



Les espaces cohérents

un modèle assez fidèle des preuves en logique linéaire multiplicative

Christian Retoré

Université de Bordeaux, LaBRI-CNRS & INRIA

PEPS Relations Maison des Sciences de l'Homme de Paris-Nord,
Saint-Denis, 15-16 décembre 2008

Sources

Pour l'essentiel : Jean-Yves Girard

- Linear Logic, *Theoretical Computer Science* (1987)
- *Cours de DEA / Proofs and types*, Cambridge University Press (1987 / 1988)
- *Le point aveugle (tomes I et II)*, Hermann (2006 et 2007)

Pour le point particulier présenté :

- Résultat initial : Christian Retoré A semantic characterisation of the correctness of a proof net, *Mathematical Structure in Computer Science* (1998)
- Développements subséquents non abordés ici : Michele Pagani *Proof nets and cliques : towards the understanding of analytical proofs*, thèse, Università Roma Tre et Université Aix-Marseille II (2006)

Niveaux de fondations

Girard distingue 3 niveaux :

(-1) prouvabilité, valeurs de vérités

(-2) preuves statiques (modulo la dynamique de l'évaluation)

(-3) dynamique des preuves, interaction entre preuves et contre preuves, jeux/ludique

évaluation : on redémontre un lemme à chaque fois qu'on l'utilise.....
passer d'un langage de haut-niveau à de l'assembleur

dénotationnel : en logique (-1) en informatique (-2)

Cet exposé porte sur le niveau (-2).

Lambda calcul typé et de la logique intuitionniste

	Types	Formules
	Preuves	Programmes
	β réduction	Evaluation
	Normalisation	
	Elimination des coupures	

Sémantique dénotationnelle

[programme avant évaluation] = [programme après évaluation]

$$(f \mapsto f \circ f)(x \mapsto 2^x)3 = 256 = (x \mapsto x/2)512$$

[Formule (propositionnelle) A] = espace cohérent A

[Preuve de $A \vdash B$ (modulo réduction)] = morphisme de $[A]$ dans $[B]$

Définition d'un espace cohérent

Espace cohérent A :

Ensembles de points $|A|$, trame

Relation symétrique et antiréflexive $t \frown t'$ entre points de $|A|$.

On utilise les abréviations très pratiques que voici :

$$x \smile x' \equiv (x \neq x' \wedge \neg(x \circ x'))$$

$$x \circ x' \equiv ((x = x') \vee (x \frown x'))$$

$$x \preceq x' \equiv ((x = x') \vee (x \smile x'))$$

Objet = "clique" ensembles de points deux à deux cohérents, notation $a \sqsubset A$.

Morphismes de A dans B : fonctions stables c.-à-d. fonction des cliques de A dans les cliques de B satisfaisant :

- croissance : $a \subset a' \sqsubset A \Rightarrow F(a) \subset F(a') \sqsubset B$
- continuité : si $a_1 \subset a_2 \cdots \subset a \sqsubset A$ alors $F(\bigcup a_i) = \bigcup F(a_i) \sqsubset B$
- stabilité : si $a \cup a' \sqsubset A$ alors $F(a \cap a') = F(a) \cap F(a')$

Propriété : si $x \in F(a)$ avec F stable alors il existe un unique $a_0 \subset_{\text{fini}} a$ minimal (pour l'inclusion) tel que $x \in F(a)$ (a est donc minimum).

Produit d'espaces cohérents

Produit : $A \& B$ trame somme disjointe $|A| \times \{0\} \cup |B| \times \{1\}$,
cohérence : $\forall x \in |A| \forall y \in |B| (x, 0) \frown (y, 1)$

Espaces fonctionnels (exponentiation)

L'ensemble des morphismes de A dans B peut être vu comme un espace cohérent $A \rightarrow B$,

- points sont les (a, y) avec $a \sqsubset_{\text{fini}} A$ (cliques finies de A) et $y \in |B|$,
- avec $(a, y) \subset (a', y')$ ssi

$$[(a \cup a') \sqsubset A \Rightarrow y \subset y'] \wedge [(a \cup a') \sqsubset A \wedge a \neq a'] \Rightarrow y \subset y'$$

Espaces fonctionnels (exponentiation)

Une fonction stable de A dans B s'identifie avec une clique de $A \rightarrow B$ en prenant les couples (a, y) tel que $y \in F(a)$ et a minimum pour cette propriété (cf. ci-avant). Ces couples sont nommés le squelette de la fonction stable (anciennement trace, mais gênant car l'algèbre linéaire est proche).

Réciproquement, étant donnée une clique C on définit la fonction stable lui correspondant par $C(a) = \{y \in |B| \mid \exists u \subset a(u, y) \in C\}$

Interprétation

On interprète ainsi la logique propositionnelle intuitionniste (le lambda calcul simplement typé) de sorte que :

- les types sont des espaces cohérents,
 - arbitraire pour les types atomiques (variables propositionnelles)
 - construit avec le produit et l'exponentiation pour les types complexes, par exemple $A \rightarrow ((A \& B) \rightarrow B)$
- une preuve d de $A_1, \dots, A_n \vdash C$ (les lambda termes de type C avec des variables libres de type A_1, \dots, A_n) est interprétée, inductivement comme un morphisme de l'espace cohérent $A_1 \& \dots \& A_n$ vers l'espace cohérent C ou comme une clique de $(A_1, \dots, A_n) \rightarrow C$

Une interprétation dénotationnelle au sens informatique

Cette interprétation, calculée inductivement sur la dérivation, est préservée par le mécanisme d'évaluation β réduction (normalisation, élimination des coupures). Un problème, la **full abstraction**, comment caractériser les cliques qui sont l'interprétation de programmes (leur maximalité de suffit pas).

Linéarité

Les morphismes dont le Squelette ne contient que des couples dont le premier élément est un singleton $(\{x\}, y)$ sont dit linéaires.

On peut séparer en deux la construction de l'espace cohérent des fonctions stables de A dans $V : A \rightarrow V = (!A) \multimap V$.

$!A$ est l'espace cohérent dont les points sont les cliques finies de A . Deux cliques finies de A sont cohérentes en tant que points de $!A$ lorsque leur union est une clique de A

$U \multimap V$ est l'espace cohérent dont la trame est $|U| \times |V|$ (le produit cartésien des trames). La cohérence $(s, t) \frown (s', t')$ est définie par $(s \subset s'[U] \rightarrow t \subset t'[V]) \wedge (s \frown s'[U] \Rightarrow t \frown t'[V])$

Les fonctions linéaires sont davantage symétriques, car $(\{x\}, y)$ s'identifie bien sur à (x, y) , très symétrique.

Négation, multiplicatifs

Effectivement, on voit apparaître une négation $(\dots)^\perp$ qui rend isomorphes $A \multimap B$ et $B^\perp \multimap A^\perp$.

A^\perp définie par $|A^\perp| = |A|$ et $x \frown x'[A^\perp]$ ssi $x \smile x'[A]$.

On peut alors voir que $A \multimap B$ n'est autre que $A^\perp \wp B$ ou \wp (un $\&$ à l'envers, en principe) est défini par

$U \wp V$ a pour trame $|U| \times |V|$ et $(x, y) \frown (x', y')[U \wp V]$ ssi $(x \frown x'[U]) \vee (y \frown y'[V])$

grâce à la négation on voit apparaître son dual $A \otimes B$

$U \otimes V$ a pour trame $|U| \times |V|$ et $(x, y) \frown (x', y')[U \otimes V]$ ssi $(x \frown x'[U]) \vee (y \frown y'[V])$

La logique linéaire

Le noyau de la logique linéaire, la logique linéaire multiplicative est un système logique sans aucune règle structurelle, avec la négation $(\dots)^\perp$, une disjonction (\wp) et une conjonction (\otimes).

Ces connecteurs sont dit multiplicatifs : leur trame est le produit cartésien des trames.

$\&$ et son dual \oplus , défini par $A \oplus B = (A^\perp \& B^\perp)^\perp$, sont dit additifs (leur trame est la somme disjointes des trames).

Propriétés algébrique des connecteurs

L'exponentielle ! (déjà vue) transforme additifs en multiplicatifs.

Les multiplicatifs sont distributifs sur les additifs de graphisme similaire (\otimes sur \oplus , et \wp sur $\&$).

Tous les connecteurs sont associatifs et commutatifs.

On a les lois de De Morgan : $(A^\perp)^\perp = A$, $(A\wp B)^\perp = A^\perp \otimes B^\perp$ et $(A \otimes B)^\perp = A^\perp \wp B^\perp$.

Et les relations, dans tout ça ?

Logique intuitionniste \longrightarrow *logique linéaire*
Preuve=fonction \longrightarrow *preuve=relation*

Syntaxe : calcul des séquents (règles structurelles)

Les lois de De Morgan permettent une formulation unilatère du calcul des séquents.

Ce calcul des séquent a pour seule règle structurelle l'échange (sans cela logique linéaire cyclique, calcul de Lambek, NL,...)

$$\frac{\vdash X_1, \dots, X_n}{\vdash X_{\sigma(1)}, \dots, X_{\sigma(n)}} \text{ échange } [\sigma \text{ permutation de } \{1, \dots, n\}]$$

Syntaxe : calcul des séquents (règles logiques)

$$\frac{\vdash X_1, \dots, X_n, A \quad \vdash B, Y_1, \dots, Y_p}{\vdash X_1, \dots, X_n, A \otimes B, Y_1, \dots, Y_p} \otimes$$

$$\frac{\vdash X_1, \dots, X_n, A, B}{\vdash X_1, \dots, X_n, A \wp B} \wp$$

Identité et dynamique

$\vdash A, A^\perp$

Composition de preuve (de $A \vdash K$ et $K \vdash C$ on déduit $A \vdash C$)

$$\frac{\vdash X_1, \dots, X_n, K \quad \vdash K^\perp, Y_1, \dots, Y_p}{\vdash X_1, \dots, X_n, Y_1, \dots, Y_p} \textit{cut}$$

Une variante : MIX

Possiblement, en tout cas avec les espaces cohérents, la règle MIX
 $(A \otimes B) \multimap (A \wp B)$:

$$\frac{\vdash X_1, \dots, X_n \quad \vdash Y_1, \dots, Y_p}{\vdash X_1, \dots, X_n, Y_1, \dots, Y_p} \text{MIX}$$

Dynamique : l'élimination des coupures (cas de base logique)

$$\frac{\frac{\frac{\vdots a}{\vdash X_1, \dots, X_n, A} \quad \frac{\vdots b}{\vdash B, Z_1, \dots, Z_m} \otimes \quad \frac{\vdots c}{\vdash A^\perp, B^\perp, Y_1, \dots, Y_p} \wp}{\vdash X_1, \dots, X_k, Z_1, \dots, Z_m, A \otimes B} \otimes \quad \frac{\vdash A^\perp \wp B^\perp, Y_1, \dots, Y_p}{} \wp}{\vdash X_1, \dots, X_n, Z_1, \dots, Z_m, Y_1, \dots, Y_p} cut$$

se réduit en

$$\frac{\frac{\vdots b}{\vdash B, Z_1, \dots, Z_m} \quad \frac{\frac{\frac{\vdots a}{\vdash X_1, \dots, X_n, A} \quad \frac{\vdots c}{\vdash A^\perp, B^\perp, Y_1, \dots, Y_p} cut}{\vdash X_1, \dots, X_n, B^\perp, Y_1, \dots, Y_p} cut}{\vdash X_1, \dots, X_n, Z_1, \dots, Z_m, Y_1, \dots, Y_p} cut$$

Dynamique : l'élimination des coupures (cas de base logique)

$$\frac{\vdash A, A^\perp \vdash X_1, \dots, X_n, A \quad \vdots a}{\vdash X_1, \dots, X_n, A} \textit{cut}$$

se réduit en :

$$\vdash X_1, \dots, X_n, A \quad \vdots a$$

Calcul standard de la sémantique

L'interprétation d'une preuve de A_1, \dots, A_k est une clique de A_1, \dots, A_n . Vérification règle à règle, par induction.

Axiome : (x, x) clique de $A \wp A^\perp$

\wp évident

\otimes assez évident (assembler les n-uplets).

cut : prendre tous les n-uplets $(x_1, \dots, x_n, y_1, \dots, y_p)$ pour lesquels il existe k tel que (x_1, \dots, x_n, k) soit dans l'interprétation de la première sous preuve et (k, y_1, \dots, y_p) dans l'interprétation de la seconde sous preuve.

Moralité

Preuve de $A_1 \wp \cdots \wp A_n$ relation n-aire (typée) sur les trames qui définit une clique par rapport à l'espace associée à la formule démontrée.

En particulier preuve de $A_1 \wp \cdots \wp A_2$ ou de $A_1^\perp \vdash A_2$ ou de $A_2^\perp \vdash A_1$ relation binaire sur $|A_1| \times |A_2|$ qui définit une clique par rapport à l'espace associée à $A_1 \wp A_2$.

Syntaxe moins séquentielle : réseaux de démonstration

Girard, Danos-Regnier, Retoré,...

Preuve inductive (il existe une dérivation) preuve comme un graphe satisfaisant une propriété universelle.

Élimination des coupures.

Au tableau...

Expériences, résultats

Expériences : choisir des valeurs pour les axiomes, propager ces valeurs, puis collecter les n-uplets sur les conclusions en en faisant un grand n-uplet — s'il y a des coupures ne garder que celles qui donnent les mêmes valeurs sur les formule K et K^\perp d'une coupure. Par exemple pour tout x de l'espace cohérent associé à A ; (x, x) est un ensemble de couple d'élément de $|A| \times |A^\perp|$ qui sont toujours cohérents deux à deux selon $A \wp A^\perp$ (deux points distincts de $|A|$ sont cohérents dans A ou dans A^\perp , et donc les couples correspondant sont cohérents dans $A \wp A^\perp$).

Correction syntaxique \Rightarrow interprétabilité sémantique

Théorème (Girard 87) Si le réseau est correct, alors deux expériences sont cohérentes dans l'espace cohérent conclusion.

Idée de la preuve, choisir une conclusion où les expériences sont incohérentes, et faire un chemin incohérent quand il monte et cohérent quand il descend. Un tel chemin est élémentaire alternant et indéfiniment prolongeable, donc il donne lieu à un cycle.

Interprétabilité sémantique \Rightarrow correction syntaxique

Réciproque Si le réseau n'est pas correct alors on peut trouver deux expériences qui sont pas cohérentes.

On peut choisir affecter le même espace cohérent N à chaque variable propositionnelle ce qui donne un critère (décidable).

Idée, lemme : quand dans un réseau correct il y a un chemin d'une conclusion X à une autre Y , on mettant tous les axiomes rencontrés $A : \curvearrowright - A^\perp : \curvearrowleft$ on obtient $X : \curvearrowright$ et $Y : \curvearrowleft$.

Réseaux pas correct : si on retire un lien conclusion et qu'il reste incorrect, hypothèse d'induction ; si on retire un lien conclusion et qu'il devient correct c'est que ce lien est un tenseur, avec un chemin entre les deux prémisses. On applique le lemme entre les deux prémisses.

Interprétation et réduction

Certains réseaux non corrects se réduisent en un réseau correct, et ont donc la même interprétation que le résultat correct.

La méthode permet aussi de prédire la correction du réseau réduit sans le réduire.

Un réseau donnera un réseau réduit correct, si deux expériences distinctes donnent toujours des résultats distincts.

Conclusion

On peut interpréter les preuves comme des relations entre les formules établies dans un même séquent, invariant par le calcul ou l'évaluation par élimination des coupures — niveau (-2) et pas (-3). Cela n'identifie pas toutes les preuves de $A \vdash B$ — niveau (-2) et non (-1).

Cette interprétation a lieu dans des ensembles munis d'une relation pour structurer l'ensemble et pour avoir une notion de fonction qui permette de construire l'espace des fonctions de A dans B . Cette relation peut se voir comme la cohérence entre des informations élémentaires (que l'on sait ensuite étendre aux types complexes).

L'interprétation en termes d'informations 2 à 2 cohérentes, un environnement logique et compositionnel, font espérer un sens intuitif pour la linguistique formelle (sémantique de Montague, sémantique lexicale). À ce jour, cela reste une simple analogie.