, for the left introduction rule. Let us first derive the multiplicative format from the additive one:

$$\dfrac{\dfrac{\dfrac{\Gamma_1 \vdash A, \Delta_1}{\Gamma_1, \Gamma_2 \vdash A, \Delta_1, \Delta_2} \quad \dfrac{\Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash B, \Delta_1, \Delta_2}}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2}}{}$$

where the double line expresses multiple use of the weakening rules. For the converse direction we have:

$$\dfrac{\dfrac{\vdash A, \Delta \quad \vdash B, \Delta}{\vdash A \wedge B, \Delta, \Delta}}{\vdash A \wedge B, \Delta}$$

using contractions. If we remove contraction and weakening, then the presentations are no longer equivalent and hence define *different* connectives, $\otimes$ and &, respectively called "tensor" and "with". Indeed, you will see in section 6 that they are interpreted very differently. Moreover, the coherence space model (to which the curious reader may jump directly) enlightens the terminology multiplicative–additive, as the reader will check that the cardinal of (the interpretation of) $A \otimes B$ (resp. $A\&B$) is the *product* (resp. the *sum*) of the cardinals of (the interpretations of) A, B.

Similarly, we split "disjunction" in two connectives, $\parr$ and $\oplus$, respectively called "par" and "plus". As usual in sequent calculus, the left rule for, say, $\otimes$, tells us by duality what the right rule for $\parr$ is, and similarly for $\oplus$. This leads us to the following monolateral sequent presentation of the four connectives:

MULTIPLICATIVES

$$\dfrac{\vdash A, B, \Gamma}{\vdash A \parr B, \Gamma} \qquad \dfrac{\vdash A, \Gamma_1 \quad \vdash B, \Gamma_2}{\vdash A \otimes B, \Gamma_1, \Gamma_2}$$

ADDITIVES

$$\dfrac{\vdash A, \Gamma}{\vdash A \oplus B, \Gamma} \quad \dfrac{\vdash B, \Gamma}{\vdash A \oplus B, \Gamma} \qquad \dfrac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \& B, \Gamma}$$

Considered as (associative and commutative) operations, these four connectives have units "true" and "false", each of them splits into the multiplicative and additive one:

$\parr$	$\otimes$	$\oplus$	$\&$
$\bot$	1	0	$\top$

(As for the terminology and for mnemotechnicity, the names 1 and 0 correspond to the usual multiplicative and additive notation in groups.) We shall synthesize the rules for the units from the requirement that the isomorphisms $A \otimes 1 \approx A$, etc..., should hold. In order to prove $\vdash A \otimes 1, \Gamma$ from $\vdash A, \Gamma$ we should have $\vdash 1$. In order to prove $\vdash A \parr \bot, \Gamma$ from $\vdash A, \Gamma$, we should have $\vdash A, \bot, \Gamma$ as an intermediate step, which suggests the rule for $\bot$ given below. We derive $\vdash A \oplus 0, \Gamma$ from $\vdash A, \Gamma$ by the (left) $\oplus$ rule, without any need for a (right) rule for 0. Finally, we need $\vdash \top, \Gamma$ to derive $\vdash A \& \top, \Gamma$ from $\vdash A, \Gamma$:

$$\dfrac{\vdash A \quad \dfrac{}{\vdash 1}}{\vdash A \otimes 1} \qquad \dfrac{\dfrac{\vdash A, \Gamma}{\vdash A, \bot, \Gamma}}{\vdash A \parr \bot, \Gamma} \qquad \dfrac{\vdash A, \Gamma}{\vdash A \oplus 0, \Gamma} \qquad \dfrac{\vdash A, \Gamma \quad \dfrac{}{\vdash \top, \Gamma}}{\vdash A \& \top, \Gamma}$$

The rules are thus:

UNITS

$$\frac{}{\vdash 1} \qquad \frac{\vdash \Gamma}{\vdash \bot, \Gamma} \qquad \text{no rule for } 0 \qquad \frac{}{\vdash \top, \Gamma}$$

An even shorter way to synthesize the rules for the units is to formulate rules for n-ary versions of the four connectives, and then to take the degenerate case $n = 0$. The assumption of the n-ary $\parr$ rule is $\vdash A_1, \ldots, A_n, \Gamma$, which degenerates to $\vdash \Gamma$. For the tensor rule there are n assumptions and the conclusion is $\vdash A_1 \otimes \ldots \otimes A_n, \Gamma$, with $\Gamma = \Gamma_1, \ldots, \Gamma_n$, and in the degenerate case we thus have no assumption and $\Gamma = \emptyset$. There are n $\oplus$ rules, and thus no rule in the degenerate case. Finally, the $\&$ rule has n assumptions, and thus no assumption in the degenerate case.

What about negation? In classical logic, negation can be boiled down to negation on atomic formulas only, thanks to De Morgan laws: $\neg(A \wedge B) = (\neg A) \vee (\neg B)$, from which the other De Morgan law follows, using $\neg\neg A = A$. This works also for linear logic, where negation is written $A^\bot$ ("A orthogonal", or "A perp"). But the logical operations being different, negation in linear logic is very different from that of classical logic. In classical logic, we have both $A = \neg\neg A$ and $\vdash A \vee \neg A$ (the latter being what constructivists criticized), while in linear logic we have $A = A^{\bot\bot}$ and $\vdash A \parr A^\bot$, but *we do not have* $\vdash A \oplus A^\bot$, and as a matter of fact linear logic retains the distinctive features that make intuitionistic logic so nice: confluence (of cut-elimination), and the disjunction property (for $\oplus$, see below).

Thanks to De Morgan laws, we can dispense with negation as a connective, and consider $A^\bot$ as an abbreviation for its De Morgan normal form obtained by applying the following rules (where we have added the not-yet introduced "!" and "?" for completeness):

$$\begin{array}{llll} (A \otimes B)^\bot \to (A^\bot) \parr (B^\bot) & (A \parr B)^\bot \to (A^\bot) \otimes (B^\bot) & 1^\bot \to \bot & \bot^\bot \to 1 \\ (A \& B)^\bot \to (A^\bot) \oplus (B^\bot) & (A \oplus B)^\bot \to (A^\bot) \& (B^\bot) & \top^\bot \to 0 & 0^\bot \to \top \\ (!A)^\bot \to ?(A^\bot) & (?A)^\bot \to !(A^\bot) & & \end{array}$$

(Notice that the dual under $^\bot$ of a multiplicative (resp. additive) connective is a multiplicative (resp. additive) connective.) A normal form according to these rules contains negations on atoms only. So, we arrive at the following syntax of formulas (where X and $X^\bot$ stand for atoms):

$$A ::= X \mid X^\bot \mid A \otimes A \mid 1 \mid A \parr A \mid \bot \mid A \oplus A \mid 0 \mid A \& A \mid \top \mid !A \mid ?A$$

In the sequel, we shall freely use bilateral sequents in examples, but they can be seen as syntactic sugar for monolateral ones, for example $A_1, A_2 \vdash B$ is a version of $\vdash A_1^\bot, A_2^\bot, B$. Hence, thanks to duality, linear logic puts all formulas of a sequent on the same ground, in contrast to intuitionistic logic, where there is a clear distinction between input (Γ) and output (A) in a sequent $\Gamma \vdash A$.

To complete the description of the multiplicative-additive fragment of linear logic, we need axioms, and the cut rule. The latter is not needed in the sense that it can be eliminated (just as in classical or intuitionisitc sequent calculus), but one can hardly use the system without cuts, which carry the intelligent part of proofs.

$$\textbf{AXIOM}\quad \frac{}{\vdash A, A^\perp} \qquad \textbf{CUT}\quad \frac{\vdash A, \Gamma_1 \quad \vdash A^\perp, \Gamma_2}{\vdash \Gamma_1, \Gamma_2}$$

(Note that the cut rule is given in a multiplicative style, i.e., it is quite similar to the tensor rule. That the axiom has this most economical format, as opposed to $\vdash A, A^\perp, \Gamma$, should come as no surprise, as the latter embodies an implicit weakening.)

As explained in the introduction, the main motivation for the removal of (weakening and) contraction is the control on normalization. Indeed, the reader can easily check that all affine λ-terms can be typed by the following rules:

$$\frac{}{x : A \vdash x : A} \qquad \frac{\Gamma_1 \vdash M_1 : A \multimap B \quad \Gamma_2 \vdash M_2 : A}{\Gamma_1, \Gamma_2 \vdash M_1 M_2 : B} \qquad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \multimap B}$$

Notice the multiplicative style of the crucial typing rule for application. As usual, "A implies B" is "not A or B", and specifically here $A \multimap B = (A^\perp) \parr B$ ($\multimap$ reads "linearly implies"). This natural deduction style rule is indeed encoded in sequent calculus using the (multiplicative) cut rule:

$$\frac{\Gamma_1 \vdash A^\perp \parr B \qquad \dfrac{\Gamma_2 \vdash A \qquad \dfrac{}{\vdash B^\perp, B}}{\Gamma_2 \vdash A \otimes B^\perp, B}}{\Gamma_1, \Gamma_2 \vdash B}$$

This leads us to the main conceptual novelty of linear logic: the understanding of formulas as *resources*, that are *consumed* through entailment: in the sequent $A \vdash B$, the resource A is consumed in order to *get* B (think also of a chemical reaction). This is like in an abstract state machine, which changes state upon performing certain actions. As a matter of fact, we present an encoding of such a machine in section 4. With this reading in mind, one easily understands how bad contraction and weakening are. Suppose that B is some good, and A is a given amount of money, say 20 Euros. Then $A, A \vdash B$ reads as: "you can acquire B against 40 Euros". The contraction rule would say that you could acquire the same good for 20 Euros. Thus, contraction is not very good for the merchant. It is not good in chemistry either: in a reaction, in order to obtain $2H_2O$ you need to have exactly four H^+ and two O^{2-}. Another way to criticize the rule is by looking from conclusion to antecedents (proof-search): if you only have A to get B, your resource A cannot be magically duplicated, as the contraction rule would imply.

As for weakening, if you can buy B with A, as formalized by $A \vdash B$, why would you – the buyer – spend an additional amount of money C to get B ($C, A \vdash B$)? Weakening is not good for the client.

So far, we have insisted on a dichotomy between additive and multiplicative connectives. There is however another grouping of connectives, that was sitting there from the beginning, and that has even been somehow made explicitly by the choice of symbols: $\otimes$ and $\oplus$ on one hand, and & and $\parr$ on the other hand. Girard noticed that $\otimes$ distributes over $\oplus$ (like in arithmetic!), and that dually $\parr$ distributes over &, while other thinkable combinations do not distribute upon each other (it is an instructive exercise to check this). Let us examine the proof of this distributivity law. We have to

prove $\vdash (A \otimes (B \oplus C))^\perp, (A \otimes B) \oplus (A \otimes C)$ and $\vdash ((A \otimes B) \oplus (A \otimes C))^\perp, A \otimes (B \oplus C)$. Both proofs begin by decomposing the $\parr$'s and the &'s. For the first sequent, this goes as follows:

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

and we are left to prove the subgoals $\vdash A^\perp, B^\perp, (A \otimes B) \oplus (A \otimes C)$ and $\vdash A^\perp, C^\perp, (A \otimes B) \oplus (A \otimes C)$. Similarly, the search of a proof of the second sequent yields $\vdash A^\perp, B^\perp, A \otimes (B \oplus C)$ and $\vdash A^\perp, C^\perp, A \otimes (B \oplus C)$ as subgoals. Before we proceed, note an important feature of & and $\parr$: in each of the two proof constructions, the two subgoals together are actually equivalent to the original goal: these two connectives are *reversible* – an affirmation that we shall make formal just below. In contrast, in order to complete the proof of any of the subgoals, we have to make (irreversible) decisions. We just give the proof of $\vdash A^\perp, B^\perp, (A \otimes B) \oplus (A \otimes C)$, but the others are similar:

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

The two decisions which we have made in this proof are: to choose the left $\oplus$ rule, and then to split $A^\perp, B^\perp$ in the way we did, assigning the resource $A^\perp$ for the proof of A and $B^\perp$ for the proof of B.

The opposition $\otimes$–$\oplus$ versus $\parr$–& is actually fundamental, and has played an important role in the genesis of ludics (see part II). The following table summarizes its significance:

$\otimes$ $\oplus$	$\parr$ &
Irreversible	Reversible
Non-deterministic	Deterministic
Active	Passive
Player	Opponent
External choice	Internal choice
Positive	Negative

We first show that the rules for $\parr$ and & are reversible, that is, that the conclusions of the rules hold if *and only if* their antecedents hold, as follows:

$$\dfrac{\vdash \Gamma, A \parr B \quad \dfrac{\dfrac{}{\vdash A^\perp, A} \quad \dfrac{}{\vdash B^\perp, B}}{\vdash A^\perp \otimes B^\perp, A, B}}{\vdash \Gamma, A, B} \qquad \dfrac{\vdash A \& B, \Gamma \quad \dfrac{\dfrac{}{\vdash A^\perp, A}}{\vdash A^\perp \oplus B^\perp, A}}{\vdash A, \Gamma}$$

Hence we lose nothing by replacing $\vdash \Gamma, A \parr B$ with $\vdash \Gamma, A, B$ in proof-search, and moreover we can gain something, since the liberated immediate subformulas A and B can then be sent to different

antecedents when decomposing a tensor (as in the proof of $\vdash A \parr B, A^\perp \otimes B^\perp$). The $\parr$ and & rules are moreover *deterministic* in the sense that, once the formula to be decomposed in the sequent is fixed, then there is no choice on how to do it: for the $\parr$ rule, just dissolve the $\parr$, and for the & rule, prove the two subgoals, which are the same sequent up to the replacement of the formula by one of its immediate subformulas. As we shall see in part II (section 2), provided a certain proof-search discipline is respected, which can be phrased as "apply reversible rules in priority", and if maximal groupings of rules concerning reversible (resp. irreversible) connectives are performed and if each such grouping is considered as a single *synthetic rule*, then sequents always contain at most one formula whose topmost connective is reversible, and therefore even the choice of which formula of the sequent to decompose is deterministic (see Remark 2.2 in part II). This absence of initiative can be termed *passivity*.

Let us examine what makes the other connectives on the countrary *active* and *irreversible*. We have already hinted at this when we proved the distributivity law. Each $\oplus$ rule, read bottom-up, chooses one of A or B, while each instance of the $\otimes$-rule makes a choice of how to split the (rest of the) sequent in two parts. The choice of which formula of the sequent to decompose is also non-deterministic. In other words, the two connectives are associated with some actions that must be taken.

The next pair in our list places us in the tradition of the *dialogue game* interpretation of proofs, which goes back to Gentzen. A proof is the work of one person, the *Player* (think of a student), which another person, the *Opponent* (think of an examiner) can check. Checking goes by tests, or *plays*. The Opponent challenges the conclusion of the proof, to which the Player has to answer by displaying the last rule he used. The Opponent then chooses one of the antecedents of the rule, and challenges the Player to justify that particular antecedent, to which the Player answers by displaying the last rule used to show this antecedent, etc... The play results in disclosing, or exploring, a part of the proof. We shall come back to this game interpretation in part II (section 3). Here, we shall content ourselves with an illustration, Yves Lafont's menu:

Menu (price 17 Euros)

Quiche or Salad
Chicken or Fish
Banana or "Surprise du Chef"*

(*) either "*Profiteroles*" or "*Tarte Tatin*"

$$17E \vdash \begin{cases} (Q\&S) \\ \otimes \\ (C\&F) \\ \otimes \\ (B\&(P \oplus T)) \end{cases}$$

We can recognize here some of the meanings that we already discussed. The right of the sequent is what you can get for 17 Euros. The tensor tells that for this price you get one "entrée", one dish and one dessert. The difference between & and $\oplus$ is a bit more subtle, and the game interpretation is helpful here. So let us start again from the beginning, considering a play between the restaurant manager (the Player) and the customer (the Opponent). It is the Player's responsibility to split the $17E$ into three parts, corresponding to the cost of the three parts of the meal. May be, this is done as follows:

$$\frac{5E \vdash Q\&S \quad 8E \vdash C\&F \quad 4E \vdash B\&(P \oplus T)}{17E \vdash (Q\&S) \otimes (C\&F) \otimes (B\&(P \oplus T))}$$

Now let the Opponent challenge $5E \vdash Q\&S$:

$$\frac{5E \vdash Q \quad 5E \vdash S}{5E \vdash Q \& S}$$

which reads as: both Quiche and Salad are available to the customer, but he can get only one, and it is *his* choice of picking one of the antecedents and to order, say, a Quiche. Thus the additive conjunction can be understood as a ... disjunction embodying a notion of *external choice* (remember that in our example the customer is the Opponent, or the context, or the environment). Let us now analyse a proof of $4E \vdash B \& (P \oplus T)$:

$$\frac{4E \vdash B \quad \dfrac{4E \vdash T}{4E \vdash P \oplus T}}{4E \vdash B \& (P \oplus T)}$$

Suppose that the Opponent chooses the Surprise. Then it is the Player's turn, who justifies $4E \vdash P \oplus T$ using the right $\oplus$ rule. So, the Opponent will get a Tarte Tatin, but the choice was in the Player's hands. Thus $\oplus$ has an associated meaning of *internal choice*. In summary, two forms of choice, external and internal, are modelled by $\&$ and $\oplus$, respectively. In the case of $\oplus$, whether A or B is chosen is controlled by the rule, that is, by the Player. In the case of $\&$, the choice between A or B is a choice of one of the antecedents of the rule, and is in the hands of the Opponent.

Actually, our image becomes even more acurate if we replace the customer with an inspector (in summer, many restaurants propose unreasonable prices to the tourists...). The inspector will not consume the whole menu, he will just check (his choice!) whether what is offered, say for the entrée, is correct (not over-priced, fresh enough...). Another inspector, or the same inspector, may want to do another experiment later, checking this time on dessert: using this sharper personification, the game as explained above is more fully reflected.

All these oppositions confirm a fundamental *polarity*: by convention, we shall term $\&$ and $\parr$ as *negative*, and $\otimes$ and $\oplus$ as *positive*.

The part of linear logic introduced so far is called multiplicative additive (MALL).

3 Full linear logic

In order to recover the power of the full λ-calculus (or of intuitionistic logic), we reintroduce the structural rules, but only on formulas marked with a modality (actually two: "!" and its dual "?"):

$$\frac{\vdash ?A, ?A, \Gamma}{\vdash ?A, \Gamma} \qquad \frac{\vdash \Gamma}{\vdash ?A, \Gamma}$$

The rules are easier to explain in a bilateral format. If you want to prove $!A, \Gamma \vdash B$, then contraction allows you to give yourself the freedom of using the assumption $!A$ twice, or more: if you have been able to prove $!A, \ldots, !A, \Gamma \vdash B$, then you can conclude by using (repeated) contractions. Similarly, weakening allows you to forget assumptions of the form $!A$: having a proof of $\Gamma \vdash B$ is enough to get $!A, \Gamma \vdash B$.

The connective ! is a connective just as the others, and thus has its left and right introduction rules (?Γ denotes a multiset of formulas each of the form ?A):

$$\textbf{Dereliction}\ \frac{\vdash \Gamma, A}{\vdash \Gamma, ?A} \qquad \textbf{Promotion}\ \frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A}$$

In bilateral form, dereliction tells us that if, say, $A \vdash B$, then also $!A \vdash B$, but one looses the precious information that B "costs" only one A. Promotion tells us that if, say, $!B \vdash A$, then $!B \vdash !A$: suppose for example that 3 B's are needed to get A, then we can get 2 A's using 6 B's (and $!A$ represents as many A's as we wish).

Our description of linear logic (LL) is now complete! The two connectives ! and ? are called the **EXPONENTIALS**.

A variation on the promotion rule, which is inspired by categorical considerations (see section 7), is:

$$\frac{\vdash \Gamma, A}{\vdash ?\Gamma, !A} \qquad \frac{\vdash ??A, \Gamma}{\vdash ?A, \Gamma}$$

These two rules together are equivalent to the promotion rule. We just show here how the second rule can be derived:

$$\dfrac{\vdash ??A, \Gamma \qquad \dfrac{\dfrac{}{\vdash !A^{\perp}, ?A}}{\vdash !!A^{\perp}, ?A}}{\vdash ?A, \Gamma}$$

For intuitionistic or classical sequent calculus, the key result to establish in order to be able to make some use of it is the *cut-elimination* theorem. It holds here too (for a proof, see for example the appendix of [21]). It has such consequences as, e.g., the disjunction property, which in linear logic concerns the $\oplus$: if $\vdash A \oplus B$ is provable, then either $\vdash A$ or $\vdash B$ is provable. This is because a cut-free proof of $\vdash A \oplus B$ can only end with one of the two $\oplus$ rules. In particular, the formula cannot have been proved using a contraction, since it does not carry the modality ?. (Note that the argument for the disjunction property in intuitionistic logic is similar, and uses the impossibility of using the contraction rule on the right of the $\vdash$: it is the only role of the constraint of having at most one formula on the right of $\vdash$).

We shall now give the cut-elimination rules of linear logic. To start with, we give two important rules:

$$\dfrac{\dfrac{}{\vdash A^{\perp}, A} \qquad \begin{matrix}\Pi \\ \vdots \\ \vdash A^{\perp}, \Gamma\end{matrix}}{\vdash A^{\perp}, \Gamma} \quad \longrightarrow \quad \begin{matrix}\Pi \\ \vdots \\ \vdash A^{\perp}, \Gamma\end{matrix}$$

$$\dfrac{\dfrac{\Pi}{\vdots}\ \vdash \Gamma_1, ?B^\perp, ?B^\perp}{\vdash \Gamma_1, ?B^\perp}\quad \dfrac{\dfrac{\Pi'}{\vdots}\ \vdash ?\Gamma_2, B}{\vdash ?\Gamma_2, !B}}{\vdash \Gamma_1, ?\Gamma_2} \quad\longrightarrow\quad \dfrac{\dfrac{\dfrac{\Pi}{\vdots}\ \vdash \Gamma_1, ?B^\perp, ?B^\perp}{\vdash \Gamma_1, ?B^\perp}\quad \dfrac{\dfrac{\Pi'}{\vdots}\ \vdash ?\Gamma_2, B}{\vdash ?\Gamma_2, !B}}{\vdash \Gamma_1, ?\Gamma_2, ?\Gamma_2}}{\vdash \Gamma_1, ?\Gamma_2}$$

The second rule illustrates duplication of proofs, while the first one is the reinsuring one: cuts may vanish! Next, we introduce the other cut-elimination rules along a working example, which highlights an important isomorphism of linear logic: $!(A\&B) \equiv (!A) \otimes (!B)$ (from which the name exponential comes: think of "$e^{A+B} = e^A \times e^B$"). The equiprovability of the two formulas is shown as follows (of course, we are doing the same job as at the beginning of section 2):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}}{\vdash ?A^\perp, A}}{\vdash ?A^\perp, ?B^\perp, A}\quad \dfrac{\dfrac{\dfrac{}{\vdash B^\perp, B}}{\vdash ?B^\perp, B}}{\vdash ?A^\perp, ?B^\perp, B}}{\vdash ?A^\perp, ?B^\perp, A\&B}}{\vdash ?A^\perp, ?B^\perp, !(A\&B)}}{\vdash ?A^\perp \parr ?B^\perp, !(A\&B)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp}}{\vdash A, (A^\perp \oplus B^\perp)}}{\vdash A, ?(A^\perp \oplus B^\perp)}\quad \dfrac{\dfrac{\dfrac{}{\vdash B, B^\perp}}{\vdash B, (A^\perp \oplus B^\perp)}}{\vdash B, ?(A^\perp \oplus B^\perp)}}{\vdash !A, ?(A^\perp \oplus B^\perp)\quad \vdash !B, ?(A^\perp \oplus B^\perp)}}{\vdash !A \otimes !B, ?(A^\perp \oplus B^\perp), ?(A^\perp \oplus B^\perp)}}{\vdash !A \otimes !B, ?(A^\perp \oplus B^\perp)}$$

Let us now introduce a cut at the bottom of the two proofs:

$$\dfrac{\dfrac{\vdots}{\vdash ?A^\perp \parr ?B^\perp, !(A\&B)}\qquad \dfrac{\vdots}{\vdash !A \otimes !B, ?(A^\perp \oplus B^\perp)}}{\vdash !(A\&B), ?(A^\perp \oplus B^\perp)}$$

Our goal is to eliminate this cut. The formula $?A^\perp \parr ?B^\perp$ which is cut in the left sequent is principal (i.e., is introduced by the rule that precedes), while its dual on the right is not: the preceding rule is a contraction on a different formula. In such cases, one performs a so-called *commutative conversion*, which brings the cut one step up on the left and leaves the contraction as the final step of our cut-free proof:

$$\dfrac{\dfrac{\vdots}{\vdash ?A^\perp \parr ?B^\perp, !(A\&B)} \qquad \dfrac{\vdots}{\vdash !A \otimes !B, ?(A^\perp \oplus B^\perp), ?(A^\perp \oplus B^\perp)}}{\dfrac{\vdash !(A\&B), ?(A^\perp \oplus B^\perp), ?(A^\perp \oplus B^\perp)}{\vdash !(A\&B), ?(A^\perp \oplus B^\perp)}}$$

Now the two dual formulas of the cut are both active. In this case, the $\parr$ rule and the $\otimes$ rule are both "consumed", and the cut is transformed in two cuts on the smaller formulas $!A$ and $!B$, in some order which should be irrelevant), say:

$$\dfrac{\dfrac{\Pi_1}{\vdots}{\vdash A^\perp, B^\perp, \Gamma_1} \qquad \dfrac{\Pi_2}{\vdots}{\vdash A, \Gamma_2} \quad \dfrac{\Pi_3}{\vdots}{\vdash B, \Gamma_3}}{\dfrac{\vdash A^\perp, B^\perp, \Gamma_1}{\vdash \Gamma_1, \Gamma_2, \Gamma_3} \qquad \dfrac{\vdash A \otimes B, \Gamma_2, \Gamma_3}{\vdash \Gamma_1, \Gamma_2, \Gamma_3}} \quad \longrightarrow \quad \dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}{\vdash A^\perp, B^\perp, \Gamma_1} \quad \dfrac{\Pi_2}{\vdots}{\vdash A, \Gamma_2}}{\vdash B^\perp, \Gamma_1, \Gamma_2} \qquad \dfrac{\Pi_3}{\vdots}{\vdash B, \Gamma_3}}{\vdash \Gamma_1, \Gamma_2, \Gamma_3}$$

Applying this rule to our example, we get:

$$\dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}{\vdash ?A^\perp, ?B^\perp, !(A\&B)} \quad \dfrac{\Pi_2}{\vdots}{\vdash !A, ?(A^\perp \oplus B^\perp)}}{\vdash ?B^\perp, !(A\&B), ?(A^\perp \oplus B^\perp)} \qquad \dfrac{\Pi_3}{\vdots}{\vdash !B, ?(A^\perp \oplus B^\perp)}}{\dfrac{\vdash !(A\&B), ?(A^\perp \oplus B^\perp), ?(A^\perp \oplus B^\perp)}{\vdash !(A\&B), ?(A^\perp \oplus B^\perp)}}$$

We first concentrate on eliminating the inner cut, over $!A$. The last rule of Π_2 is a promotion, but there is no immediate way to transform the cut into a cut on the smaller formula A. We permute the cut with the promotion and the $\&$ rules of Π_1, yielding:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A^\perp, A}}{\vdash ?A^\perp, A} \quad \dfrac{\Pi_2}{\vdots}{\vdash !A, ?(A^\perp \oplus B^\perp)}}{\vdash ?A^\perp, ?B^\perp, A} \qquad \dfrac{\dfrac{\dfrac{}{\vdash B^\perp, B}}{\vdash ?B^\perp, B} \quad \dfrac{\Pi_2}{\vdots}{\vdash !A, ?(A^\perp \oplus B^\perp)}}{\vdash ?A^\perp, ?B^\perp, B}}{\dfrac{\vdash ?B^\perp, A, ?(A^\perp \oplus B^\perp) \qquad \vdash ?B^\perp, B, ?(A^\perp \oplus B^\perp)}{\vdash ?B^\perp, (A\&B), ?(A^\perp \oplus B^\perp)}}}{\vdash ?B^\perp, !(A\&B), ?(A^\perp \oplus B^\perp)}$$

Let us now pursue the elimination of the left cut. It commutes with the weakening, after which a new true cut elimination step occurs, that consumes a dereliction on the left and the promotion of Π_2 on the right. The general form of the rule is:

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1\\ \vdots\\ \vdash A^\perp, \Delta\end{array}}{\vdash ?A^\perp, \Gamma} \quad \dfrac{\begin{array}{c}\Pi_2\\ \vdots\\ \vdash A, ?\Delta\end{array}}{\vdash !A, ?\Delta}}{\vdash \Gamma, ?\Delta} \quad \longrightarrow \quad \dfrac{\begin{array}{c}\Pi_1\\ \vdots\\ \vdash A^\perp, \Gamma\end{array} \quad \begin{array}{c}\Pi_2\\ \vdots\\ \vdash A, ?\Delta\end{array}}{\vdash \Gamma, ?\Delta}$$

In the present case, we get (after elimination of the topmost left axiom using the first rule introduced above):

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp}}{\vdash A, (A^\perp \oplus B^\perp)}}{\vdash A, ?(A^\perp \oplus B^\perp)}}{\vdash ?B^\perp, A, ?(A^\perp \oplus B^\perp)}$$

The right cut is eliminated thanks to a new rule. If a principal $!A$ is cut against a $?A^\perp$ which has just been introduced by a weakening, then all the proof of $!A$ disappears, and the weakening is adjusted, as follows:

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1\\ \vdots\\ \vdash \Gamma\end{array}}{\vdash ?A^\perp, \Gamma} \quad \dfrac{\begin{array}{c}\Pi_2\\ \vdots\\ \vdash A, ?\Delta\end{array}}{\vdash !A, ?\Delta}}{\vdash \Gamma, ?\Delta} \quad \longrightarrow \quad \dfrac{\begin{array}{c}\Pi_1\\ \vdots\\ \vdash \Gamma\end{array}}{\vdash \Gamma, ?\Delta}$$

where the double line stands for possibly repeated weakenings. Coming back to our example, we get:

$$\dfrac{\dfrac{\dfrac{}{\vdash B^\perp, B}}{\vdash ?B^\perp, B}}{\vdash ?B^\perp, B, ?(A^\perp \oplus ?B^\perp)}$$

Putting the results together, we are left with the outer cut on $!B$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp}}{\vdash A, (A^\perp \oplus B^\perp)}}{\vdash A, ?(A^\perp \oplus B^\perp)}}{\vdash ?B^\perp, A, ?(A^\perp \oplus B^\perp)} \qquad \dfrac{\dfrac{\dfrac{}{\vdash B^\perp, B}}{\vdash ?B^\perp, B}}{\vdash ?B^\perp, B, ?(A^\perp \oplus ?B^\perp)}}{\dfrac{\vdash ?B^\perp, (A\&B), ?(A^\perp \oplus B^\perp)}{\dfrac{\vdash ?B^\perp, !(A\&B), ?(A^\perp \oplus B^\perp)}{\vdash !(A\&B), ?(A^\perp \oplus B^\perp), ?(A^\perp \oplus B^\perp)}} \qquad \begin{array}{c}\Pi_3 \\ \vdots \\ \vdash !B, ?(A^\perp \oplus B^\perp)\end{array}}$$

We don't need new rules for this, and we leave this last phase of elimination to the reader. The final cut-free proof is:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp}}{\vdash A, A^\perp \oplus B^\perp}}{\vdash A, ?(A^\perp \oplus B^\perp)}}{\vdash A, ?(A^\perp \oplus B^\perp), ?(A^\perp \oplus B^\perp)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash B, B^\perp}}{\vdash B, A^\perp \oplus B^\perp}}{\vdash B, ?(A^\perp \oplus B^\perp)}}{\vdash B, ?(A^\perp \oplus B^\perp), ?(A^\perp \oplus B^\perp)}}{\vdash A\&B, ?(A^\perp \oplus B^\perp), ?(A^\perp \oplus B^\perp)}}{\vdash !(A\&B), ?(A^\perp \oplus B^\perp), ?(A^\perp \oplus B^\perp)}}{\vdash !(A\&B), ?(A^\perp \oplus B^\perp)}$$

Remark 3.1 *Note that we do not get the most economical proof of this sequent, which can be proved using the axiom only. It is not either the most economical proof one would get by insisting in applying axioms only to the more atomic formulas A and B, but see Exercise 1.22 in part II. We just notice here that what we have done is to compose two proofs of $!(A\&B) \vdash !A \otimes !B$ and $!A \otimes !B \vdash !(A\&B)$. We could also have composed them the other way around, and would then have got a (non-economical) proof of $!A \otimes !B \vdash !A \otimes !B$.*

In part II (section 1), we shall present a better representation of proofs, called proof nets, which factor out irrelevant details, such as the order of the cuts in the $\otimes/\parr$ elimination or the contraction rule, and the commutative conversion rules (actually, all but one).

We end the section by giving a translation of (simply-typed) λ-calculus:

$$\frac{}{\Gamma, x : A \vdash x : A} \qquad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \to B} \qquad \frac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B}$$

into LL proofs. This translation takes (a proof of) a judgement $\Gamma \vdash M : A$ and turns it into

$$\text{a proof } [\![\Gamma \vdash M : A]\!] \text{ of } \vdash ?(\Gamma^*)^\perp, A^* \ ,$$

where * and $?(\Gamma^*)^\perp$ are defined as follows:

$$A^* = A \ \ (A \text{ atomic}) \qquad (B \to C)^* = ?(B^*)^\perp \parr C^* \qquad ?(\Gamma^*)^\perp = \{?(A^*)^\perp \mid A \in \Gamma\}$$

The reason why $\Gamma \vdash A$ becomes $\vdash ?\Gamma^\perp, A$ (or $!\Gamma \vdash A$) should be clear: a variable can have several occurrences in a term. Note that the translation uses multiplicative and exponential connectives only. (For the affine λ-calculus, only the multiplicative connectives are needed, cf. above.) The translation is as follows (we omit the * for a better readability):

Variable

$$[\![\Gamma, x : A \vdash x : A]\!] \ = \ \cfrac{\cfrac{}{\vdash A^\perp, A}}{\vdash ?\Gamma^\perp, A^\perp, A}$$

Abstraction

$$[\![\Gamma \vdash \lambda x.M : A \to B]\!] \ = \ \cfrac{\begin{array}{c}[\![\Gamma, x : A \vdash M : B]\!] \\ \vdots \\ \vdash ?\Gamma^\perp, ?A^\perp, B\end{array}}{\vdash ?\Gamma^\perp, (?A^\perp \parr B)}$$

Application

$$[\![\Gamma \vdash MN : B]\!] \ = \ \cfrac{\cfrac{\begin{array}{c}[\![\Gamma \vdash M : A \to B]\!] \\ \vdots \\ \vdash ?\Gamma^\perp, ?A^\perp \parr B\end{array} \qquad \cfrac{\cfrac{\begin{array}{c}[\![\Gamma \vdash N : A]\!] \\ \vdots \\ \vdash ?\Gamma^\perp, A\end{array}}{\vdash ?\Gamma^\perp, !A} \qquad \cfrac{}{\vdash B^\perp, B}}{\vdash ?\Gamma^\perp, !A \otimes B^\perp, B}}{\vdash ?\Gamma^\perp, ?\Gamma^\perp, B}}{\vdash ?\Gamma^\perp, B}$$

Of course, this is not enough to declare that we have a satisfactory translation. The translation should be also computationally sound, in the sense that if M reduces to N, then the translation of M reduces to the translation of N. It is the case with this translation, but it is not so immediate to establish, as the translation does two things at the same time: it factors a translation from intuitionistic natural deduction (NJ) to intuitionistic sequent calculus (LJ) and a translation of LJ to LL.

There are also other qualities that one may require of a translation: for example, that it should send cut-free proofs to cut-free proofs. Another (stronger) requirement is that the translation should

respect the skeleton of the translated proof, that is, the translation contents itself with introducing some derelictions and promotions in the original proof. We refrain from going into this here. Let us just say that the (LJ to LL part of the) above translation does not respect these two requirements, but other "more verbose" ones (i.e., using more occurrences of the modalities) do. A thorough analysis of the translations of intuitionistic (and also classical) logic in linear logic can be found in [6, 7] (see also [5]).

4 Proposition linear logic is undecidable

We are interested in the decidability of the following problem: given Γ, is $\vdash \Gamma$ provable? For MALL, this problem is decidable, as the possible cut-free proofs of a given sequent can be enumerated. This is because in a cut-free proof the formulas that can appear in the proof are subformulas of the formulas in the conclusion (this is the well-known *subformula property*), so there is a finite number of them, and moreover the absence of contraction guarantees that there are also finitely many possible sequents. Think of a proof of $\vdash \Gamma, A$ that would repeatedly apply contraction to A, thus searching $\vdash \Gamma, A, A$, $\vdash \Gamma, A, A, A, \ldots$. This is not allowed in MALL (since the exponentials are omitted). But the complexity is high, and in fact the problem is NP-complete (we refer to [21, Section 2] for the instructive and pleasing proof, which relies on an encoding of quantified boolean formulas in MALL).

What about full LL? It turns out that the Halting Problem for (a variant of) Two Counter Machines can be faithfully encoded in propositional linear logic, which entails the undecidability of the logic [21, Section 3]. (Note that this is in sharp contrast with classical propositional logic, for which decidability follows from the possibility of an exhaustive check of the truth values.) We next explain the encoding, and the structure of the proof of its faithfulness.

A Two Counter Machine (TCM) is given by a set S of *states*, with two distinguished states q_I and q_F (the *initial* and *final* states, respectively) and by 5 sets of *instructions* I_1, I_2, I_3, I_4, I_5, where I_1 through I_4 are subsets of $S \times S$ and I_5 is a subset of $S \times S \times S$. We use the following user-friendlier notation:

$$\left.\begin{array}{r} q_i \xrightarrow{+_A} q_j \\ q_i \xrightarrow{-_A} q_j \\ q_i \xrightarrow{+_B} q_j \\ q_i \xrightarrow{-_B} q_j \\ q_i \xrightarrow{fork} q_j, q_k \end{array}\right\} \text{ for } \left\{\begin{array}{l} (q_i, q_j) \in I_1 \\ (q_i, q_j) \in I_2 \\ (q_i, q_j) \in I_3 \\ (q_i, q_j) \in I_4 \\ (q_i, q_j, q_k) \in I_5 \end{array}\right.$$

These instructions act on *instantaneous descriptions* (ID's), which are multisets s of triplets of the form $(q, m, n) \in S \times \omega \times \omega$ (ω being the set of natural numbers), as follows (where union is taken in the sense of multisets, e.g. $\{x, y\} \cup \{x\} = \{x, x, y\}$):

$$\frac{q_i \xrightarrow{+_A} q_j \quad (q_i, m, n) \in s}{s \to s \setminus \{(q_i, m, n)\} \cup \{(q_j, m+1, n)\}} \qquad \frac{q_i \xrightarrow{-_A} q_j \quad (q_i, m, n) \in s \quad m > 0}{s \to s \setminus \{(q_i, m, n)\} \cup \{(q_j, m-1, n)\}}$$

$$\frac{q_i \xrightarrow{+_B} q_j \quad (q_i, m, n) \in s}{s \to s \setminus \{(q_i, m, n)\} \cup \{(q_j, m, n+1)\}} \qquad \frac{q_i \xrightarrow{-_B} q_j \quad (q_i, m, n) \in s \quad n > 0}{s \to s \setminus \{(q_i, m, n)\} \cup \{(q_j, m, n-1)\}}$$

$$\frac{q_i \xrightarrow{fork} q_j, q_k \quad (q_i, m, n) \in s}{s \to s \setminus \{(q_i, m, n)\} \cup \{(q_j, m, n), (q_k, m, n)\}}$$

Note that the instructions $-_A$ and $-_B$ can only act on triplets of the form (q, m, n) with $m > 0$ and $n > 0$, respectively. A triplet (q, m, n) formalizes a machine in state q whose two counters A and B hold values $m \geq 0$ and $n \geq 0$, respectively. The last type of instructions is what makes these TCM's a variant of the standard ones, which have instead two zero-test instructions for the two counters A, B, and which act on triplets (q, m, n), rather than on multisets of such triplets (see Exercise 4.3). The *fork* instruction necessitates these more complicated instantaneous descriptions, which formalize a cluster of machines working in parallel, one for each triplet, or local ID, of the multiset. A fork instruction executed by one of the machines M can be understood as launching a new TCM M' with initial local ID, say, (q_k, m, n), while M evolves to local ID (q_j, m, n). The counters are local to the machines, hence the counters of M' can later evolve differently from the counters of M.

We are now ready for the encoding. States are encoded as (distinct) atomic formulas of the same name. Moreover, we pick two fresh distinct atomic formulas a and b, and we set $a^0 = 1$, $a^1 = a$, and $a^{n+1} = a^n \otimes a$, and similarly for b. The fact that counter A holds value n will be encoded by the formula a^n. We next encode rules as follows:

$$\left.\begin{array}{r} q_i \xrightarrow{+_A} q_j \\ q_i \xrightarrow{-_A} q_j \\ q_i \xrightarrow{+_B} q_j \\ q_i \xrightarrow{-_B} q_j \\ q_i \xrightarrow{fork} q_j, q_k \end{array}\right\} \text{ for } \left\{\begin{array}{l} q_i \multimap (q_j \otimes a) \\ (q_i \otimes a) \multimap q_j \\ q_i \multimap (q_j \otimes b) \\ (q_i \otimes b) \multimap q_j \\ q_i \multimap (q_j \oplus q_k) \end{array}\right.$$

One reads, say, the first kind of rules as: "exchange q_i for q_j and for one more a" (incrementing the counter A). We shall soon see why $\oplus$ is the right connective to use for the fifth sort of rules. Formally, we interpret each rule as a formula, as follows:

$$\begin{array}{l} [\![q_i \xrightarrow{+_A} q_j]\!] = ?((q_i^\perp \parr (q_j \otimes a))^\perp) \\ [\![q_i \xrightarrow{-_A} q_j]\!] = ?(((q_i \otimes a)^\perp \parr q_j)^\perp) \\ [\![q_i \xrightarrow{+_B} q_j]\!] = ?((q_i^\perp \parr (q_j \otimes b))^\perp) \\ [\![q_i \xrightarrow{-_B} q_j]\!] = ?(((q_i \otimes b)^\perp \parr q_j)^\perp) \\ [\![q_i \xrightarrow{fork} q_j, q_k]\!] = ?((q_i^\perp \parr (q_j \oplus q_k))^\perp) \end{array}$$

The reason for the $?((\_)^\perp)$ format is that we want to be able to use the encodings of rules as axioms, whenever needed, and hence possibly repetitively. We write $\vdash' \Gamma$ for $\vdash \Gamma \cup [\![I_1]\!] \cup [\![I_2]\!] \cup [\![I_3]\!] \cup [\![I_4]\!] \cup [\![I_5]\!]$.

Proposition 4.1 *Let M be a TCM, and s be an ID for M. Then M accepts from s (i.e., there exists a sequence of transitions $s \to^* s'$ where s' consists only of identical triplets $(q_F, 0, 0)$) if and only if, for every triplet $(q, m, n) \in s$, the sequent $\vdash' q^\perp, (a^m)^\perp, (b^n)^\perp, q_F$ is provable.*

Informally, the characterization in the statement reads as: for any triplet (q, m, n) of s, assuming $q \otimes a^m \otimes b^n$ and all the (encodings of the) rules, we can deduce q_F. Let us observe that M accepts from s if and only it accepts from each of the members of s, since each triplet of s' can be traced back to exactly one triplet of s, whence the "for all" form of the statement.

PROOF (INDICATION). We first sketch the easy part of the proof, namely that accepting implies provable. The proof is by induction on the length of the reduction $s \to^* s'$. In the base case we have $s = s'$, hence all the elements of s are $(q_F, 0, 0)$, and the conclusion holds by weakening of the axiom $\vdash q_F^\perp, q_F$. So, let $s \to s_1 \to^* s'$. If $s_1 = s \setminus \{(q_i, m, n)\} \cup \{(q_j, m+1, n)\}$, then all we are left to prove is that $\vdash' q_i^\perp, (a^m)^\perp, (b^n)^\perp, q_F$, knowing that $\vdash' q_j^\perp, (a^{m+1})^\perp, (b^n)^\perp, q_F$. The proof is as follows:

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash' q_j^\perp, (a^{m+1})^\perp, (b^n)^\perp, q_F}}{\vdash' q_j^\perp \parr a^\perp, (a^m)^\perp, (b^n)^\perp, q_F} \qquad \dfrac{\dfrac{\vdash (q_i^\perp \parr (q_j \otimes a))^\perp, q_i^\perp \parr (q_j \otimes a)}{\vdash ?((q_i^\perp \parr (q_j \otimes a))^\perp), q_i^\perp \parr (q_j \otimes a)}}{\vdash ?((q_i^\perp \parr (q_j \otimes a))^\perp), q_i^\perp, q_j \otimes a}}{\dfrac{\vdash' ?((q_i^\perp \parr (q_j \otimes a))^\perp), q_i^\perp, (a^m)^\perp, (b^n)^\perp, q_F}{\vdash' q_i^\perp, (a^m)^\perp, (b^n)^\perp, q_F}}$$

(modulo the reversibility of $\parr$, and using the contraction rule at the end). We chek the case $s_1 = s \setminus \{(q_i, m, n)\} \cup \{(q_j, m, n), (q_k, m, n)\}$ similarly, as follows:

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash' q_j^\perp, (a^m)^\perp, (b^n)^\perp, q_F} \qquad \dfrac{\vdots}{\vdash' q_k^\perp, (a^m)^\perp, (b^n)^\perp, q_F}}{\vdash' q_j^\perp \& q_k^\perp, (a^m)^\perp, (b^n)^\perp, q_F} \qquad \dfrac{\vdots}{\vdash' q_i^\perp, q_j \oplus q_k}}{\vdash' q_i^\perp, (a^m)^\perp, (b^n)^\perp, q_F}$$

Note that from a dialogue game point of view, the opponent of the proof has the choice of which triplet to check, either (q_j, m, n) or (q_k, m, n), whence the presence of the external choice connective & in the encoding $?(q_i \otimes (q_j^\perp \& q_k^\perp))$ of the fork rule.

The converse direction (provable implies accepting) goes by analysing the cut-free proofs of the encodings of acceptation, and by showing that they are essentially unique and that one can read back an accepting sequence of transitions. □

Since given M and s it is undecidable whether M accepts from s, we conclude by reduction that LL is undecidable.

Exercise 4.2 *Formalize the proof of decidability of MALL outlined above. Hints: (1) associate with each sequent $\vdash \Delta$ a complexity measure $c(\vdash \Delta)$ such that for each instance of a MALL rule:*

$$\dfrac{\textit{antecedent 1} \quad \ldots \quad \textit{antecedent n}}{\textit{conclusion}}$$

we have $c(\textit{antecedent } i) < c(\textit{conclusion})$ for all i; (2) then show that the set of "possible proofs" of a sequent (i.e., the trees whose internal nodes correspond to correct applications of the rules of MALL and whose leaves are sequents $\vdash \Gamma$ where Γ consists of atomic formulas only) can be effectively

generated; (3) then show that one can effectively check which among these "possible proofs" are real proofs (look at the leaves).

Exercise 4.3 *In a standard TCM, fork instructions are replaced by two sets of instructions of the form* $q_i \xrightarrow{0_A} q_j$ *and* $q_i \xrightarrow{0_B} q_j$*, respectively, and the transitions transform triplets, as follows:*

$$\frac{q_i \xrightarrow{+_A} q_j}{(q_i, m, n) \to (q_j, m+1, n)} \qquad \cdots \qquad \frac{q_i \xrightarrow{0_A} q_j}{(q_i, 0, n) \to (q_j, 0, n)} \qquad \frac{q_i \xrightarrow{0_B} q_j}{(q_i, m, 0) \to (q_j, m, 0)}$$

Show that for any standard TCM M *one can build a variant TCM* M' *as defined here, whose collection of states contains the collection of states of* M*, which is such that the machine* M *accepts from a triple* (q, m, n) *(i.e.,* $(q, m, n) \to^* (q_F, 0, 0)$*) if and only if* M' *accepts from* s *(in the sense of Proposition 4.1). (Hints: Show that one can restrict attention to a TCM* M *with no outgoing transitions from its final state. Use two new states* Z_A *and* Z_B *and replace the zero-test instructions by suitable fork instructions involving these new states.)*

5 Phase semantics

Phase semantics is a semantics of provability. Like in Kripke models for modal logics or intuitionisitic logic, a formula is not true or false, we rather have ways to express the extent to which it is true. In Kripke semantics, the meaning of a formula is the set of so-called worlds at which it holds. In phase semantics, a similar, but more structured, notion of *phases* is used. Formulas are interpreted by *facts*, which are well-behaved sets of phases.

When setting up a notion of model, one has in mind both soundness and completeness of the class of models to be defined. This class must be large enough to include most natural examples of candidate models, and in particular it must contain the candidate *syntactic model* which will serve to prove completeness. As a guide to the understanding of the notion of phase space, we expose first what this syntactic model looks like. Its phases are just sequences of formulas. The intention is that the interpretation of a formula A in this model is the set of all Γ's such that $\vdash \Gamma, A$. The soundness theorem will have the following form: if $\vdash A$, then A is valid, in the following sense: the special phase 1 (think of it as expressing the certitude that A holds) belongs to the interpretation of A. In the syntactic model, 1 will be the empty sequence of formulas. Thus, in this model, the validity of A is exactly the provability of $\vdash \emptyset, A$, i.e., of $\vdash A$. With these preparations, we can now define phase spaces. We deal with MALL first.

Definition 5.1 *A* phase space *is a pair* $(P, \bot)$ *where* P *is a commutative monoid (in multiplicative notation:* pq*,* 1*) and* $\bot \subseteq M$ *is a distinguished subset of* antiphases*. One defines the following operation on subsets of* P*:* $X^\bot = \{q \mid \forall p \in X \;\; pq \in \bot\}$*.*

It may be useful to think of the q's as observers of the elements of X and of $pq \in \bot$ as a form of agreement between the observer q and the observed p (somehow, a degenerated form of the kind of dialogue described in section 2, and in part II (section 5)). We may say that "p passes the test q" when $pq \in \bot$. A *fact* is a subset $F \subseteq P$ such that $F^{\bot\bot} = F$.

The following properties are easy to check, and the reader must have seen them somewhere already (linear algebra!):

$X \subseteq Y \Rightarrow Y^\perp \subseteq X^\perp$
$X \subseteq X^{\perp\perp}$
$X^\perp = X^{\perp\perp\perp}$
F is a fact if and only if $F = X^\perp$ for some X
$(X \cup Y)^\perp = X^\perp \cap Y^\perp$

Thus a fact is a set of elements that pass the same tests, an idea which will be re-used in the richer setting of ludics. Notice also that facts obey $F^{\perp\perp} = F$, so that $^\perp$ is suitable for interpreting the linear negation, provided all formulas are interpreted by facts. Notice also that $\perp = \{1\}^\perp$, hence $\perp$ is a fact, which we use to interpret the constant $\perp$. Also, $P = \emptyset^\perp$ is a fact.

We now define the various connectives as operations on facts. We write $XY = \{pq \mid p \in X, q \in Y\}$.

$$F \otimes G = (FG)^{\perp\perp} \qquad \top = \emptyset^\perp \qquad F\&G = F \cap G\ .$$

The rest can be deduced by duality:

$$F⅋G = (F^\perp G^\perp)^\perp \quad F \oplus G = (F \cup G)^{\perp\perp} \quad 0 = P^\perp \quad 1 = \perp^\perp$$

(recall that $\perp$ is interpreted by $\perp$). This determines the interpretation of formulas, provided we have assigned facts to atomic formulas. We freely say that A is interpreted by A, and if $\Gamma = A_1, \ldots, A_n$, we also write freely Γ for (the interpretation of) $A_1⅋\ldots⅋A_n$. The soundness theorem is stated as follows:

Proposition 5.2 *For any interpretation in a phase space, if $\vdash A_1, \ldots, A_n$, then $1 \in A_1⅋\ldots⅋A_n$ (we say that $A_1, \ldots, A_n$ is valid).*

Proof. We just check the case of $\perp$. Suppose $1 \in \Gamma$. We have to show that $1 \in (\Gamma^\perp \perp^\perp)^\perp$, i.e., that $\Gamma^\perp \perp^\perp \subseteq \perp$. Let $p \in \Gamma^\perp$ and $q \in \perp^\perp$. Since $1 \in \Gamma$, we have $p \in \perp$, and since $q \in \perp^\perp$ we have $pq \in \perp$. □

The following is a less symmetric, but more intuitive characterization of the notion of validity.

Lemma 5.3 *For any $\Gamma = A_1, \ldots, A_n$, and any $1 \leq i \leq n$, Γ is valid if and only if (the interpretation of) $A_i^\perp$ is included in (the interpretation of) $A_1⅋\ldots⅋A_{i-1}⅋A_{i+1}⅋\ldots⅋A_n$.*

Proof. For simplicity, we take $n = 2$, and we set $A_1^\perp = A$ and $A_2 = B$. We have:

$$1 \in (A^{\perp\perp} B^\perp)^\perp \Leftrightarrow A^{\perp\perp} B^\perp \subseteq \perp \Leftrightarrow A^{\perp\perp} \subseteq B^{\perp\perp} \Leftrightarrow A \subseteq B\ .$$

□

Hence, if $A \approx B$, i.e., if $A \vdash B$ and $B \vdash A$, then A and B are interpreted by the same fact. In particular, we have that $F⅋(G\&H) = (F⅋G)\&(F⅋H)$, for arbitrary facts F, G, H (take the formulas $P⅋(Q\&R)$ and $(P⅋Q)\&(P⅋R)$, with P, Q, R atomic and interpreted by F, G, H, respectively). As an exercise, we provide below an ad hoc proof of this equality, which makes use of the following property.

Lemma 5.4 *Let $X, Y \subseteq P$. The following inclusion holds: $X^{\perp\perp} Y^{\perp\perp} \subseteq (XY)^{\perp\perp}$.*

PROOF. We have to show that $pqr \in \bot$ for any $p \in X^{\bot\bot}$, $q \in Y^{\bot\bot}$ and $r \in (XY)^\bot$. Taking some $f \in X$, we get that $rf \in Y^\bot$, hence $q(rf) = (rq)f \in \bot$. Since this was for arbitrary $f \in X$, we get $rq \in X^\bot$, and $p(rq) = pqr \in \bot$. □

We have to prove $(F^\bot(G \cap H)^\bot)^\bot = (F^\bot G^\bot)^\bot \cap (F^\bot H^\bot)^\bot$. The right hand side can be rewritten as follows:

$$(F^\bot G^\bot)^\bot \cap (F^\bot H^\bot)^\bot = (F^\bot G^\bot \cup F^\bot H^\bot)^\bot = (F^\bot(G^\bot \cup H^\bot))^\bot \ .$$

Then we observe that $G \cap H \subseteq G$ entails $(G \cap H)^\bot \supseteq G^\bot$. Similarly, we have $(G \cap H)^\bot \supseteq H^\bot$. Hence $F^\bot(G \cap H)^\bot \supseteq F^\bot(G^\bot \cup H^\bot)$, from which $(F^\bot(G \cap H)^\bot)^\bot \subseteq (F^\bot(G^\bot \cup H^\bot))^\bot$ follows. For the converse direction, we exploit the information that F, G, H are facts, i.e., that $F = X^\bot$, $G = Y^\bot$, and $H = Z^\bot$ for some subsets X, Y, Z of P. We have then, using Lemma 5.4:

$$\begin{array}{rcl} (F^\bot(G \cap H)^\bot)^\bot = (X^{\bot\bot}(Y^\bot \cap Z^\bot)^\bot)^\bot & = & (X^{\bot\bot}((Y \cup Z)^{\bot\bot})^\bot \\ & \supseteq & (X(Y \cup Z))^{\bot\bot\bot} \\ & = & (X(Y \cup Z))^\bot \\ & \supseteq & (X^{\bot\bot}(Y^{\bot\bot} \cup Z^{\bot\bot}))^\bot = (F^\bot(G^\bot \cup H^\bot))^\bot \ . \end{array}$$

We now define the syntactic model. As announced, P is the set of the $\Gamma = A_1 \dots A_n$'s (up to the order of the formulas), written by juxtaposition (the monoid is given by concatenation), and $\bot = \{\Gamma \mid \vdash \Gamma\}$.

Proposition 5.5 *Phase spaces form a complete class of models, i.e., if a MALL formula A is valid in all phase spaces, then $\vdash A$.*

PROOF. We set $Pr(A) = \{\Gamma \mid \vdash \Gamma, A\}$. We show by induction that the interpretation of A in the syntactic model is $Pr(A)$, and we conclude then as indicated at the beginning of the section: if A is valid, then $\emptyset \in Pr(A)$, i.e., $\vdash A$ is provable. For atomic formulas, we just fix the intepretation of A to be $Pr(A)$, but to this aim we must first verify that $Pr(A)$ is a fact, which we prove for an arbitrary formula A. We have to show that if $\Delta \in Pr(A)^{\bot\bot}$, then $\vdash \Delta, A$. It follows easily from the fact that $A \in Pr(A)^\bot$. We check only that $Pr(A \otimes B) \subseteq (Pr(A)Pr(B))^{\bot\bot}$. Let $X = Pr(A)Pr(B) = \{\Gamma_1\Gamma_2 \mid \vdash A, \Gamma_1 \text{ and } \vdash B, \Gamma_2\}$. We have to prove that if $\Delta \in X^\bot$, then, for all Γ, $\vdash A \otimes B, \Gamma$ entails $\vdash \Gamma, \Delta$. We notice that $A^\bot B^\bot \in X$ since $\vdash A^\bot, A$ and $\vdash B^\bot, B$. Hence $\vdash A^\bot, B^\bot, \Delta$, and:

$$\dfrac{\vdash A \otimes B, \Gamma \qquad \dfrac{\vdash A^\bot, B^\bot, \Delta}{\vdash A^\bot \parr B^\bot, \Delta}}{\vdash \Gamma, \Delta}$$

□

We next give the phase semantics of exponentials. Like for intuitionistic logic, topological ideas are useful. In the case of intuitionistic logic, in order to avoid the tautology (A or $\neg A$), one interprets, say, $\neg A$ by the interior of the complement of A in some topology. In the case of linear logic, we still have to choose the right infinite conjunction and the finite disjunction used to define the "closed" sets.

Definition 5.6 *A* topolinear *space is a structure* $(P, \bot, \mathbf{F})$*, where* $(P, \bot)$ *is a phase space, and where* $\mathbf{F}$ *is a set of facts that satisfies the following conditions:*

(1) $\mathbf{F}$ *is closed by arbitrary intersections,*
(2) $\mathbf{F}$ *is closed by (finite)* $\parr$*, and (in particular)* $\bot \in \mathbf{F}$*,*
(3) $\bot$ *is the smallest fact of* $\mathbf{F}$*,*
(4) $F \parr F \in \mathbf{F}$*, for all* $F \in \mathbf{F}$*.*

The facts of $\mathbf{F}$ *are called the* closed *facts. Given a fact* F*, we define* $?F$ *as the smallest closed fact containing* F*.*

Notice that, defining the open facts as the orthogonals of closed facts, we get a definition of $!F$ as the largest open fact contained in F.

The soundness theorem extends to full LL. For weakening, we proceed exactly as for the $\bot$ rule, using $\bot \subseteq ?A$. The validity of contraction is an obvious consequence of axiom (4). Using Lemma 5.3, the validity of dereliction and of promotion are immediate consequences of the axioms (3) and (2), respectively.

To prove completeness, we extend the definition of the syntactic model as follows. We take as closed facts arbitrary intersections of sets of the form $Pr(?A)$. Let us verify that this collection is closed under finite $\parr$'s. We have proved $F \parr (G \with H) = (F \parr G) \with (F \parr H)$ above. The infinitary version of this equality is proved in the same way, so that we get:

$$\begin{array}{rcl} (\bigcap_{i\in I} Pr(?A_i)) \parr (\bigcap_{j\in J} Pr(?B_j)) & = & \bigcap_{i\in I, j\in J} (Pr(?A_i) \parr Pr(?B_j)) \\ & = & \bigcap_{i\in I, j\in J} Pr(?A_i \parr ?B_j) \\ & = & \bigcap_{i\in I, j\in J} Pr(?(A_i \oplus B_j)) \end{array}$$

where the last equality follows from $?A_i \parr ?B_j \approx ?(A_i \oplus B_j)$. Also, $\bot$ is a closed fact since $\bot \approx ?0$, and it is the smallest one, by the weakening rule. Axiom (4) is the consequence of two observations:

$$(\dagger) \quad ?A \approx ?A \parr ?A \qquad\qquad (\ddagger) \quad ?A_i \vdash ?A_i, ?A_j \ .$$

($\dagger$) follows from $A \vdash A \oplus A$ (by either of the $\oplus$ rules) and from $\vdash A^\bot \with A^\bot, A$, and ($\ddagger$) is immediate by weakening. Then we have:

$$\begin{array}{rcll} (\bigcap_{i\in I} Pr(?A_i)) \parr (\bigcap_{j\in J} Pr(?A_j)) & = & \bigcap_{i\in I, j\in J} (Pr(?A_i) \parr Pr(?A_j)) & \\ & = & \bigcap_{i\in I} (Pr(?A_i) \parr Pr(?A_i)) & \text{by } (\ddagger) \\ & = & \bigcap_{i\in I} Pr(?A_i) & \text{by } (\dagger) \end{array}$$

Thus the syntactic structure is a topolinear space.

We have to prove that $Pr(?A) = \bigcap \{Pr(?B) \mid Pr(A) \subseteq Pr(?B)\}$. Since $Pr(A) \subseteq Pr(?A)$ by dereliction, we have one inclusion. For the other, we have to show that if $Pr(A) \subseteq Pr(?B)$ then $Pr(?A) \subseteq Pr(?B)$. So let $\vdash \Gamma, ?A$. Since $Pr(A) \subseteq Pr(?B)$, then in particular $\vdash A^\bot, ?B$, hence $\vdash !A^\bot, ?B$ by promotion. We conclude that $\Gamma \in Pr(?B)$ by using the cut rule. This completes the proof of completeness.

6 Coherence spaces

With coherence spaces, we give a semantics of proofs. Coherence spaces may be understood as concrete descriptions of certain sets or *domains*, in the terminology of denotational semantics. They are a simplified version of event structures [25].

Definition 6.1 *A* coherence space $(E, \frown)$ *(E for short) is given by a set E of* events*, or tokens, and by a reflexive and symmetric relation* $\frown \subseteq E \times E$*. E is called the* web *of* $(E, \frown)$*. A state, or* clique*, of E is a set x of tokens satisfying the following consistency condition:*

$$\forall\, e_1, e_2 \in x \;\; e_1 \frown e_2.$$

We denote with $D(E)$ *the set of states of E, ordered by inclusion. If* $(E, \frown)$ *is a coherence space, its* incoherence *is the relation defined by:*

$$e_1 \smile\!\!\!\frown e_2 \Leftrightarrow \neg(e_1 \frown e_2) \text{ or } e_1 = e_2 \ .$$

Notice that the incoherence is not the complement of the coherence, since the coherence and the incoherence are both reflexive. We also define strict incoherence *and* strict coherence *as follows, respectively:*

$$e_1 \smile e_2 \Leftrightarrow \neg(e_1 \frown e_2) \qquad e_1 \frown e_2 \Leftrightarrow \neg(e_1 \smile\!\!\!\frown e_2) \ .$$

Clearly, coherence can be recovered from incoherence:

$$e_1 \frown e_2 \Leftrightarrow \neg(e_1 \smile\!\!\!\frown e_2) \text{ or } e_1 = e_2 \ .$$

In fact, it is easy to check that all the relations $\frown$, $\smile\!\!\!\frown$, $\frown$ and $\smile$ are interdefinable, that is, if one of them is given, then the other three can be defined from it.

We illustrate coherence spaces with a few ewamples. The coherence space **Nat**$=(\omega, \frown)$, where $m \frown n$ if and only if $m = n$, is such that $D(\mathbf{Nat}) = \{\emptyset\} \cup \{\{n\} \mid n \in \omega\}$, that is, $D(\mathbf{Nat})$ is isomorphic to the partial order $\{\bot\} \cup \omega$, ordered by the *flat* ordering $x \leq y$ if and only if $x = \bot$ or $x = y$. This partial order is used in denotational semantics to interpret the type of natural numbers.

We next show how to interpret the connectives of linear logic as constructions of coherence spaces. We shall write often E for $(E, \frown)$, and it should be clear to which coherence space each use of the symbol $\frown$ refers.

Definition 6.2 *The product, or "with", E&E′ of two coherence spaces E and E′ is the coherence space whose tokens are either e.*1*, with* $e \in E$*, or* $e'.2$*, with* $e' \in E'$ *(using an explicit notation for disjoint unions), and whose coherence is defined as the smallest relation such that:*

$$\frac{}{e.1 \frown e'.2} \qquad \frac{e_1 \frown e_2}{e_1.1 \frown e_2.1} \qquad \frac{e'_1 \frown e'_2}{e'_1.2 \frown e'_2.2}$$

This definition is such that $D(E\&E')$ is isomorphic to $D(E) \times D(E')$, where $\times$ is the good old set-theoretical cartesian product. For example, taking $E = E' = \mathbf{Nat}$, we have that $(\bot, \bot)$, $(m, \bot)$, $(\bot, n)$, and (m, n) are represented as $\emptyset$, $\{m.1\}$, $\{n.2\}$, and $\{m.1, n.2\}$, respectively.

Definition 6.3 *The tensor product $E \otimes E'$ of two coherence spaces E and E' is the coherence space whose tokens are pairs (e, e') where $e \in E$ and $e' \in E'$, and whose coherence is given by:*

$$(e_1, e'_1) \frown (e_2, e'_2) \Leftrightarrow (e_1 \frown e_2 \text{ and } e'_1 \frown e'_2) .$$

We next introduce the duality, or linear negation.

Definition 6.4 *The linear negation $E^\perp$ of a coherence space $(E, \frown)$ is defined as $E^\perp = (E, \asymp)$.*

The definitions of (the interpretation of) $\parr$, $\multimap$, and $\oplus$ are then obtained by De Morgan duality.

Definition 6.5 *Let E, E' be coherence spaces. Their "par" $E \parr E'$ is the coherence space whose tokens are pairs (e, e') where $e \in E$ and $e' \in E'$, and whose incoherence is given by:*

$$(e_1, e'_1) \asymp (e_2, e'_2) \Leftrightarrow (e_1 \asymp e_2 \text{ and } e'_1 \asymp e'_2) .$$

Definition 6.6 *Let E, E' be coherence spaces. Their linear implication $E \multimap E'$ is the coherence space whose tokens are pairs (e, e') where $e \in E$ and $e' \in E'$, and whose incoherence is given by:*

$$(e_1, e'_1) \asymp (e_2, e'_2) \Leftrightarrow (e_1 \frown e_2 \text{ and } e'_1 \asymp e'_2) .$$

As for the $\oplus$, referring to the definition of $E \& E'$, one first gets by contraposition that two events of $E \& E'$ are strictly incoherent (for the $\&$) if and only if they are from the same component and are already strictly incoherent there. By definition of incoherence, one can remove "strict" from the last sentence, and then we obtain the following definition by duality.

Definition 6.7 *The sum, or "plus", $E \oplus E'$ of two coherence spaces E and E' is the coherence space whose tokens are either $e.1$, with $e \in E$, or $e'.2$, with $e' \in E'$, and whose coherence is defined as the smallest relation suh that:*

$$\frac{e_1 \frown e_2}{e_1.1 \frown e_2.1} \qquad \frac{e'_1 \frown e'_2}{e'_1.2 \frown e'_2.2}$$

It remains to define the interpretation of the exponentials.

Definition 6.8 *Let $(E, \frown)$ be a coherence space. The exponential $!E$ is the coherence space whose tokens are the finite cliques of E, and whose coherence is given by $(x_1 \frown x_2 \Leftrightarrow x_1 \uparrow x_2)$, where $x_1 \uparrow x_2$ means that there exists a clique x of E such that $x_1 \subseteq x$ and $x_2 \subseteq x$.*

Now we explain briefly the interpretation of LL in coherence spaces.

1. A formula A is interpreted by a coherence space (it does not harm to use the same name, as we did already for phase semantics).
2. A proof π of a sequent $\vdash A_1, \ldots, A_n$ is interpreted as a clique $[\![\pi]\!]$ of $A_1 \parr \ldots \parr A_n$.
3. If π rewrites through cut-elimination to π', then $[\![\pi]\!] = [\![\pi']\!]$.

As an example, we show (2) for the cut rule. We first remark that a token of $A_1 \parr \ldots \parr A_n$ is a vector $\vec{e} = (e_1, \ldots, e_n)$, and that (cf. the definition of $\parr$) we have:

$$(\dagger) \quad \vec{e} \frown \vec{f} \quad \text{if and only if} \quad e_i \frown f_i \text{ for some } i \ .$$

Let π_1 be a proof of $\vdash \Gamma, A$ and π_2 be a proof of $\vdash \Gamma', A^\perp$. and let π be the proof of $\vdash \Gamma, \Gamma'$ resulting from applying the cut rule. We define the interpretation of π as follows (relation composition!):

$$[\![\pi]\!] = \{(\vec{e}, \vec{e'}) \mid \exists a \ (\vec{e}, a) \in [\![\pi_1]\!] \text{ and } (\vec{e'}, a) \in [\![\pi_2]\!]\} \ .$$

We have to show that $[\![\pi]\!]$ is a clique. Let $(\vec{e}, \vec{e'}), (\vec{f}, \vec{f'}) \in [\![\pi]\!]$. Then there exist a and b such that $(\vec{e}, a) \in [\![\pi_1]\!], (\vec{e'}, a) \in [\![\pi_2]\!], (\vec{f}, b) \in [\![\pi_1]\!]$, and $(\vec{f'}, b) \in [\![\pi_2]\!]$. So, because we know by induction that $[\![\pi_1]\!]$ and $[\![\pi_2]\!]$ are cliques, we have $(\vec{e}, a) \subsetdot (\vec{f}, b)$ and $(\vec{e'}, a) \subsetdot (\vec{f'}, b)$. If both $(\vec{e}, a) = (\vec{f}, b)$ and $(\vec{e'}, a) = (\vec{f'}, b)$, then we have also $(\vec{e}, \vec{e'}) = (\vec{f}, \vec{f'})$ and a fortiori $(\vec{e}, \vec{e'}) \subsetdot (\vec{f}, \vec{f'})$, so we are done. Let us suppose thus that, say, $(\vec{e}, a) \frown (\vec{f}, b)$. By property (†), there are two cases: either we have $e_i \frown f_i$ for some i, or $a \frown_A b$ (the subscript A means that $\frown$ is relative to A). In the first case, we have directly that $(\vec{e}, \vec{e'}) \frown (\vec{f}, \vec{f'})$, using (†). In the second case, we know that $a \neq b$ (by the definition of $\frown$), so a fortiori we have $(\vec{e'}, a) \frown (\vec{f'}, b)$. Hence, by (†), either there exists i' such that $e'_{i'} \frown f'_{i'}$, and then we conclude as above, or $a \frown_{A^\perp} b$. But this cannot happen, because we have $a \frown_A b$, hence a fortiori $a \subsetdot_A b$, which can be rephrased as $a \smile_{A^\perp} b$ and in turn can be rephrased as $\neg(a \frown_{A^\perp} b)$. This ends the proof.

But there is more to this semantics. Coherence spaces can be organized in a category, actually two categories: the category of stable functions (this is where it all started), and the category of linear functions. The domains $D(E)$ are closed under union of increasing sequences, that is, they are *complete partial orders*. It remains to find appropriate morphisms between coherence spaces, defined as appropriate functions from cliques to cliques.

Definition 6.9 *Let $(E, \subsetdot)$ and $(E', \subsetdot)$ be two coherence spaces. A monotonous function $f : D(E) \to D(E')$ is called* stable *if it is continuous, i.e., $f(\bigcup_{n\in\omega} x_n) = \bigcup_{n\in\omega} f(x_n)$ for every increasing sequence x_n, and if it preserves compatible intersections, i.e.:*

$$\forall x, y \ \ x \uparrow y \Rightarrow f(x \cap y) = f(x) \cap f(y)$$

(notice that if $x \uparrow y$, then $x \cap y$ is a clique). If moreover f preserves compatible finite unions, i.e.:

$$f(\emptyset) = \emptyset \qquad \text{and} \qquad \forall x, y \ \ x \uparrow y \Rightarrow f(x \cup y) = f(x) \cup f(y) \ ,$$

then f is called linear*. Stable functions are ordered by the* stable ordering $\leq_s$*, defined as follows: $f \leq_s g$ if and only if $(\forall x \in D(E) \ \ f(x) \leq g(x))$ (pointwise ordering) and*

$$\forall x \leq y \ \ f(x) = g(x) \cap f(y) \ .$$

Proposition 6.10 *For all $(E, \subsetdot)$, $(E', \subsetdot)$, $(\mathbf{Coh}[E, E'], \leq_s)$ (the partial order of stable functions) is order-isomorphic to $(D(!E \multimap E'), \subseteq)$.*

Proof (indication). The inverse bijections are defined as follows. Given a stable function f we define its *trace*, and given a clique ϕ of $!E \multimap E'$ we define the inverse transformation as follows, respectively:

$$trace(f) = \{(x, e') \mid e' \in f(x) \text{ and } (\forall\, y < x \;\; e' \notin f(y))\}$$
$$fun(\phi)(z) = \{e' \mid \exists\, x \;\; x \leq z \text{ and } (x, e') \in \phi\}\ .$$

The most interesting part of the proof consists in verifying that $trace(f)$ is a clique, and that the stable ordering is just the inclusion of traces. One uses the following characterization of the coherence relation of $!E \multimap E'$ (cf. Exercise 6.11):

$$(x_1, e'_1) \frown (x_2, e'_2) \Leftrightarrow (x_1 \frown x_2 \Rightarrow (e'_1 \frown e'_2 \text{ and } (e'_1 = e'_2 \Rightarrow x_1 = x_2)))\ .$$

The trace has an operational flavour: one can read $(x, e') \in trace(f)$ and $x \leq z$ as: "x is *the* (finite) part of z which is used to compute the output event $e' \in f(z)$". Indeed, x is unique with that property, by the above characterization of the coherence, and is called the minimum point for z and e'.

The stable ordering now also has an operational flavour. We show that $f \leq_s g$ implies $trace(f) \subseteq trace(g)$: if $f \leq_s g$, then "f and g are computed in the same way" in the sense that g has to respect the minimum points of f. Let $(x, e') \in trace(f)$. Then $e' \in f(x) \subseteq g(x)$, and hence there exists $(y, e') \in trace(g)$ such that $y \leq x$. We show that $y = x$, which will establish the inclusion. Suppose $y < x$. Then we would have $e' \in f(y) = f(x) \cap g(y)$, which contradicts the minimality of x. The converse implication is proved similarly. □

This proposition has a capital historical importance: it is the observation of the quasi-symmetry of input and output in the traces of stable functions which led Girard to force a complete symmetry by deciding that finite cliques can be considered as atoms, or events of a new coherence space, and hence by decomposing $E \to E'$ as $!E \multimap E'$. Then it "only remained" to realize the logical importance of this decompostion!

Exercise 6.11 *Show that the following are other equivalent definitions of the coherence of the linear function space:*

$$(1) \quad (e_1, e'_1) \frown (e_2, e'_2) \Leftrightarrow (e_1 \frown e_2 \Rightarrow (e'_1 \frown e'_2 \text{ and } (e_1 \neq e_2 \Rightarrow e'_1 \neq e'_2)))$$
$$(2) \quad (e_1, e'_1) \frown (e_2, e'_2) \Leftrightarrow (e_1 \frown e_2 \Rightarrow e'_1 \frown e'_2) \text{ and } (e'_1 \smile e'_2 \Rightarrow e_1 \smile e_2)\ .$$

Exercise 6.12 *Show that for all $(E, \frown)$, $(E', \frown)$, $(\mathbf{Coh_l}[E, E'], \leq_s)$ (the partial order of linear functions) is order-isomorphic to $(D(E \multimap E'), \subseteq)$.*

7 Categorical models of linear logic

In this section, we describe a general categorical semantics for linear logic, and we introduce the appropriate categorical apparatus. We assume that the reader knows about categories, functors, natural transformations, and adjunctions. We briefly reintroduce other rather standard notions such as monoidal categories and comonads, as well as more ad hoc notions and axioms that are needed to complete the picture.

Definition 7.1 *A* monoidal *category is a category $\mathbf{C}$ equipped with a functor $\otimes : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$, called the* tensor product*, a distinguished object* 1*, called the* tensor unit*, and natural isomorphisms, also called the canonical isomorphisms:*

$$\alpha : A \otimes (B \otimes C) \to (A \otimes B) \otimes C \qquad \iota_l : 1 \otimes A \to A \qquad \iota_r : A \otimes 1 \to A\ ,$$

satisfying the following two so-called coherence equations:

$$(\alpha - \alpha) \quad \alpha \circ \alpha = (\alpha \otimes id) \circ \alpha \circ (id \otimes \alpha) \qquad (\alpha - \iota) \quad (\iota_r \otimes id) \circ \alpha = id \otimes \iota_l \ .$$

Where do the two coherence equations come from? As observed by Huet (unpublished), a good answer comes from rewriting theory (a subject that did not exist as such when monoidal categories were defined by Mac Lane in the early sixties). Consider the domains and codomains of the canonical isomorphisms as the left and right hand sides of rewriting rules and rewriting sequences, respectively:

$$(\alpha) \ \ A \otimes (B \otimes C) \to (A \otimes B) \otimes C \qquad (\iota_l) \ \ 1 \otimes A \to A \qquad (\iota_r) \ \ A \otimes 1 \to A$$

The two coherence equations correspond to equating different reduction sequences: $\alpha \circ \alpha$ encodes

$$A \otimes (B \otimes (C \otimes D)) \to (A \otimes B) \otimes (C \otimes D) \to ((A \otimes B) \otimes C) \otimes D \ ,$$

while $(\alpha \otimes id) \circ \alpha \circ (id \otimes \alpha)$ encodes

$$A \otimes (B \otimes (C \otimes D)) \to A \otimes ((B \otimes C) \otimes D) \to^* ((A \otimes B) \otimes C) \otimes D \ .$$

Similarly, the two sides of the second equation encode

$$\begin{array}{l} A \otimes (1 \otimes B) \to (A \otimes 1) \otimes B \to A \otimes B \\ A \otimes (1 \otimes B) \to A \otimes B \ . \end{array}$$

These pairs of derivations form local confluence diagrams for the rewriting system on objects induced by $(\alpha), (\iota_l),$ and (ι_r).

In monoidal categories, the following *Coherence theorem* holds: given two objects A and B, all morphisms from A to B which are obtained from the canonical isomorphisms are equal (see Exercise 7.2 for details).

Exercise 7.2 *(1) Find all the critical pairs of the rewriting system underlying $\alpha, \iota_l,$ and ι_r, and show that the corresponding equations between canonical isomorphisms are derivable from the two equations given in definition 7.1. (Hint: There are three other critical pairs; exploit the fact that $\alpha, \iota_l,$ and ι_r are isos.) (2) Prove the so-called coherence theorem for monoidal categories: every two canonical morphisms (that is, terms over the signature $\{\circ,\ id,\ \otimes,\ \alpha,\ \alpha^{-1},\ \iota_l,\ \iota_l^{-1},\ \iota_r,\ \iota_r^{-1}\}$) with the same domain and codomain are equal. (Hint: Remove first $\alpha^{-1}, \iota_l^{-1},$ and ι_r^{-1}, and proceed as in the proof of Knuth-Bendix theorem [18]).*

Definition 7.3 *A symmetric monoidal category is a monoidal category together with an additional canonical isomorphism $\gamma : A \otimes B \to B \otimes A$ satisfying:*

$$\begin{array}{lll} (\gamma - \gamma) & \gamma \circ \gamma & = \ id \\ (\alpha - \gamma) & \alpha \circ \gamma \circ \alpha & = \ (\gamma \otimes id) \circ \alpha \circ (id \otimes \gamma) \ . \end{array}$$

The coherence theorem still holds in the symmetric monoidal case, but needs more care: clearly we do not want to identify $\gamma : A \otimes A \to A \otimes A$ and $id : A \otimes A \to A \otimes A$. Category theorists exclude this by speaking, not of terms, but of natural transformations (see Exercise 7.4): in the present case, we see that $\gamma : (\lambda(A, B).A \otimes B) \to (\lambda(A, B).B \otimes A)$ and $id : (\lambda(A, B).A \otimes B) \to (\lambda(A, B).A \otimes B)$ do not have the same codomain. A more elementary point of view is to restrict attention to linear terms for objects.

Exercise 7.4 *Show that, in a symmetric monoidal category, any two canonical natural transformations between the same functors are equal. Hints: Use monoidal coherence, and the following presentation of the symmetric group by means of the transpositions σ_i which permute two successive elements i and $i+1$:*

$$\sigma_i \circ \sigma_i = id \quad \sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i \ \ (j - i > 1) \quad \sigma_i \circ \sigma_{i+1} \circ \sigma_i = \sigma_{i+1} \circ \sigma_i \circ \sigma_{i+1}.$$

Definition 7.5 *A monoidal closed category is a monoidal category $\mathbf{C}$ such that for all A the functor $\lambda C.(C \otimes A)$ has a right adjoint, written $\lambda B.(A \multimap B)$. In other words, for every objects A, B, there exists an object $A \multimap B$, called the* linear exponent*, and natural bijections (for all C):*

$$\Lambda_l : \mathbf{C}[C \otimes A, B] \to \mathbf{C}[C, A \multimap B].$$

Notice that there are no accompanying additional coherence equations for monoidal closed categories. This comes from the difference in nature between the constructions $\otimes$ and $\multimap$: the latter is given together with a universal construction (an adjunction), while the first is just a functor with some associated isomorphisms. This difference is often referred to as the difference between "additional structure" ($\otimes$) and "property" ($\multimap$). The notion of dualizing object, due to Barr [2] and introduced next, is additional structure.

Definition 7.6 *A symmetric monoidal closed category $\mathbf{C}$ is called $*$-autonomous if it has a distinguished object $\perp$, called a* dualizing object*, such that for any A the morphisms*

$$\Lambda_l(\Lambda_l^{-1}(id) \circ \gamma) : \mathbf{C}[A, (A \multimap \perp) \multimap \perp],$$

called canonical, have an inverse. We write $A^\perp$ for $A \multimap \perp$, and $A^{\perp\perp}$ for $(A^\perp)^\perp$.

The dualizing object can be understood as the multiplicative false (see Exercise 7.12[part (3)]). The last ingredient we need is the notion of comonad.

Definition 7.7 *A comonad over a category $\mathbf{C}$ is a triple (T, ϵ, δ) where $T : \mathbf{C} \to \mathbf{C}$ is a functor, $\epsilon : T \to id_{\mathbf{C}}$, $\delta : T \to T \circ T$ are natural transformations, and the following equations hold:*

$$\epsilon_{TA} \circ \delta_A = id_{TA} \qquad T\epsilon_A \circ \delta_A = id_{TA} \qquad \delta_{TA} \circ \delta_A = T\delta_A \circ \delta_A \ ,$$

where e.g. $\delta_A : TA \to T(TA)$ stands for the component of δ at A. The following derived operation is useful. For all $f : TA \to B$, one constructs $\kappa(f) : TA \to TB$ as follows:

$$\kappa(f) = Tf \circ \delta.$$

We define the co-Kleisli category $\mathbf{C}_T$ as follows. The objects of $\mathbf{C}_T$ are the objects of $\mathbf{C}$, and for any A, B:

$$\mathbf{C}_T[A, B] = \mathbf{C}[TA, B].$$

The identity morphisms are given by ϵ, and composition $\circ_T$ is defined by:

$$g \circ_T f = g \circ \kappa(f).$$

Comonads are tightly linked with adjunctions (see Exercises 7.14 and 7.15).

We next follow [24] for a first attempt of interpretation of LL. We recall that a category $\mathbf{C}$ is cartesian if it has a terminal object $\top$ (i.e., such that for any A the homset $\mathbf{C}[A, \top]$ has exactly one arrow $\top_A$) and binary products (i.e., for every objects A, B there exists $(A\&B, \pi : A\&B \to A, \pi' : A\&B \to B)$ such that for all C, $f : C \to A$, and $g : C \to B$ there exists a unique arrow $\langle f, g\rangle : C \to A\&B$ such that $\pi \circ \langle f, g\rangle = f$ and $\pi' \circ \langle f, g\rangle = g$; the product is then a functor, with $f\&g = \langle f \circ \pi, f \circ \pi'\rangle$).

Definition 7.8 *A* Seely category *is a structure consisting of the following data: (1) a $*$-autonomous category $\mathbf{C}$ which is at the same time cartesian; (2) a comonad $(!, \epsilon, \delta)$ over $\mathbf{C}$, called the* exponential*, together with two natural isomorphisms:*

$$n_{A,B} : (!A) \otimes (!B) \cong !(A\&B) \qquad p : 1 \cong !\top \ .$$

Proposition 7.9 *If $\mathbf{C}$ is a Seely category, then the associated co-Kleisli category $\mathbf{C}_!$ is cartesian.*

Proof. We take the product on objects and the pairing of arrows of $\mathbf{C}$. As projections we take $\pi_1 \circ \epsilon$ and $\pi_2 \circ \epsilon$. We check one commutation diagram:

$$\begin{array}{rcll} (\pi_1 \circ \epsilon) \circ_! \langle f, f'\rangle & = & \pi_1 \circ (\epsilon \circ \kappa(\langle f, f'\rangle)) & \\ & = & \pi_1 \circ \langle f, f'\rangle & = \quad f \ . \end{array}$$ □

Another implied structure is that each object of the form $!A$ is endowed with the structure of a commutative comonoid: there are two arrows

$$e_A : !A \to 1 \qquad d_A : !A \to (!A) \otimes (!A)$$

satisfying the three (categorical versions of the) comonoid laws (see Exercise 7.10). These arrows are constructed as follows:

$$e = p^{-1} \circ !(\top) \circ \delta \qquad d = n^{-1} \circ !(\langle \epsilon, \epsilon\rangle) \circ \delta \ .$$

This definition of d and e may seem ad hoc, but it is actually derived from the underlying co-Kleisli adjunction (Exercise 7.15) and from the comonoid structure induced by the cartesian products of $\mathbf{C}_!$ (cf. Proposition 7.9 and Exercise 7.11): $e = p^{-1} \circ F\top$ and $d = n^{-1} \circ F\Delta$.

Exercise 7.10 *Let d and e be as above. Show that the following equations are satisfied:*

$$\begin{array}{rclrcl} \iota_l \circ (e \otimes id) \circ d & = & id & \iota_r \circ (id \otimes e) \circ d & = & id \\ \alpha \circ (id \otimes d) \circ d & = & (d \otimes id) \circ d & \gamma \circ d & = & d \ . \end{array}$$

Exercise 7.11 *Let $\mathbf{C}$ be a cartesian category. Let $\Delta = \langle id, id\rangle : A \to A\&A$. Show that Δ and $\top_A$ define a commutative comonoid structure, i.e., verify the equations of Exercise 7.10.*

Exercise 7.12 *Let $\mathbf{C}$ be a $*$-autonomous category. Show that: (1) there exists a natural bijection between $\mathbf{C}[A, B]$ and $\mathbf{C}[B^\perp, A^\perp]$; (2) there exists a natural isomorphism $(A \multimap B)^\perp \cong A \otimes B^\perp$; (3) there exists a natural isomorphism $1 \cong \perp^\perp$.*

Exercise 7.13 *Suppose that* $\mathbf{C}$ *is a symmetric monoidal category, and that* $(\_)^\perp : \mathbf{C}^{op} \to \mathbf{C}$ *is a functor given together with: (1) a natural isomorphism* $A \cong A^{\perp\perp}$*; (2) a natural bijection* $\mathbf{C}[I, (A \otimes B^\perp)^\perp] \cong \mathbf{C}[A, B]$*. Show that* $\mathbf{C}$ *is monoidal closed, with* $\multimap$ *defined by* $A \multimap B = (A \otimes B^\perp)^\perp$*.*

Exercise 7.14 *Show that every adjunction* (F, G, η, ϵ)*, where* $F : \mathbf{C} \to \mathbf{C}'$ *and* $G : \mathbf{C}' \to \mathbf{C}$*, induces a comonad* $(F \circ G, \epsilon, \delta)$ *on* $\mathbf{C}'$*, where* ϵ *is the counit of the adjunction, and where* $\delta = F\eta G$*, i.e.,* $\delta_B = F(\eta_{GB})$ *(for all* B*). Show that the co-Kleisli category associated with the comonad is equivalent to the full subcategory of* $\mathbf{C}$ *whose objects are in the image of* G*.*

Exercise 7.15 *Let* (T, ϵ, δ) *be a comonad over a category* $\mathbf{C}$*. Show that the following data define adjoint functors* F *and* U *between* $\mathbf{C}$ *and* $\mathbf{C}_T$ *in such a way that* $T = FU$*:*

$$FA = !A \quad Ff = \kappa(f) \qquad UA = A \quad Ug = g \circ \epsilon$$

with id *as unit and* ϵ *as counit of the adjunction.*

Exercise 7.16 *Show that if* $\mathbf{C}$ *is a Seely category, then the associated co-Kleisli category* $\mathbf{C}_!$ *is cartesian closed (i.e., for any object* A *the functor* $\lambda C.(C\&A)$ *has a right adjoint).*

Exercise 7.17 *Let* $\mathbf{C}$ *be a* $*$*-autonomous category which is at the same time cartesian, and which is equipped with a comonad* $(!, \epsilon, \delta)$ *such that the associated Kleisli category* $\mathbf{C}_!$ *is cartesian closed. Show that there exists a natural isomorphism from* $(!A) \otimes (!B)$ *to* $!(A\&B)$*.*

We are now in a position to sketch the interpretation of the sequents of linear logic in a Seely category $\mathbf{C}$. A proof of a sequent $\vdash A_1, \ldots, A_n$ is interpreted by a morphism $f : 1 \to (A_1 ⅋ \ldots ⅋ A_n)$ (confusing the formulas with their interpretations as objects of $\mathbf{C}_l$), or (cf. Exercise 7.12) as a morphism from $\Gamma^\perp$ to Δ, for any splitting $A_1, \ldots, A_n = \Gamma \cup \Delta$. We shall freely go from one of these representations to another. The rules are interpreted as follows:

(1) $\vdash 1$ is interpreted by $id : 1 \to 1$.

($\perp$) Obvious, since $\perp$ is the dual of 1 (see Exercise 7.12) and since $1 \otimes 1 \cong 1$.

($\otimes$) From $f : \Gamma^\perp \to A$ and $g : \Delta^\perp \to B$, we form $f \otimes g : \Gamma^\perp \otimes \Delta^\perp \to A \otimes B$.

($⅋$) Obvious by associativity of $⅋$.

(*Axiom*) We simply take $id : A \to A$.

(*Cut*) Compose $f : \Gamma^\perp \to A$ and $g : A \to \Delta$.

($\top$) Interpreting $\vdash \top, \Gamma$ amounts to giving an arrow from $\Gamma^\perp$ to $\top$. Since $\top$ is terminal, we take the unique such arrow.

(&) The pairing of $f : \Gamma^\perp \to A$ and $g : \Gamma^\perp \to B$ yields $\langle f, g \rangle : \Gamma^\perp \to (A\&B)$.

($\oplus$) Given $f : A^\perp \to \Gamma$, we build $f \circ \pi_1 : A^\perp \& B^\perp \to \Gamma$, which we can consider as a morphism from 1 to $(A \oplus B) ⅋ \Gamma$.

(*Dereliction*) Given $f : A^\perp \to \Gamma$, we build $f \circ \epsilon : !(A^\perp) \to \Gamma$, where ϵ is the first natural transformation of the comonad.

(*Promotion*) Let $f : 1 \to (A \parr ?B_1 \parr \ldots \parr ?B_n)$, considered as an arrow from $!(B_1^\perp \& \ldots \& B_n^\perp)$ to A. Here we have made an essential use of the natural isomorphisms required in the definition of a Seely category. Then we can consider $\kappa(f) : !(B_1^\perp \& \ldots \& B_n^\perp) \to !A$ as a proof of $\vdash !A, ?B_1, \ldots, ?B_n$.

(*Weakening*) For this case and the following one, we use the comonoid structure induced on $!A$. Let $f : 1 \to \Gamma$. Then we can consider that $f \circ e = !(A^\perp) \to \Gamma$ is a proof of $\vdash ?A, \Gamma$.

(*Contraction*) This case is similar to the case (*Weakening*), replacing e by d.

Exchange rule: By associativity and commutativity.

So far, so good. But is the interpretation invariant under cut-elimination, which is what we want of a model? The answer is: almost. We shall treat the contraction reduction in detail. Referring to section 3 for notation, the proof Π of $\vdash \Gamma_1, ?B^\perp, ?B^\perp$ is interpreted by, say, a morphism $h : !B \otimes !B \to C$, where C interprets Γ_1, and the proof Π' of $\vdash ?\Gamma_2, B$ is interpreted by, say, a morphism $g : !A \to B$, where A interprets $\Gamma_2^\perp$, assuming for the time being that Γ_2 is just one formula. Then the validation of the contraction reduction amounts to the following equation:

$$(*) \quad d_B \circ !g \circ \delta_A = ((!g \circ \delta_A) \otimes (!g \circ \delta_A)) \circ d_A \ ,$$

which is a consequence of the following two commutativity equations:

$$d_{!A} \circ \delta_A = (\delta_A \otimes \delta_A) \circ d_A \qquad (!g \otimes !g) \circ d_{!A} = d_B \circ !g \ .$$

These two equations are instances of the following more general statement:

$$\begin{array}{ll} (P) \quad \forall f : !A \to !A' \ (\delta_{A'} \circ f = !f \circ \delta_A) & \text{(every free coalgebra morphism} \\ \qquad \Rightarrow (d_{A'} \circ f = (f \otimes f) \circ d_A) & \text{is also a comonoid morphism)} \end{array}$$

(A coalgebra over A is a morphism $f : A \to !A$ and the free coalgebras are the coalgebras δ_A over $!A$.) Indeed, δ is a free coalgebra morphism, by the law $\delta_{!A} \circ \delta_A = !\delta_A \circ \delta_A$, and, for any $g : A \to A'$, $!g$ is a free coalgebra morphism by naturality of δ.

Property (P) cannot be derived from the sole axioms of Seely, as was noted by Benton, Bierman, Hyland and de Paiva [3] (for a survey and more references, see [23]). Below, we show how to prove (P) assuming only one new equation (S^+) with respect to Seely's axiomatization. The reasoning could be carried out entirely in the category $\mathbf{C}$, but it really arises via a tour into the co-Kleisli adjunction of the comonad ! (cf. Exercise 7.15), without which the equation (S^+) would seem ad hoc.

The equation (S^+) asserts the naturality of n, between the two functors $F_{\text{-}1} \otimes F_{\text{-}2}$ and $F(_{\text{-}1} \& _{\text{-}2})$ from $\mathbf{C}_! \& \mathbf{C}_!$ to $\mathbf{C}$, that is, for all $f \in \mathbf{C}_![A, A']$, $g \in \mathbf{C}_![B, B']$:

$$(S^+) \quad F(f \& g) \circ n_{A,B} = n_{A',B'} \circ (Ff \otimes Fg)$$

or, in a form that only mentions $\mathbf{C}$:

$$(S^+) \quad ! < f \circ !\pi, g \circ !\pi' > \circ \delta_{A \& B} \circ n_{A,B} = n_{A',B'} \circ ((!f \circ \delta_A) \otimes (!g \circ \delta_B)) \ .$$

Now we show that (P) holds (we follow [23, section 3.5]). We first remark that d can be reformulated as follows:

$$
\begin{array}{rcll}
d & = & n^{-1}_{UA,UA} \circ F\Delta_{UA} & \\
& = & (\epsilon_{FUA} \otimes \epsilon_{FUA}) \circ (F\eta_{UA} \otimes F\eta_{UA}) \circ n^{-1}_{UA,UA} \circ F\Delta_{UA} & \text{(adjunction law)} \\
& = & (\epsilon_{FUA} \otimes \epsilon_{FUA}) \circ n^{-1}_{UFUA,UFUA} \circ F(\eta_{UA} \& \eta_{UA}) \circ F\Delta_{UA} & \text{(by } (S^+)\text{)} \\
& = & (\epsilon_{FUA} \otimes \epsilon_{FUA}) \circ n^{-1}_{UFUA,UFUA} \circ F\Delta_{UFUA} \circ F\eta_{UA} & (\Delta \text{ natural})
\end{array}
$$

As $F\eta_{UA} = \kappa(id) = \delta_A$ (cf. Exercise 7.15), this gives us a handle to use the assumption of (P) in the proof of its conclusion:

$$
\begin{array}{ll}
d_{A'} \circ f & \\
= (\epsilon_{FUA'} \otimes \epsilon_{FUA'}) \circ n^{-1}_{UFUA',UFUA'} \circ F\Delta_{UFUA'} \circ \delta_{A'} \circ f & \\
= (\epsilon_{FUA'} \otimes \epsilon_{FUA'}) \circ n^{-1}_{UFUA',UFUA'} \circ F\Delta_{UFUA'} \circ FUf \circ \delta_A & \text{(assumption)} \\
= (\epsilon_{FUA'} \otimes \epsilon_{FUA'}) \circ n^{-1}_{UFUA',UFUA'} \circ F(Uf \& Uf) \circ F\Delta_{UFUA} \circ \delta_A & (\Delta \text{ natural}) \\
= (\epsilon_{FUA'} \otimes \epsilon_{FUA'}) \circ (FUf \otimes FUf) \circ n^{-1}_{UFUA,UFUA} \circ F\Delta_{UFUA} \circ \delta_A & \text{(by } (S^+)\text{)} \\
= (f \otimes f) \circ (\epsilon_{FUA} \otimes \epsilon_{FUA}) \circ n^{-1}_{UFUA,UFUA} \circ F\Delta_{UFUA} \circ \delta_A & (\epsilon \text{ natural}) \\
= (f \otimes f) \circ d_A &
\end{array}
$$

Now, we have to lift the restriction on the context Γ_2. What happens if Γ_2 consists of two or more formulas, say, $\Gamma_2 = A_1^\perp, A_2^\perp$? Well, not a big deal, since $!A_1 \otimes !A_2$ is isomorphic to $!(A_1 \& A_2)$, so we can proceed as we did. Yes, but there are two distinct contraction rules in

$$
\dfrac{\vdash \Gamma_1, ?A_1^\perp, ?A_2^\perp, ?A_1^\perp, ?A_2^\perp}{\vdash \Gamma_1, ?A_1^\perp, ?A_2^\perp}
$$

and hence the right hand side of equation $(*)$ is now $((!g \circ \delta_A) \otimes (!g \circ \delta_A)) \circ (d_{A_1} \otimes d_{A_2})$ and *not* $((!g \circ \delta_A) \otimes (!g \circ \delta_A)) \circ d_{A_1 \& A_2}$. We shall be done if we have $d_{A_1} \otimes d_{A_2} = d_{A_1 \& A_2}$ up to associativity and commutativity.

It remains to consider the case where Γ_2 is empty. Then one still proceeds as we did, setting $A = \top$, but at the price of introducing a useless $d : !\top \to !\top \otimes !\top$, which should be the identity up to the two canonical isomorphisms $\iota_l \circ (p^{-1} \otimes !\top)$ and $\iota_r \circ (!\top \otimes p^{-1})$.

Exercise 7.18 *Formulate these equalities more precisely, and show that they are consequences of the following equations (taken from [23, section 4]):*

$$
\begin{array}{ll}
(S^+_\alpha) & n_{A\&B,C} \circ (n_{A,B} \otimes !C) \circ \alpha_{!A,!B,!C} = !\alpha_{A,B,C} \circ n_{A,B\&C} \circ (!A \otimes n_{B,C}) \\
(S^+_\gamma) & n_{B,A} \circ \gamma_{!A,!B} = !\gamma_{A,B} \circ n_{A,B} \\
(S^+_{\iota_l}) & (\iota_l)_{!A} = !(\iota_l)_A \circ n_{\top,A} \circ (p \otimes !A) \\
(S^+_{\iota_r}) & (\iota_r)_{!A} = !(\iota_r)_A \circ n_{A,\top} \circ (!A \otimes p)
\end{array}
$$

which use the fact that a cartesian category is a fortiori monoidal, and where α, ι_l, ι_r and γ in the right hand sides refer to that induced monoidal structure.

Exercise 7.19 *With the help of the same equations, show that the weakening reduction and the reduction of a cut between two promotions $\vdash ?\Gamma_1, ?B^\perp, !C$ and $\vdash ?\Gamma_2, !B$ (cf. section 3) are valid. Hint: For the latter, prove first that $\delta \circ Ff = !Ff \circ \delta$, for any $f : !A \to B$.*

We have completed the definition of a categorical model of linear logic, which we wrap in the following definition.

Definition 7.20 *A Seely$^+$ category is a Seely category which moreover satisifes the five axioms* (S^+), (S^+_α), $(S^+_{\iota_l})$, $(S^+_{\iota_r})$, *and* (S^+_γ).

In more synthetic terms, this definition says that the functor $F : \mathbf{C}_! \to \mathbf{C}$ is (strong) *monoidal*.

We end the section by sketching the proof that the category $\mathbf{Coh}_l$ of coherence spaces and linear functions forms a Seely$^+$ category.

Proposition 7.21 *The inclusion functor from* $\mathbf{Coh}_l$ *to the category* $\mathbf{Coh}$ *of coherence spaces and stable functions has a left adjoint, and* $\mathbf{Coh}_l$ *together with the comonad on* $\mathbf{Coh}_l$ *induced by the adjunction yields a Seely category whose co-Kleisli category is equivalent to* $\mathbf{Coh}$.

Proof. The adjunction is an immediate consequence of Proposition 6.10 and Exercise 6.12. For the symmetric monoidal structure, we just notice that at the level of events the canonical isomorphisms are given by:

$$((e,e'),e'') \leftrightarrow (e,(e',e'')) \quad (e,*) \leftrightarrow e \quad (*,e) \leftrightarrow e \quad (e,e') \leftrightarrow (e',e) \ .$$

There is a natural bijection $\mathbf{Coh}_l[1,E] \cong D(E)$, since $(*,e_1) \frown (*,e_2)$ boils down to $e_1 \frown e_2$. Hence we have:

$$\begin{array}{rcll} \mathbf{Coh}_l[1,(E \otimes E'^{\perp})^{\perp}] & \cong & D(E \otimes E'^{\perp})^{\perp}) & \\ & = & D(E \multimap E') & \\ & \cong & \mathbf{Coh}_l[E,E'] & \text{(cf. Exercise 6.12)} \ . \end{array}$$

Then the closed structure follows from Exercise 7.13. To see that $\mathbf{Coh}_l$ is $*$-autonomous, we set $\perp = 1^{\perp}$ $(= 1)$, and we observe the trace of $\Lambda_l(\Lambda_l^{-1}(id) \circ \gamma) : A \to (A \multimap \perp) \multimap \perp$, which is $\{(e,((e,*),*)) \mid e \in E\}$. It has as inverse the function whose trace is $\{(((e,*),*),e) \mid e \in E\}$.

That $\mathbf{Coh}$ is equivalent to the co-Kleisli category follows from Exercise 7.14. We are left to verify the two natural isomorphisms. The first one holds by Exercise 7.17. For the second one, notice that $D(1)$ is a singleton. □

Exercise 7.22 *Show that the transformations* ϵ *and* δ *associated with the comonad* $! \circ \subseteq$ *on* $\mathbf{Coh}_l$ *are the following functions:*

$$\epsilon(X) = \{e \mid \{e\} \in X\} \qquad \delta(X) = \{Y \mid \bigcup Y \in X\} \ ,$$

and check that the coherent model satisfies the other axioms of Seely$^+$ categories.

References

[1] H. Barendregt, The lambda calculus; its syntax and semantics, North-Holland (1984).

[2] M. Barr, $*$-autonomous categories and linear logic, Mathematical Structures in Computer Science 1(2), 159-178 (1991).

[3] G. Bierman, What is a categorical model of intuitionistic linear logic?, in Proc. Typed Lambda Calculi and Applications, Springer Lect. Notes in Comp. Sci. 902, (1995).

[4] P.-L. Curien, Introduction to ludics, draft notes (2001).

[5] V. Danos and R. Di Cosmo, The linear logic primer, available from `http://www.pps.jussieu.fr/~dicosmo`.

[6] V. Danos, J.-B. Joinet, and H. Schellinx, The structure of exponentials: uncovering the dynamics of linear logic proofs, in Proc. Kurt Gödel Symposiun '93, Lecture Notes in Computer Science 713 (1993).

[7] V. Danos, J.-B. Joinet, and H. Schellinx, A new deconstructive logic: linear logic, Journal of Symbolic Logic 62(3), 755-807 (1997).

[8] V. Danos and L. Regnier, The structure of multiplicatives, Archive for Mathematical Logic 28, 181-203 (1989).

[9] J.-Y. Girard, The system F of variable types, fifteen years later, Theoretical Computer Science 45, 159-192 (1986).

[10] J.-Y. Girard, Linear logic, Theoretical Computer Science 50, 1-102 (1987).

[11] J.-Y. Girard, Y. Lafont, and P. Taylor, Proofs and Types, Cambridge University Press (1989).

[12] J.-Y. Girard, Linear logic: its syntax and semantics, in Advances of Linear Logic, J.-Y. Girard, Y. Lafont, and L. Regnier eds, Cambridge University Press, 1-42 (1995).

[13] J.-Y. Girard, Locus solum: from the rules of logic to the logic of rules, Mathematical Structures in Computer Science 11(3), 301-506 (2001).

[14] J.-Y. Girard, From foundations to ludics, Bulletin of Symbolic Logic 9, 131-168 (2003).

[15] J. Goubault-Larrecq and I. Mackie, Proof theory and automated deduction, Kluwer (1997).

[16] Stefano Guerrini and Andrea Masini, Parsing MELL proof nets. Theoretical Computer Science 254(1-2), 317-335 (2001).

[17] R. Hindley and J. Seldin, Introduction to combinators and lambda-calculus, Cambridge University Press (1986).

[18] G. Huet and D. Oppen, Equations and Rewrite Rules: a Survey, in Formal Language Theory: Perspectives and Open Problems, R. Book (ed.), Academic Press, 349-405 (1980).

[19] M. Hyland, Game semantics, in Semantics and Logics of Computation, Pitts and Dybjer (eds.), Cambridge University Press, (1997).

[20] J.-L. Krivine, Lambda-calculus, types and models, Ellis Horwood (1993).

[21] P. Lincoln, J. Mitchell, A. Scedrov, Decision problems for propositional linear logic, Annals of Pure and Applied Logic 56, 239-311 (1992).

[22] S. Mac Lane, Categories for the working mathematician, Springer-Verlag (1971).

[23] P.-A. Melliès, Categorical models of linear logic revisited, to appear in Theoretical Computer Science (2004).

[24] R. Seely, Linear logic, $*$-autonomous categories and cofree coalgebras, in Applications of categories in logic and computer science, Contempory Mathematics 92 (1989).

[25] G. Winskel, Event structures, Springer Lect. Notes in Comp. Sci. 255 (1986).