What is Linear Logic?

Thomas Ehrhard, IRIF, CNRS and Université de Paris
ehrhard@irif.fr
https://www.irif.fr/~ehrhard

February 15, 2021

Linear Logic seems to be everywhere.

How I met LL: as a natural structure of a model of sequential computations (strong stability $\rightsquigarrow$ *hypercoherences* in 1992).

The same thing happened

- earlier for Berry's stable semantics (stability $\rightsquigarrow$ *coherence spaces*): this is how Girard discovered LL
- later for Scott semantics (Scott continuity $\rightsquigarrow$ *prime algebraic complete lattices*, Krivine, Huth, Winskel).

We know now dozens of models of programming languages which can nicely be described as models of LL.

In what does it differ from usual logic?

- Logic is usually thought of as a formalism to express and prove properties of things.
- In the 20th century one understood that proofs *are* programs (Gentzen cut-elimination, Gödel Dialectica, Curry Howard correspondence). Logical formulas become types.
- Linear logic is a Curry Howard logic: LL formulas are types.
- LL shows up when one builds universes (categories) of spaces and morphisms representing computations between them.

This talk: illustration on the example of probabilistic coherence spaces.

The category of substochastic matrices

Example

For some reason, we want to build a simple theory of subprobabilistic distributions and substochastic matrices acting on them.

It can be described as a category:

- objects are sets I, J, ...
- a morphism $I \to J$ is a matrix $s \in (\mathbb{R}_{\geq 0})^{I \times J}$ such that $\forall i \in I \ \sum_{j \in J} s_{i,j} \leq 1$.

So a matrix $s : I \to I$ is a submarkovian chain (we accept loss of mass: possibly diverging computations).

As a category

This simply means that we have objects (sets), morphisms (matrices), a way of composing them:

If $s : I \to J$ and $t : J \to K$ then $t\,s : I \to K$ is the product of matrices

$$(t\,s)_{i,k} = \sum_{j \in J} s_{i,j} t_{j,k}$$

And identity matrices $\mathrm{Id}_I : I \to I$, $(\mathrm{Id}_I)_{i,i'} = \delta_{i,i'}$.

Matrices and vectors (distributions)

This seems very stupid, but there are interesting structures behind. . .

The singleton set $\mathbb{1} = \{*\}$.

- A matrix $x : \mathbb{1} \to I$ is just a subprobability distribution on I, $x \in \mathrm{D}(I)$.
- up to trivial iso $x \in \mathrm{D}(I)$ simply means $x \in (\mathbb{R}_{\geq 0})^I$ with $\sum_{i \in I} x_i \leq 1$.
- If $s : I \to J$ then $s\,x \in \mathrm{D}(J)$ is the image distribution of x:

$$(s\,x)_j = \sum_{i \in I} s_{i,j} x_i \,.$$

Codistributions and transpose

What is a matrix $x' : I \to \mathbb{1}$, say $x' \in \mathrm{D}'(I)$?

- It means $x' \in (\mathbb{R}_{\geq 0})^I$ with $\forall i \in I\ x'_i \leq 1$
- If $s : J \to I$ then the *transpose* $s^\perp \in (\mathbb{R}_{\geq 0})^{J \times I}$ of s, defined by $s^\perp_{j,i} = s_{i,j}$ satisfies $s^\perp\, x' \in \mathrm{D}'(J)$
- If $x \in \mathrm{D}(I)$, that is $x : \mathbb{1} \to I$, then $x'\, x : \mathbb{1} \to \mathbb{1}$ is just an element of $[0, 1]$, notation

$$\langle x, x' \rangle = (x'\, x) = \sum_{i \in I} x_i x'_i \in [0, 1] \quad \text{(NB: } I \text{ can be } \infty\text{)}$$

Adjunction

Fact

$$\langle s\, x, x' \rangle = \langle x, s^{\perp}\, x' \rangle = \sum_{i \in I,\, j \in J} x_i s_{i,j} x'_j \,.$$

Duality and linear negation

There is a duality between $\mathsf{D}(I)$ and $\mathsf{D}'(I)$ similar to the duality between ℓ^1 and ℓ^∞ in Banach spaces.

Fact

$$\mathsf{D}'(I) = \left\{x' \in (\mathbb{R}_{\geq 0})^I \mid \forall x \in \mathsf{D}(I)\ \langle x, x' \rangle \leq 1\right\}$$
$$\mathsf{D}(I) = \left\{x \in (\mathbb{R}_{\geq 0})^I \mid \forall x' \in \mathsf{D}'(I)\ \langle x, x' \rangle \leq 1\right\}$$

A space of substochastic matrices

Let I and J be two sets.

Let $\mathrm{Stoc}(I, J)$ be the set of all $s : I \to J$, so $\mathrm{Stoc}(I, J) \subseteq (\mathbb{R}_{\geq 0})^{I \times J}$.

Definition

If $u \in (\mathbb{R}_{\geq 0})^I$ and $v \in (\mathbb{R}_{\geq 0})^J$ let $u \otimes v \in (\mathbb{R}_{\geq 0})^{I \times J}$ be defined by $(u \otimes v)_{i,j} = u_i v_j$.

Fact

$$\mathrm{Stoc}(I, J) = \left\{ s \in (\mathbb{R}_{\geq 0})^{I \times J} \mid \forall x \in \mathrm{D}(I)\, y' \in \mathrm{D}'(J) \quad \langle s, x \otimes y' \rangle \leq 1 \right\}$$

Indeed

$$
\begin{aligned}
s \in \mathrm{Stoc}(I, J) &\Leftrightarrow \forall x \in \mathrm{D}(I)\ s\,x \in \mathrm{D}(J) \\
&\Leftrightarrow \forall x \in \mathrm{D}(I)\,\forall y' \in \mathrm{D}'(J)\ \langle s\,x, y' \rangle \leq 1 \\
&\Leftrightarrow \forall x \in \mathrm{D}(I)\,\forall y' \in \mathrm{D}'(J)\ \langle s, x \otimes y' \rangle \leq 1
\end{aligned}
$$

since

$$
\begin{aligned}
\langle s\,x, y' \rangle &= \sum_{j \in J} \left(\sum_{i \in I} s_{i,j} x_i \right) y'_j \\
&= \sum_{i \in I,\, j \in J} s_{i,j} x_i y'_j \\
&= \langle s, x \otimes y' \rangle
\end{aligned}
$$

A common pattern!

In all these cases we have defined a $\mathcal{P} \subseteq (\mathbb{R}_{\geq 0})^I$ for some set I.

This $\mathcal{P}$ is characterized by

$$\mathcal{P} = \left\{x \in (\mathbb{R}_{\geq 0})^I \mid \forall x' \in \mathcal{P}' \ \langle x, x' \rangle \leq 1\right\} = \mathcal{P}'^{\perp}$$

for some $\mathcal{P}' \subseteq (\mathbb{R}_{\geq 0})^I$. A *predual* of $\mathcal{P}$.

Fact

The existence of such a $\mathcal{P}'$ is equivalent to $\mathcal{P} = \mathcal{P}^{\perp\perp}$.

For all $\mathcal{P}, \mathcal{Q} \subseteq (\mathbb{R}_{\geq 0})^I$

- $\mathcal{P} \subseteq \mathcal{Q} \Rightarrow \mathcal{Q}^{\perp} \subseteq \mathcal{P}^{\perp}$
- $\mathcal{P} \subseteq \mathcal{P}^{\perp\perp}$

So $\mathcal{P}^{\perp} = \mathcal{P}^{\perp\perp\perp}$ always holds.

Probabilistic coherence spaces (PCS)

A PCS is a pair $X = (|X|, \mathrm{P}X)$ where

- $|X|$ is a set (the web)
- $\mathrm{P}X \subseteq (\mathbb{R}_{\geq 0})^{|X|}$ such that $\mathrm{P}X = \mathrm{P}X^{\perp\perp}$
- we also assume

$$\forall a \in |X| \quad 0 < \sup\{x_a \mid x \in \mathrm{P}X\} < \infty$$

so that all coeffs remain finite.

$X^{\perp} = (|X|, \mathrm{P}X^{\perp})$ is also a PCS.

Of course $(I, \mathrm{D}(I))$ and $(I, \mathrm{D}'(I))$ are PCS simply denoted $\mathrm{D}(I)$ and $\mathrm{D}'(I)$. We have $\mathrm{D}'(I) = \mathrm{D}(I)^{\perp}$.

$\mathrm{Stoc}(I, J)$ is an instance of a more general construction:

Definition

If X and Y are PCS, we define a PCS $X \multimap Y$ by $|X \multimap Y| = |X| \times |Y|$ and

$$\begin{aligned} \mathrm{P}(X \multimap Y) &= \left\{ s \in (\mathbb{R}_{\geq 0})^{|X \multimap Y|} \mid \forall x \in \mathrm{P}X \ \ s\,x \in \mathrm{P}Y \right\} \\ &= \left\{ x \otimes y' \mid x \in \mathrm{P}X \text{ and } y' \in \mathrm{P}Y^{\perp} \right\}^{\perp} . \end{aligned}$$

Just as in the special case of $\mathrm{Stoc}(I, J)$. By construction, it is a PCS.

So we have $\mathrm{Stoc}(I, J) = (\mathrm{D}(I) \multimap \mathrm{D}(J))$.

LL multiplicative constructs

- $\mathbb{1}$ unit object, $\mathrm{P}\mathbb{1} = [0,1]$, and $\mathbb{1}^\perp = \mathbb{1}$.
- $X \multimap Y$ is *linear implication*.
- $X^\perp = (|X|, \mathrm{P}X^\perp)$, *linear negation*, and we have $X^{\perp\perp} = X$ as in classical logic.
- $X \otimes Y = (X \multimap Y^\perp)^\perp$, multiplicative conjuction, tensor product, *times*. Then $|X \otimes Y| = |X| \times |Y|$ and

  $$\mathrm{P}(X \otimes Y) = \{x \otimes y \mid x \in \mathrm{P}X \text{ and } y \in \mathrm{P}Y\}^{\perp\perp}$$

  Think of $A \wedge B = \neg(A \to \neg B)$ in classical logic.
- $X \parr Y = X^\perp \multimap Y = \left(X^\perp \otimes Y^\perp\right)^\perp$, multiplicative disjunction, cotensor product, *par*. Think of $A \vee B = \neg A \to B$.

A category

We have now also a generalization of substochastic matrices: the elements s of $\mathsf{P}(X \multimap Y)$.

Remember: they are characterized by a simple property. Given $s \in (\mathbb{R}_{\geq 0})^{|X| \times |Y|}$, one has

$$s \in \mathsf{P}(X \multimap Y) \Leftrightarrow \forall x \in \mathsf{P}X \ \ s\,x \in \mathsf{P}\,Y$$

so $\mathsf{Id}_{|X|} \in \mathsf{P}(X \multimap X)$ and if $s \in \mathsf{P}(X \multimap Y)$ and $t \in \mathsf{P}(Y \multimap Z)$ then $t\,s \in \mathsf{P}(X \multimap Z)$. Because $(t\,s)\,x = t\,(s\,x)$.

Matrices are linear maps

An element s of $\mathsf{P}(X \multimap Y)$ is a *linear morphism* from X to Y. And it is really linear (and continuous) in the sense that if $(x(i))_{i\in\mathbb{N}}$ are elements of $\mathsf{P}X$ such that $\sum_{i\in\mathbb{N}} x(i) \in \mathsf{P}X$, one has

$$s\,(\sum_{i\in\mathbb{N}} x(i)) = \sum_{i\in\mathbb{N}} s\,x(i)$$

and also $s\,(\lambda x) = \lambda(s\,x)$ for $\lambda \in [0,1]$.

$X^\perp \simeq (X \multimap \mathbb{1})$ so $X^\perp$ is the space of linear continuous forms on X, exactly like E^* (linear dual) in linear algebra. And here we have $X^{\perp\perp} \simeq X$ exactly like $E^{**} \simeq E$ in finite dimensional vector spaces.

Here this reflexivity holds also in infinite dimension (when $|X|$ is infinite). Very difficulte to achieve with vector spaces.

Tensor product and multilinear maps

We have them for free: let $s \in \mathsf{P}(X_1 \otimes \cdots \otimes X_k \multimap Y)$.

Then the map

$$\begin{aligned} \widehat{s} : \prod_{i=1}^{k} \mathsf{P}X_i &\to \mathsf{P}Y \\ (x(1), \ldots, x(k)) &\mapsto s\,(x(1) \otimes \cdots \otimes x(k)) \end{aligned}$$

is k-linear, that is, separately linear in each argument.

A bilinear map

For instance, we can internalize matrix composition as a bilinear map:

$$\gamma \in \mathrm{P}(((Y \multimap Z) \otimes (X \multimap Y)) \multimap (X \multimap Y))$$

such that

$$\forall t \in \mathrm{P}(Y \multimap Z)\,, \forall s \in \mathrm{P}(X \multimap Y) \quad \widehat{\gamma}(t, s) = \gamma\,(t \otimes s) = t\, s$$

namely $\gamma_{(b,c),(a,b')} = \delta_{b,b'}$.

Categories

The right categorical setting for describing the situation is that of a *symmetric monoidal category* (SMC), here the category **Pcoh**:

- objects are the PCS X
- morphisms from X to Y ($\mathbf{Pcoh}(X, Y)$) are the elements of $\mathsf{P}(X \multimap Y)$, identities and composition as described
- together with $\otimes$ which is a functor $\mathbf{Pcoh}^2 \to \mathbf{Pcoh}$
- and additional structures expressing that $\otimes$ has $\mathbb{1}$ as neutral element, is associative, commutative
- and moreover it is *closed*, meaning that we have $X \multimap Y$ such that $\mathbf{Pcoh}(Z \otimes X, Y) \simeq \mathbf{Pcoh}(Z, X \multimap Y)$
- and $X^\perp = (X \multimap \mathbb{1})$ with $X^{\perp\perp} \simeq X$ ($*$-autonomy).

Cartesian product

Warning

$X \otimes Y$ is not the "cartesian product" (or categorical product) of X_1 and X_2

- there are no projections $p_i \in \mathbf{Pcoh}(X_1 \otimes X_2, X_i)$ such that $p_i\,(x(1) \otimes x(2)) = x(i)$ in general.
- and there is no duplication $d \in \mathbf{Pcoh}(X, X \otimes X)$ such that $d\,x = x \otimes x$.

Take $X_1 = \mathbb{1}$. Then for each $x \in \mathrm{P}X_2$ and $\lambda \in \mathrm{P}X_1 = [0,1]$ we should have $p_1\,(\lambda \otimes x) = p_1\,(\lambda x) = \lambda$. This contradicts linearity in x (take $x = 0$).

Projection as marginalization

In some cases, there are projections, for instance, we have a linear morphisme $\theta_I \in \mathbf{Pcoh}(\mathsf{D}(I), \mathbb{1})$ given by $(\theta_I)_{i,*} = 1$

$$\begin{aligned}\theta_I : \mathsf{D}(I) &\to \mathbb{1} \\ x &\mapsto \sum_{i \in I} x_i\end{aligned}$$

Does not work for $\mathsf{D}'(I)$!

So by functoriality of $\otimes$ we have
$\pi_2 = \theta_I \otimes \mathsf{Id} \in \mathbf{Pcoh}(\mathsf{D}(I) \otimes \mathsf{D}(J), \mathsf{D}(J))$.

We have $\mathsf{D}(I) \otimes \mathsf{D}(J) = \mathsf{D}(I \times J)$. Given $z \in \mathsf{D}(I \times J)$, we have

$$\pi_2\, z = \left(\sum_{i \in I} z_{i,j}\right)_{j \in J}$$

the marginal distribution.

The existence of θ_I is related to a crucial logical structure of $\mathsf{D}(I)$: positivity.

Similarity with vector spaces

Again, strong similarity with vector spaces: there is a cartesian product of vector space, the so-called *direct product* of vector spaces $E \times F$ (which coincides with *direct sum* $E \oplus F$).

direct product vs. tensor product

But $E \times F$ does not coincide with the tensor product $E \otimes F$! A linear map $E \times F \to G$ is not the same thing as a bilinear map $E \times F \to G$. Also $\dim E \otimes F = \dim E \dim F$ whereas $\dim E \times F = \dim E + \dim F$.

We also have a direct product $X \,\&\, Y$ and a direct sum $X \oplus Y$ in PCS, but they do not coincide.

If $(X_i)_{i\in I}$ is a family of PCS we can define $X = \&_{i\in I} X_i$ by

- $|X| = \bigcup_{i\in I} \{i\} \times |X_i|$
- and, for $z \in (\mathbb{R}_{\geq 0})^{|X|}$, $z \in \mathrm{P}X$ if for all $i \in I$ one has $\pi_i\, z \in \mathrm{P}X_i$ where $\pi_i \in (\mathbb{R}_{\geq 0})^{|X \multimap X_i|}$, the ith projection is

$$(\pi_i)_{(j,a),a'} = \delta_{i,j}\delta_{a,a'}\,.$$

- so that $\mathrm{P}X \simeq \prod_{i\in I} \mathrm{P}X_i$ by $z \mapsto (\pi_i\, z)_{i\in I}$ and $(x(i))_{i\in I} \mapsto \langle x(i)\rangle_{i\in I}$ given by $z_{(i,a)} = x(i)_a$.

By construction we do have now linear projections $\pi_i \in \mathbf{Pcoh}(\&_{j\in J} X_j, X_i)$.

We can use duality to define the coproduct:

$$\bigoplus_{i\in I} X_i = (\mathop{\&}_{i\in I} X_i^{\perp})^{\perp}$$

then we have

$$\mathsf{P}(\bigoplus_{i\in I} X_i) = \left\{ \langle \lambda_i x(i) \rangle_{i\in I} \mid \vec{\lambda} \in \mathsf{D}(I) \text{ and } \forall i \; x(i) \in \mathsf{P}X_i \right\} \subseteq \mathsf{P}(\mathop{\&}_{i\in I} X_i)\,.$$

Beyond linearity: the exponential

A polynomial function on matrices

Given $k \in \mathbb{N}$ imagine we want to consider the function

$$f : \mathsf{P}(X \multimap X) \to \mathsf{P}(X \multimap X)$$
$$t \mapsto t^k = \overbrace{t \cdots t}^{k\times}$$

so that

$$f(t)_{a,c} = \sum_{\substack{b_0,\ldots,b_k \in |X| \\ b_0 = a,\ b_k = c}} t_{b_0,b_1} \cdots t_{b_{k-2},b_{k-1}} t_{b_{k-1},b_k} \, .$$

This is not a linear function when $k > 1$: $f(\lambda s) = \lambda^k f(s)$.

An analytic function on matrices

Or even the function

$$\begin{aligned} g : \mathrm{P}(X \multimap X) &\to \mathrm{P}(X \multimap X) \\ t &\mapsto e^{-1} \sum_{k=0}^{\infty} \frac{1}{k!} t^k \end{aligned}$$

If $m \in \mathcal{M}_{\mathrm{fin}}(I)$ (finite multiset) and $u \in (\mathbb{R}_{\geq 0})^I$ we set

$$u^m = \prod_{i \in I} u_i^{m(i)}$$

and $u^{(!)} \in (\mathbb{R}_{\geq 0})^{\mathcal{M}_{\mathrm{fin}}(I)}$ is defined by $u^{(!)}_m = u^m$.

Then we define a PCS $!X$ by $|!X| = \mathcal{M}_{\mathrm{fin}}(|X|)$ and

$$\mathsf{P}(!X) = \left\{ x^{(!)} \mid x \in \mathsf{P}X \right\}^{\perp\perp} .$$

Fact

If $t \in (\mathbb{R}_{\geq 0})^{|!X \multimap Y|}$, *one has*

$$t \in \mathbf{Pcoh}(!X, Y) \Leftrightarrow \forall x \in \mathrm{P}X \;\; t\, x^{(!)} \in \mathrm{P}Y$$

The function

$$\begin{aligned} \widehat{t} : \mathrm{P}X &\to \mathrm{P}Y \\ x &\mapsto t\, x^{(!)} \end{aligned}$$

is an “analytic function”, t (the powerseries) is completely determined by this function.

Examples of analytic functions

Let $k \in \mathbb{N}$. Take $f \in (\mathbb{R}_{\geq 0})^{!(X \multimap X) \multimap (X \multimap X)}$ given by

$$f_{m,(a,c)} = \begin{cases} 1 & \text{if } \exists b_0, \dots, b_k \in |X| \ b_0 = a, \ b_k = c \text{ and} \\ & \qquad m = [(b_0, b_1), (b_1, b_2), \dots, (b_{k-1}, b_k)] \\ 0 & \text{otherwise.} \end{cases}$$

Then given $s \in \mathrm{P}(X \multimap X)$ we have $\widehat{f}(s) = s^k$.

Let $g \in (\mathbb{R}_{\geq 0})^{!(X \multimap X) \multimap (X \multimap X)}$ given by

$$g_{m,(a,c)} = \begin{cases} \frac{e^{-1}}{k!} & \text{if } \exists b_0, \ldots, b_k \in |X|,\ b_0 = a,\ b_k = c \text{ and} \\ & \qquad m = [(b_0, b_1), (b_1, b_2), \ldots, (b_{k-1}, b_k)] \\ 0 & \text{otherwise.} \end{cases}$$

Let $s \in \mathrm{P}(X \multimap X)$ and $t = \widehat{g}(s) \in \overline{\mathbb{R}_{\geq 0}}^{|X \multimap X|}$, we have

$$\forall x \in \mathrm{P}X \quad \widehat{t}(x) = \sum_{k=0}^{\infty} \frac{e^{-1}}{k!} \widehat{s}^k(x) \in \mathrm{P}X$$

because $\forall k \in \mathbb{N}\ \widehat{s}^k(x) \in \mathrm{P}X$ and $\sum_{k=0}^{\infty} \frac{e^{-1}}{k!} = 1$.

Hence $\widehat{g}(s) \in \mathrm{P}(X \multimap X)$.

Since this holds for all $s \in \mathrm{P}(X \multimap X)$, we have $g \in \mathbf{Pcoh}(!(X \multimap X), X \multimap X)$.

Example: stochastic automata

Let A (alphabet) and Q (states) be sets.

$\mathsf{D}(A) \otimes \mathsf{D}(Q) \multimap \mathsf{D}(Q)$ is the space of stochastic automata.

The space of words is the "least" solution W of $W = \mathbb{1} \oplus (\mathsf{D}(A) \otimes W)$. Then it is easy to see that $W = \mathsf{D}(A^{<\omega})$.

There is an analytic "iteration" function $r \in \mathbf{Pcoh}(W \otimes !(\mathsf{D}(A) \otimes \mathsf{D}(Q) \multimap \mathsf{D}(Q)), \mathsf{D}(Q) \multimap \mathsf{D}(Q))$.

$$r_{w,m,(a,c)} = \begin{cases} 1 & \text{if } w = \langle \alpha_1, \ldots, \alpha_k \rangle, \\ & m = [(\alpha_1, b_0, b_1), \ldots, (\alpha_k, b_{k-1}, b_k)] \\ & b_0 = a,\ \ b_k = c \\ 0 & \text{otherwise.} \end{cases}$$

So r defines a function

$$\begin{aligned} \widehat{r} : \mathrm{PD}(W) \times \mathrm{P}(\mathrm{D}(A) \otimes \mathrm{D}(Q) \multimap \mathrm{D}(Q)) &\to \mathrm{P}(\mathrm{D}(Q) \multimap \mathrm{D}(Q)) \\ (z, s) &\mapsto r\left(z \otimes s^{(!)}\right) \end{aligned}$$

linear in its first argument but not in the second argument.

Given

- $z \in \mathrm{PD}(W)$, that is z is a subprobability distribution on words
- $s \in \mathrm{P}(\mathrm{D}(A) \otimes \mathrm{D}(Q) \multimap \mathrm{D}(Q))$ is a stochastic automaton

$$\widehat{r}(z, s) = \sum_{k \in \mathbb{N}} \sum_{\alpha_1, \ldots, \alpha_k \in A} z_{\langle \alpha_1, \ldots, \alpha_k \rangle} s(\alpha_k) \cdots s(\alpha_1)$$

where $s(\alpha) \in \mathrm{P}(\mathrm{D}(Q) \multimap \mathrm{D}(Q))$ is given by $s(\alpha)_{q,q'} = s_{\alpha,q,q'}$: the transition matrix associated with letter α.

If $i, f \in Q$ (initial and finite state), $\widehat{r}(z, s)_{i,f} \in [0, 1]$ is the probability that we can reach f starting from i.

Pcoh is a very expressive setting

Fact

If $s \in \mathrm{P}(!X \multimap X)$ *then* $\widehat{s} : \mathrm{P}X \to \mathrm{P}X$ *is Scott continuous, that is*

- $x \leq y \Rightarrow \widehat{s}(x) \leq \widehat{s}(y)$ *(where* $x \leq y$ *simply means* $\forall a \in |X|\ x_a \leq y_a$*)*
- *and if* $(x(n))_{n\in\mathbb{N}}$ *is a monotone sequence in* $\mathrm{P}X$*, we have*

$$\widehat{s}(\sup_{n\in\mathbb{N}} x(n)) = \sup_{n\in\mathbb{N}} \widehat{s}(x(n))\,.$$

As a consequence $\widehat{s}$ *has a least fixed point* $\sup_{n\in\mathbb{N}} \widehat{s}^n(0) \in \mathrm{P}X$*.*

And better, we have $\mathcal{Y} \in \mathbf{Pcoh}(!(!X \multimap X), X)$ such that

$$\forall s \in \mathsf{P}(!X \multimap X) \quad \widehat{\mathcal{Y}}(s) = \sup_{n \in \mathbb{N}} \widehat{s}^n(0)\,.$$

So we have general recursion in **Pcoh**.

A simple example of fixed point

For instance consider

$$t \in \mathbf{Pcoh}((\mathbb{1} \oplus \mathbb{1}) \otimes (!\mathbb{1} \multimap \mathbb{1}), !\mathbb{1} \multimap \mathbb{1})$$

such that, for $x \in \mathrm{P}(\mathbb{1} \oplus \mathbb{1})$, $s \in \mathrm{P}(!\mathbb{1} \multimap \mathbb{1})$,
$s' = \widehat{t}(x, s) \in \mathrm{P}(!\mathbb{1} \multimap \mathbb{1})$ is characterized by

$$\widehat{s'}(y) = x_{\mathbf{t}} y + x_{\mathbf{f}} \widehat{s}(y)^2$$

For each $x \in \mathrm{P}(\mathbb{1} \oplus \mathbb{1})$, the function $s \mapsto s'$ has a least fixed point s which satisfies

$$\forall y \in [0,1] \quad \widehat{s}(y) = x_{\mathbf{t}} y + x_{\mathbf{f}} \widehat{s}(y)^2$$

We can solve this equation:

$$\widehat{s}(y) = \begin{cases} x_{\mathbf{t}} y & \text{if } x_f = 0 \\ \dfrac{1 - \sqrt{1 - 4 x_{\mathbf{t}} x_{\mathbf{f}} y}}{2 x_{\mathbf{f}}} & \text{otherwise} \end{cases}$$

This can be written as a power series with ≥ 0 coefficients in y, $x_{\mathbf{t}}$ and $x_{\mathbf{f}}$.

Using $\mathcal{Y}$ we have defined an element $f \in \mathbf{Pcoh}((\mathbb{1} \oplus \mathbb{1}) \otimes !\mathbb{1}, \mathbb{1})$ such that

$$\widehat{f}(x, y) = x_{\mathbf{t}} y + x_{\mathbf{f}} \widehat{f}(x, y)^2$$

We can also solve general “recursive systems of type equations”, for instance find a unique “minimal” PCS D such that

$$D = \mathbb{1} \,\&\, (!D \multimap D) = \mathbb{1} \,\&\, (?D^{\perp} \parr D)$$

that is, a model of the pure λ-calculus.

A simpler example of recursive type

There is a “minimal solution” to the equation

$$S = \mathbb{1} \,\&\, (S \oplus S)$$

$|S|$ is obtained by iteration from $\emptyset$ of the following operation on sets:

$$E \mapsto \{(1, *)\} \cup \{(2, (1, a)) \mid a \in E\} \cup \{(2, (2, a)) \mid a \in E\}$$

so up to renaming

$$|S| = \{0, 1\}^{<\omega}$$

An *antichain* is a subset u' of $|S|$ such that $\forall a, b \in u' \ a \leq b \Rightarrow a = b$ where $\leq$ is the prefix order.

Then $x \in (\mathbb{R}_{\geq 0})^{|S|}$ is in PS iff for any antichain u' one has $\sum_{a \in u'} x_a \leq 1$.

For instance, if $s \in \{0,1\}^\omega$ then the $x \in (\mathbb{R}_{\geq 0})^{|S|}$ such that

$$x_a = \begin{cases} 1 & \text{if } a \text{ is a prefix of } s \\ 0 & \text{otherwise} \end{cases}$$

is in PS.

More generally if μ is a sub-probability measure wrt. the Borelian σ-algebra of the Cantor space $\{0,1\}^\omega$, we can define $x \in (\mathbb{R}_{\geq 0})^{|S|}$ by

$$x_a = \mu \left\{ s \in \{0,1\}^\omega \mid a \text{ prefix of } s \right\}$$

and then $x \in \mathrm{P}S$. Let us set $x = r(\mu)$.

Idea: antichains $\simeq$ open subsets of the Cantor space.

Let $t \in (\mathbb{R}_{\geq 0})^{|S \multimap S|}$ be defined by

$$t_{a,b} = \begin{cases} 1 & \text{if } a = b0 \text{ or } a = b1 \\ 0 & \text{otherwise} \end{cases}$$

We have $t \in \mathbf{Pcoh}(S, S)$.

Simply because if u' is an antichain then $\{b0, b1 \mid a \in u'\}$ is again an antichain.

Then for $x \in \mathsf{P}S$, we have $t \cdot x = x$ iff

$$\forall b \in |S| \quad x_b = x_{b0} + x_{b1}$$

which is equivalent to the existence of a subprobability distribution μ on the Cantor space such that $x = r(\mu)$.

What is so special about !_, logically?

If we have $s \in \mathbf{Pcoh}(X \otimes X, Y)$, which induces the bilinear function

$$\begin{aligned} \widehat{s} : \mathsf{P}X \times \mathsf{P}X &\to \mathsf{P}Y \\ (x(1), x(2)) &\mapsto s\,(x(1) \otimes x(2)) \end{aligned}$$

we cannot "diagonalize": the map $f : \mathsf{P}X \to \mathsf{P}Y$ defined by $f(x) = \widehat{s}(x, x)$ is not linear (it is quadratic).

We obtain the "cone" of measures on the Cantor space as the equalizer of t and the identity.

In contrast if $s \in \mathbf{Pcoh}(!X \otimes !X, Y)$, which represents the two-parameter analytic function

$$\begin{aligned} \widehat{s} : \mathsf{P}X \times \mathsf{P}X &\to \mathsf{P}Y \\ (x(1), x(2)) &\mapsto s\left(x(1)^{(!)} \otimes x(2)^{(!)}\right) \end{aligned}$$

then we can diagonalize: there is a $t \in \mathbf{Pcoh}(!X, Y)$ such that

$$\widehat{t}(x) = \widehat{s}(x, x)\,.$$

The deep reason is that we have $\mathsf{c}_X : \mathbf{Pcoh}(!X, !X \otimes !X)$ such that

$$\mathsf{c}_X \, x^{(!)} = x^{(!)} \otimes x^{(!)}$$

namely $(\mathsf{c}_X)_{m,(l,r)} = \delta_{m,l+r}$. Then $t = s \, \mathsf{c}_X$. This is *Contraction*, allows to duplicate data.

Similarly if $y \in \mathsf{P}Y$, the constant function

$$\begin{aligned} \mathsf{P}X &\to \mathsf{P}Y \\ x &\mapsto y \end{aligned}$$

is not linear (unless $y = 0$). But there is $s \in \mathbf{Pcoh}(!X, Y)$ such that $\widehat{s}(x) = s \cdot x^{(!)} = y$.

The deep reason is that we have $\mathsf{w}_X \in \mathbf{Pcoh}(!X, \mathbb{1})$ such that $\mathsf{w}_X \, x^{(!)} = 1$. This is *Weakening*, allows to erase data.

$(\mathsf{w}_X)_{m,*} = \delta_{m,[]}$

And now, what is LL?

A possible answer

A logical formalization of this kind of situation, that is, of an idealized multi-linear algebra with the following features:

- It is non degenerate in the sense that $\otimes$ and its dual $\parr$ are different operations, and similarly for direct product & and direct sum $\oplus$.
- All objects are reflexive, in the sense that $A^{\perp\perp} = A$.
- There is an exponential !_ allowing to write non-linear proofs/programs.

LL can be split in 3 fragments:

- multiplicative: constants 1 (true), $\perp$ (false), binary connectives $\otimes$ (conjunction) and $\parr$ (disjunction)
- additive: constants $\top$ (true), 0 (false), binary connectives & (conjuction) and $\oplus$ (disjunction)
- exponentials: unary connectives ! and ?.

Linear negation is defined by induction

$$1^\perp = \bot \qquad \bot^\perp = 1$$

$$(A \otimes B)^\perp = A^\perp \parr B^\perp \qquad (A \parr B)^\perp = A^\perp \otimes B^\perp$$

$$0^\perp = \top \qquad \top^\perp = 0$$

$$(A \oplus B)^\perp = A^\perp \,\&\, B^\perp \qquad (A \,\&\, B)^\perp = A^\perp \oplus B^\perp$$

$$(!A)^\perp = ?(A^\perp) \qquad (?A)^\perp = !(A^\perp)$$

so that

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

We define $A \multimap B = A^\perp \parr B$.

Interpretation of formulas in **Pcoh**

Then we define in an obvious way $[\![A]\!]$ as a PCS for each formula A:

- $[\![1]\!] = [\![\bot]\!] = \mathbb{1}$ as indeed $\mathbb{1}^\perp = \mathbb{1}$ in **Pcoh**
- $[\![\top]\!] = [\![0]\!] = \mathbb{T}$ the PCS such that $|\mathbb{T}| = \emptyset$.
- $[\![A \otimes B]\!] = [\![A]\!] \otimes [\![B]\!]$ etc

Example

$$[\![1 \oplus 1]\!] = \mathbb{1} \oplus \mathbb{1} = (\{0,1\}, \{(x_0, x_1) \in (\mathbb{R}_{\geq 0})^2 \mid x_0 + x_1 \leq 1\})$$

$$[\![1 \,\&\, 1]\!] = \mathbb{1} \,\&\, \mathbb{1} = (\{0,1\}, \{(x_0, x_1) \in (\mathbb{R}_{\geq 0})^2 \mid x_0, x_1 \leq 1\})$$

$$[\![(1 \,\&\, 1) \oplus (1 \,\&\, 1)]\!] = \{(x_0, x_1, x_2, x_3) \in (\mathbb{R}_{\geq 0})^4 \mid x_0 + x_2, x_0 + x_3, x_1 + x_2, x_1 + x_3 \leq 1\}$$

The *LL sequent calculus* is a logical system which allows to prove sequents $\vdash \Gamma$ where Γ is a list $(A_1, \ldots, A_n)$ of formulas.

Intuitively, the "," is a "meta" $\parr$ connective. As in Gentzen LK, where the "," in the sequent $\vdash F_1, \ldots, F_k$ stands for a $\vee$.

A proof is a tree whose nodes are labeled by *logical rules*, written in the format

$$\frac{\vdash \Gamma_1 \qquad \cdots \qquad \vdash \Gamma_k}{\vdash \Delta}$$

If π is a proof of $\vdash A_1, \ldots, A_k$, one defines (by induction on the tree π)

$$[\![\pi]\!] \in \mathbf{Pcoh}(\mathbb{1}, [\![A_1]\!] \parr \cdots \parr [\![A_k]\!])$$

or equivalently

$$[\![\pi]\!] \in \mathbf{Pcoh}([\![A_1^\perp]\!] \otimes \cdots \otimes [\![A_{i-1}^\perp]\!] \otimes [\![A_{i+1}^\perp]\!] \otimes \cdots \otimes [\![A_k^\perp]\!], [\![A_i]\!])$$

Multiplicative rules

Multiplicative constants:

$$\frac{}{\vdash 1} \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \bot}$$

Multiplicative connectives:

$$\frac{\vdash \Gamma_1, A_1 \qquad \vdash \Gamma_2, A_2}{\vdash \Gamma_1, \Gamma_2, A_1 \otimes A_2} \qquad \frac{\vdash \Gamma, A_1, A_2}{\vdash \Gamma, A_1 \parr A_2}$$

Juxtaposition of contexts

Additive rules

Additive constants:

no rule for 0 $$\frac{}{\vdash \Gamma, \top}$$

Additive connectives:

$$\frac{\vdash \Gamma, A_i}{\vdash \Gamma, A_1 \oplus A_2} \qquad \frac{\vdash \Gamma, A_1 \quad \vdash \Gamma, A_2}{\vdash \Gamma, A_1 \,\&\, A_2}$$

Superposition of contexts

Example

The "and" function of type

$$(1 \oplus 1) \otimes (1 \oplus 1) \multimap 1 \oplus 1 = ((\bot \,\&\, \bot) \parr (\bot \,\&\, \bot)) \parr (1 \oplus 1)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdash 1}{\vdash \bot, 1}}{\vdash \bot, \bot, 1}}{\vdash \bot, \bot, 1 \oplus 1}\,(\mathsf{l}) \qquad \dfrac{\dfrac{\dfrac{\vdash 1}{\vdash \bot, 1}}{\vdash \bot, \bot, 1}}{\vdash \bot, \bot, 1 \oplus 1}\,(\mathsf{r})}{\vdash \bot, \bot \,\&\, \bot, 1 \oplus 1} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\vdash 1}{\vdash \bot, 1}}{\vdash \bot, \bot, 1}}{\vdash \bot, \bot, 1 \oplus 1}\,(\mathsf{r}) \qquad \dfrac{\dfrac{\dfrac{\vdash 1}{\vdash \bot, 1}}{\vdash \bot, \bot, 1}}{\vdash \bot, \bot, 1 \oplus 1}\,(\mathsf{r})}{\vdash \bot, \bot \,\&\, \bot, 1 \oplus 1}}{\vdash \underline{\bot \,\&\, \bot}, \bot \,\&\, \bot, 1 \oplus 1}}{\vdash (\bot \,\&\, \bot) \parr (\bot \,\&\, \bot), 1 \oplus 1}}{\vdash ((\bot \,\&\, \bot) \parr (\bot \,\&\, \bot)) \parr (1 \oplus 1)}$$

Interpreted by $t \in \mathbf{Pcoh}((1 \oplus 1) \otimes (1 \oplus 1), 1 \oplus 1)$ such that

$$\widehat{t}(x, y) = x_{\mathbf{t}} y_{\mathbf{t}} e_{\mathbf{t}} + (x_{\mathbf{f}} y_{\mathbf{t}} + x_{\mathbf{t}} y_{\mathbf{f}} + x_{\mathbf{f}} y_{\mathbf{f}}) e_{\mathbf{f}}$$

$e_i \in (\mathbb{R}_{\geq 0})^I$ defined by $(e_i)_j = \delta_{i,j}$.

Exponential rules

Weakening and contraction:

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

Dereliction and promotion:

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, ?A} \qquad \frac{\vdash ?A_1, \ldots, ?A_k, B}{\vdash ?A_1, \ldots, ?A_k, !B}$$

The axiom

$$\frac{}{\vdash A^{\perp}, A}$$

There is also an echange rule

$$\frac{\vdash A_1, \ldots, A_k}{\vdash A_{f(1)}, \ldots, A_{f(k)}}$$

where $f : \{1, \ldots, k\} \to \{1, \ldots, k\}$ is a bijection. We keep its use implicit.

The cut rule

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

Theorem (Hauptsatz)

Any proof π *of* $\vdash \Gamma$ *can be transformed (by rewriting) into a cut-free proof* π_0 *of* $\vdash \Gamma$.

Moreover $[\![\pi]\!] = [\![\pi_0]\!]$.

We have built a proof π (the *and* function on booleans) of

$$\vdash \bot \,\&\, \bot, \bot \,\&\, \bot, 1 \oplus 1$$

We can "diagonalize" it as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots\,\pi}{\vdash \bot \,\&\, \bot, \bot \,\&\, \bot, 1 \oplus 1}}{\vdash ?(\bot \,\&\, \bot), \bot \,\&\, \bot, 1 \oplus 1}\ \text{der}}{\vdash ?(\bot \,\&\, \bot), ?(\bot \,\&\, \bot), 1 \oplus 1}\ \text{der}}{\vdash ?(\bot \,\&\, \bot), 1 \oplus 1}\ \text{contr}$$

This is a proof ρ and $[\![\rho]\!] = s \in \mathbf{Pcoh}(!(1 \oplus 1), 1 \oplus 1)$ such that

$$\widehat{s}(x) = \widehat{t}(x, x) = x_{\mathbf{t}}^2 e_{\mathbf{t}} + (2x_{\mathbf{t}} x_{\mathbf{f}} + x_{\mathbf{f}}^2) e_{\mathbf{f}}\ .$$

A simple use of promotion

This proof ρ represents a non-linear (actually quadratic) function $1 \oplus 1 \to 1 \oplus 1$.

We should be able to "compose it with itself", this is exactly the purpose of the promotion rule (combined with cut):

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ \rho\\ \vdash ?(\bot \,\&\, \bot), 1 \oplus 1\end{array}}{\vdash ?(\bot \,\&\, \bot), !(1 \oplus 1)}\ \text{prom} \qquad \begin{array}{c}\vdots\ \rho\\ \vdash ?(\bot \,\&\, \bot), 1 \oplus 1\end{array}}{\vdash ?(\bot \,\&\, \bot), 1 \oplus 1}\ \text{cut}$$

getting an "homogeneous polynomial of degree 4" on booleans:

$$x_{\mathbf{t}}^4 e_{\mathbf{t}} + (4x_{\mathbf{t}}^3 y_{\mathbf{f}} + 6x_{\mathbf{t}}^2 y_{\mathbf{f}}^2 + 4x_{\mathbf{t}} y_{\mathbf{f}}^3 + y_{\mathbf{f}}^4) e_{\mathbf{f}}$$

The Girard translation: representing the CBN λ-calculus in LL

Types

Let ι be a ground type.

$$\sigma, \tau, \cdots := \iota \mid \sigma \Rightarrow \tau$$

We choose a formula ι of LL and we define σ^* as a formula of LL by

$$(\sigma \Rightarrow \tau)^* = (!\sigma^* \multimap \tau^*)$$

Terms

$$M, N, \cdots := x \mid \lambda x^{\sigma}\, M \mid (M)\, N$$

Given a term M, a context $\Sigma = (x_1 : \sigma_1, \ldots, x_k : \sigma_k)$ and a type τ such that $\Sigma \vdash M : \tau$, we can define M^*_Σ, a proof of

$$\vdash ?({\sigma_1}^*)^\perp, \ldots, ?({\sigma_k}^*)^\perp, \tau^*$$

The translation is by induction on M.

If $M = x_i$, so that $\tau = \sigma_i$, M^* is

$$\dfrac{\dfrac{\overline{\vdash ({\sigma_i}^*)^\perp, {\sigma_i}^*}\ \text{ax}}{\vdash ?({\sigma_i}^*)^\perp, {\sigma_i}^*}\ \text{der}}{\vdash ?({\sigma_1}^*)^\perp, \ldots, ?({\sigma_i}^*)^\perp, \ldots, ?({\sigma_k}^*)^\perp, {\sigma_i}^*}\ \text{weak}$$

If $M = \lambda x^\sigma N$ so that $\tau = \sigma \Rightarrow \varphi$ and hence $\tau^* = ?(\sigma^*)^\perp \parr \varphi^*$, then by inductive hypothesis we have a proof

$$\dfrac{\begin{array}{c}\vdots\ M^*_{\Sigma, x:\sigma} \\ \vdash ?({\sigma_1}^*)^\perp, \ldots, ?({\sigma_k}^*)^\perp, ?(\sigma^*)^\perp, \varphi^*\end{array}}{\vdash ?({\sigma_1}^*)^\perp, \ldots, ?({\sigma_k}^*)^\perp, ?(\sigma^*)^\perp \parr \varphi^*}\ \parr$$

If $M = (N)\,P$ with $\Sigma \vdash N : \varphi \Rightarrow \tau$ and $\Sigma \vdash P : \varphi$. Let $\Gamma = (?({\sigma_1}^*)^\perp, \ldots, ?({\sigma_k}^*)^\perp)$ then M^*_Σ is

$$
\dfrac{
\begin{array}{c} \vdots\ N^*_\Sigma \\ \vdash \Gamma, ?(\varphi^*)^\perp \parr \tau^* \end{array}
\qquad
\dfrac{
\dfrac{\begin{array}{c} \vdots\ P^*_\Sigma \\ \vdash \Gamma, \varphi^* \end{array}}{\vdash \Gamma, !\varphi^*}\,\text{prom}
\qquad
\dfrac{}{\vdash \tau^*, (\tau^*)^\perp}\,\text{ax}
}{\vdash \Gamma, \tau^*, !\varphi^* \otimes (\tau^*)^\perp}\,\otimes
}{
\dfrac{\vdash \Gamma, \Gamma, \tau^*}{\vdash \Gamma, \tau^*}\,\text{contr}
}\,\text{cut}
$$

because all formulas of Γ are of shape $?A$. It is only for this reason that we can use promotion and contraction.

This translation preserves β-reduction: if $M \; \beta \; M'$ then M^*_Σ reduces to M'^*_Σ by cut elimination.

The converse is morally true.

What can we compute in LL?

Nothing more than in the simply typed λ-calculus. . .

But we can extend LL so as to make it more expressive:

- 2nd order (or more)
- least and greatest fixed points of types
- extension allowing non-terminating "proofs": "untyped" LL *à la* Danos-Regnier, LL with a ground type of integers and general recursion analog to PCF etc.

Conclusion (provisional)

LL allows to embed functional computations in a more symmetric world, where the input/output or program/environment dichotomy is transformed.

LL *polarities* are exactly about this dichotomy.

Polarities

To be continued!