Focalisation and Classical Realisability

Guillaume Munch-Maccagnoni

Pablo Donato

1er avril 2020

Université de Paris

Contexte et motivations

Preuves et programmes

Deux approches historiques à la correspondance preuves-programmes :

- **Formules = types** (Curry, Howard, Griffin…) :

$$\text{preuve} \Longleftrightarrow \text{programme}$$

- **Formules = spécifications** (Kleene, Kreisel, Krivine…) :

$$\text{preuve} \Longrightarrow \text{programme}$$

Isomorphisme **syntaxique** entre logique et calcul :

Formule	$\iff$	Type
Preuve	$\iff$	Programme
Élimination des coupures	$\iff$	Exécution

- On ne s'intéresse qu'aux programmes **bien typés**...
- ...vus comme une syntaxe de **termes** pour les preuves

S'applique à de nombreuses logiques, incarnées dans divers systèmes de déduction/langages de programmation :

	Intuitionniste	Classique
Systèmes à la Hilbert	Logique Combinatoire	Logique Combinatoire Classique
Déduction naturelle	λ-calcul (simplement typé, polymorphe…)	$\lambda\mu$-calcul
Calcul des séquents	Machine de Krivine	Système L

Mais aussi logique linéaire, logiques modales… et biensûr *théorie des types* !

Interprétation “**sémantique**” de la logique dans le calcul :

Interprétation BHK (Brouwer-Heyting-Kolmogorov)

Une preuve de $A \Rightarrow B$ est une **fonction** qui prend une preuve de A et renvoie une preuve de B.

- On s’autorise un espace de fonctions **plus riche** que celui des preuves !
- Permet de donner un contenu calculatoire à des théories **mathématiques** et pas seulement logiques

S'applique à diverses théories intuitionnistes et classiques, interprétées dans divers langages de programmations :

	Intuitionniste	Classique
Logique du 2^{nd} ordre	Système F	Système L
Arithmétique du 2^{nd} ordre	Système F	λ_c-calcul
Théorie des ensembles	?	λ_c-calcul
HoTT	Théorie des types cubiques	–

Séquents $\Longleftrightarrow$ Machines abstraites

Groupe identité

$$\frac{}{A \vdash A}\,\mathrm{ax} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\mathrm{cut}$$

Groupe structurel

$$\frac{\Gamma \vdash \Delta, A, B, \Delta'}{\Gamma \vdash \Delta, B, A, \Delta'}\,xR \qquad \frac{\Gamma, A, B, \Gamma' \vdash \Delta}{\Gamma, B, A, \Gamma' \vdash \Delta}\,xL$$

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

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

Groupe logique

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\neg R \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\neg L$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}\Rightarrow R \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \Rightarrow B \vdash \Delta, \Delta'}\Rightarrow L$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\wedge R \qquad \frac{\Gamma, A_i \vdash \Delta}{\Gamma, A_1 \wedge A_2 \vdash \Delta}\wedge L_i$$

$$\frac{\Gamma \vdash A_i, \Delta}{\Gamma \vdash A_1 \vee A_2, \Delta}\vee R_i \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\vee L$$

Termes

$$
\begin{array}{rcll}
t, u & ::= & x & \text{(Variable)} \\
& | & \mu\alpha.c & \text{(Abstraction de contexte)} \\
& | & [e] & \text{(Réification de contexte)} \\
& | & \lambda x.t & \text{(Fonction)} \\
& | & \mu\,(\pi_1 \cdot \alpha_1.c_1 \mid \pi_2 \cdot \alpha_2.c_2) & \text{(Paire)} \\
& | & \iota_1(t) \mid \iota_2(t) & \text{(Injections)}
\end{array}
$$

Contextes d'évaluation

$$
\begin{array}{rcll}
e & ::= & \alpha & \text{(Co-variable)} \\
& | & \tilde{\mu}x.c & \text{(Abstraction de terme)} \\
& | & \tilde{\mu}[\alpha].c & \text{(Récupération de contexte)} \\
& | & t \cdot e & \text{(Argument)} \\
& | & \pi_1 \cdot e \mid \pi_2 \cdot e & \text{(Projections)} \\
& | & \tilde{\mu}\,(\iota_1(x_1).c_1 \mid \iota_2(x_2).c_2) & \text{(Pattern matching)}
\end{array}
$$

Commandes

$$c ::= \langle t \parallel e \rangle$$

Groupe identité

$$\frac{}{x : A \vdash x : A \mid}\,\mathrm{ax}R \qquad \frac{}{\mid \alpha : A \vdash \alpha : A}\,\mathrm{ax}L$$

$$\frac{\Gamma \vdash t : A \mid \Delta \quad \Gamma' \mid e : A \vdash \Delta'}{\langle t \parallel e \rangle : (\Gamma, \Gamma' \vdash \Delta, \Delta')}\,\mathrm{cut}$$

Groupe structurel

$$\frac{c : (\Gamma \vdash \Delta, \alpha : A, \beta : B, \Delta')}{c : (\Gamma \vdash \Delta, \beta : B, \alpha : A, \Delta')}\,xR \qquad \frac{c : (\Gamma, x : A, y : B, \Gamma' \vdash \Delta)}{c : (\Gamma, y : B, x : A, \Gamma' \vdash \Delta)}\,xL$$

$$\frac{c : (\Gamma \vdash \Delta)}{c : (\Gamma \vdash \alpha : A, \Delta)}\,wR \qquad \frac{c : (\Gamma \vdash \Delta)}{c : (\Gamma, x : A \vdash \Delta)}\,wL$$

$$\frac{c : (\Gamma \vdash \alpha : A, \beta : A, \Delta)}{c[\alpha \,/\, \beta] : (\Gamma \vdash \alpha : A, \Delta)}\,cR \qquad \frac{c : (\Gamma, x : A, y : A \vdash \Delta)}{c[x \,/\, y] : (\Gamma, x : A \vdash \Delta)}\,cL$$

Groupe logique

$$\frac{\Gamma \mid e : A \vdash \Delta}{\Gamma \vdash [e] : \neg A \mid \Delta}\,\neg R \qquad \frac{c : (\Gamma \vdash \alpha : A, \Delta)}{\Gamma \mid \tilde{\mu}[\alpha].c : \neg A \vdash \Delta}\,\neg L$$

$$\frac{\Gamma, x : A \vdash t : B \mid \Delta}{\Gamma \vdash \lambda x.t : A \Rightarrow B \mid \Delta}\,{\Rightarrow}R \qquad \frac{\Gamma \vdash t : A \mid \Delta \quad \Gamma' \mid e : B \vdash \Delta'}{\Gamma, \Gamma' \mid t \cdot e : A \Rightarrow B \vdash \Delta, \Delta'}\,{\Rightarrow}L$$

$$\frac{c_1 : (\Gamma \vdash \alpha_1 : A, \Delta) \quad c_2 : (\Gamma \vdash \alpha_2 : B, \Delta)}{\Gamma \vdash \mu\,(\pi_1 \cdot \alpha_1.c_1 \mid \pi_2 \cdot \alpha_2.c_2) : A \wedge B \mid \Delta}\,\wedge R \qquad \frac{\Gamma \mid e : A_i \vdash \Delta}{\Gamma \mid \pi_i \cdot e : A_1 \wedge A_2 \vdash \Delta}\,\wedge L_i$$

$$\frac{\Gamma \vdash t : A_i \mid \Delta}{\Gamma \vdash \iota_i(t) : A_1 \vee A_2 \mid \Delta}\,\vee R_i \qquad \frac{c_1 : (\Gamma, x_1 : A \vdash \Delta) \quad c_2 : (\Gamma, x_2 : B \vdash \Delta)}{\Gamma \mid \tilde{\mu}\,(\iota_1(x_1).c_1 \mid \iota_2(x_2).c_2) : A \vee B \vdash \Delta}\,\vee L$$

Calcul défini comme **interaction** entre un terme t et son contexte e dans la commande $\langle t \parallel e \rangle$:

β-réduction

$$\langle \lambda x.t \parallel u \cdot e \rangle \to_\beta \langle u \parallel \tilde{\mu} x. \langle t \parallel e \rangle \rangle \qquad \text{(Fonction/Argument)}$$

$$\langle \mu\, (\pi_1 \cdot \alpha_1.c_1 \mid \pi_2 \cdot \alpha_2.c_2) \parallel \pi_1 \cdot e \rangle \to_\beta c_1[e \,/\, \alpha_1] \qquad \text{(Paire/Projection)}$$

$$\langle \iota_1(t) \parallel \tilde{\mu}\, (\iota_1(x_1).c_1 \mid \iota_2(x_2).c_2) \rangle \to_\beta c_1[t \,/\, x_1] \qquad \text{(Injection/Pattern-matching)}$$

$$\vdots$$

μ-réduction

$$\langle \mu\alpha.c \parallel e \rangle \to_\mu c[e \,/\, \alpha]$$

$$\langle t \parallel \tilde{\mu} x.c \rangle \to_\mu c[t \,/\, x]$$

$\rightarrow_\mu$ **non-confluente** à cause de la *paire critique* :

$$c[\tilde{\mu}x.c' \,/\, \alpha] \overset{?}{\leftarrow} \langle \mu\alpha.c \parallel \tilde{\mu}x.c' \rangle \overset{?}{\rightarrow} c'[\mu\alpha.c \,/\, x]$$

Deux solutions possibles :

1. (Curien/Herbelin) choix *global* en fixant une **stratégie d'évaluation** :

$$c[\tilde{\mu}x.c' \,/\, \alpha] \xleftarrow{\text{cbv}} \langle \mu\alpha.c \parallel \tilde{\mu}x.c' \rangle \xrightarrow{\text{cbn}} c'[\mu\alpha.c \,/\, x]$$

2. (Munch-Maccagnoni) choix *local* en fixant l'ordre d'évaluation dans les **constructions du langage** (termes/types)

Focalisation

Formules

$$\begin{array}{rcll} A, B & ::= & X \mid X^\perp & \text{(Atomes)} \\ & \mid & A \otimes B \mid A \mathbin{\&} B & \text{(Conjonctions)} \\ & \mid & A \oplus B \mid A \parr B & \text{(Disjonctions)} \end{array}$$

Négation

$\cdot^\perp$ définie inductivement par dualité de De Morgan :

$$\begin{array}{ll} (A \otimes B)^\perp \triangleq A^\perp \parr B^\perp & (A \parr B)^\perp \triangleq A^\perp \otimes B^\perp \\ (A \oplus B)^\perp \triangleq A^\perp \mathbin{\&} B^\perp & (A \mathbin{\&} B)^\perp \triangleq A^\perp \oplus B^\perp \end{array}$$

En programmation logique, Andreoli découvre que la recherche d'une preuve peut être organisée en une **alternance** de deux phases :

- **Asynchrone** : décomposition de toutes les formules **négatives** *dès que possible*
- **Synchrone** : choix d'une formule **positive**, et décomposition de toutes ses sous-formules jusqu'à la prochaine phase asynchrone (c'est la focalisation)

Cette nouvelle dualité reflète l'**inversibilité** des règles d'introduction des connecteurs.

Formules

$$
\begin{array}{rcll}
A, B & ::= & X \mid X^{\perp} & \text{(Atomes)} \\
 & \mid & A \otimes B \mid A \,\&\, B & \text{(Conjonctions)} \\
 & \mid & A \oplus B \mid A \parr B & \text{(Disjonctions)}
\end{array}
$$

Négation

$\cdot^{\perp}$ définie inductivement par dualité de De Morgan :

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

Polarité $\iff$ Ordre d'évaluation

- Munch-Maccagnoni interprète cette dualité comme celle entre évaluations stricte (cbv) et paresseuse (cbn)
- Réduction **focalisante** basée sur une syntaxe de **valeurs polarisées** :

$$\begin{aligned} V &::= V_+ \mid t_- \\ V_+ &::= x \mid (V, V) \mid \iota_i(V) \\ t_- &::= \alpha \mid \mu\,(\kappa, \kappa')\,.c \mid \mu\,(\iota_1(\kappa_1).c_1 \mid \iota_2(\kappa_2).c_2) \end{aligned}$$

- Formes normales $\iff$ Preuves focalisées

Remarque : on a remplacé la dualité terme/contexte par positif/négatif, on peut alors oublier la distinction droite/gauche des séquents.

$$\frac{}{\vdash x : P \mid x : P^{\perp}}\ (ax_+) \qquad \frac{}{\vdash \alpha : N \mid \alpha : N^{\perp}}\ (ax_-)$$

$$\frac{c : (\vdash \kappa : A, \Gamma)}{\vdash \mu\kappa.c : A \mid \Gamma}\ (\mu) \qquad \frac{\vdash t : A \mid \Gamma \qquad \vdash u : A^{\perp} \mid \Delta}{\langle t \parallel u \rangle : (\vdash \Gamma, \Delta)}\ (\text{cut})$$

$$\frac{\vdash t : A \mid \Gamma \qquad \vdash u : B \mid \Delta}{\vdash (t, u) : A \otimes B \mid \Gamma, \Delta}\ (\otimes) \qquad \frac{c : (\vdash \kappa : A, \kappa' : B, \Gamma)}{\vdash \mu(\kappa, \kappa').c : A \parr B \mid \Gamma}\ (\parr)$$

$$\frac{c : (\vdash \kappa : A, \Gamma) \qquad c' : (\vdash \kappa' : B, \Gamma)}{\vdash \mu\left(\iota_1(\kappa).c \,\middle|\, \iota_2(\kappa').c'\right) : A \,\&\, B \mid \Gamma}\ (\&) \qquad \frac{\vdash t : A \mid \Gamma}{\vdash \iota_i(t) : A_1 \oplus A_2 \mid \Gamma}\ (\oplus_i)$$

$$\frac{c : (\vdash \Gamma)}{c : (\vdash \kappa : A, \Gamma)}\ (w) \qquad \frac{c : (\vdash \kappa : A, \kappa' : A, \Gamma)}{c[\kappa/\kappa'] : (\vdash \kappa : A, \Gamma)}\ (c)$$

Réalisabilité classique

Définition (Observation)

Une *observation* $\perp\!\!\!\perp$ est un ensemble de commandes closes, qui est clos par anti-réduction :

$$c \to c', c' \in \perp\!\!\!\perp \implies c \in \perp\!\!\!\perp$$

Définition (Orthogonalité)

t_+ est *orthogonal* à t_- (noté $t_+ \perp\!\!\!\perp t_-$) ssi $\langle t_+ \parallel t_- \rangle \in \perp\!\!\!\perp$.

Définition (Orthogonal)

L'*orthogonal* $T^\perp$ d'un ensemble de termes de même polarité T est défini par :

$$T^\perp \triangleq \{u \mid \forall t \in T, t \perp\!\!\!\perp u\}$$

On peut alors interpréter les connecteurs de la logique par des **comportements**, c'est-à-dire des ensembles de termes de même polarité **clos par biorthogonal** $\cdot^{\perp\perp}$:

$$|A \otimes B| \triangleq (|A| \times |B|)^{\perp\perp} \qquad |A \parr B| \triangleq (|A^{\perp}| \times |B^{\perp}|)^{\perp}$$
$$|A \oplus B| \triangleq (|A| + |B|)^{\perp\perp} \qquad |A \mathbin{\&} B| \triangleq (|A^{\perp}| + |B^{\perp}|)^{\perp}$$

avec

$$T \times U \triangleq \{(t, u) \mid t \in T, u \in U\}$$
$$T + U \triangleq \{\iota_1(t) \mid t \in T\} \cup \{\iota_2(u) \mid u \in U\}$$

Définition (Relation de réalisabilité)

On dit que t *réalise* A (noté $t \Vdash A$) lorsque $t \in |A|$.

Théorème (Lemme d'adéquation)

Soit t *un terme typable dans* $\mathsf{LK}_{\mathsf{pol}}$ *par* $\vdash t : B \mid \kappa_1 : A_1, ..., \kappa_n : A_n$. *Alors pour tous termes clos* $u_1, ..., u_n$, *on a :*

$$u_1 \Vdash A_1^{\perp}, ..., u_n \Vdash A_n^{\perp} \quad \Longrightarrow \quad t[\vec{u}_i / \vec{\kappa}_i] \Vdash B$$

- Propriété de **constructivité** des connecteurs (notamment propriété de la disjonction pour $\oplus$)
- **Normalisation** (faible)
- **Paramétricité** (en passant au second ordre)

Merci !