Vers une représentation finie opérationnelle des preuves infinies pour μ/ν

Rémi Nollet
avec Christine Tasson et Alexis Saurin

12–13 octobre 2017

Pourquoi les points fixes

Mon sujet

La correspondance preuve-programme entre les logiques temporelles et la programmation fonctionnelle réactive.

Exemple

$$\big(\bigcirc A\big)(n) = A(n+1)$$
$$\big(\Box A\big)(n) = \forall n' \geqslant n, A(n)$$
$$\big(\Diamond A\big)(n) = \exists n' \geqslant n, A(n)$$

Pourquoi les points fixes

$$\Box A = A \wedge \bigcirc(\Box A) \qquad \Diamond A = A \vee \bigcirc(\Diamond A)$$

Pourquoi les points fixes

$$\Box A = A \wedge \bigcirc(\Box A) \qquad \Diamond A = A \vee \bigcirc(\Diamond A)$$

$$\Box A \leftrightarrow \bot ? \qquad \Diamond A \leftrightarrow \top ?$$

$$\bot \leftrightarrow A \wedge \bigcirc \bot \qquad \top \leftrightarrow A \vee \bigcirc \top$$

Pourquoi les points fixes

$$\Box A = A \wedge \bigcirc(\Box A) \qquad \Diamond A = A \vee \bigcirc(\Diamond A)$$

$$\Box A \leftrightarrow \bot ? \qquad \Diamond A \leftrightarrow \top ?$$

$$\bot \leftrightarrow A \wedge \bigcirc \bot \qquad \top \leftrightarrow A \vee \bigcirc \top$$

$$\begin{cases} \Box A \to A \wedge \bigcirc(\Box A) \\ \dfrac{B \to A \wedge \bigcirc B}{B \to \Box A} \end{cases} \qquad \begin{cases} A \vee \bigcirc(\Diamond A) \to \Diamond A \\ \dfrac{A \vee \bigcirc B \to B}{\Diamond A \to B} \end{cases}$$

Pourquoi les points fixes

$$\Box A = A \wedge \bigcirc(\Box A) \qquad \Diamond A = A \vee \bigcirc(\Diamond A)$$

$$\cancel{\Box A \leftrightarrow \bot} \qquad \cancel{\Diamond A \leftrightarrow \top}$$

$$\bot \leftrightarrow A \wedge \bigcirc \bot \qquad \top \leftrightarrow A \vee \bigcirc \top$$

$$\begin{cases} \Box A \to A \wedge \bigcirc(\Box A) \\ \dfrac{B \to A \wedge \bigcirc B}{B \to \Box A} \end{cases} \qquad \begin{cases} A \vee \bigcirc(\Diamond A) \to \Diamond A \\ \dfrac{A \vee \bigcirc B \to B}{\Diamond A \to B} \end{cases}$$

Pourquoi les points fixes

$$\Box A \underset{\nu}{=} A \wedge \bigcirc(\Box A)$$

$$\cancel{\Box A \leftrightarrow \bot}$$

$$\bot \leftrightarrow A \wedge \bigcirc \bot$$

$$\begin{cases} \Box A \to A \wedge \bigcirc(\Box A) \\ \dfrac{B \to A \wedge \bigcirc B}{B \to \Box A} \end{cases}$$

$$\Box A = \nu X.(A \wedge \bigcirc X)$$

$$\Diamond A \underset{\mu}{=} A \vee \bigcirc(\Diamond A)$$

$$\cancel{\Diamond A \leftrightarrow \top}$$

$$\top \leftrightarrow A \vee \bigcirc \top$$

$$\begin{cases} A \vee \bigcirc(\Diamond A) \to \Diamond A \\ \dfrac{A \vee \bigcirc B \to B}{\Diamond A \to B} \end{cases}$$

$$\Diamond A = \mu X.(A \vee \bigcirc X)$$

Pourquoi les points fixes

$$\Box A \underset{\nu}{=} A \wedge \bigcirc(\Box A) \qquad \Diamond A \underset{\mu}{=} A \vee \bigcirc(\Diamond A)$$

$$\cancel{\Box A \leftrightarrow \bot} \qquad \cancel{\Diamond A \leftrightarrow \top}$$

$$\bot \leftrightarrow A \wedge \bigcirc \bot \qquad \top \leftrightarrow A \vee \bigcirc \top$$

$$\begin{cases} \Box A \to A \wedge \bigcirc(\Box A) \\ \dfrac{B \to A \wedge \bigcirc B}{B \to \Box A} \end{cases} \qquad \begin{cases} A \vee \bigcirc(\Diamond A) \to \Diamond A \\ \dfrac{A \vee \bigcirc B \to B}{\Diamond A \to B} \end{cases}$$

$$\Box A = \nu X.(A \wedge \bigcirc X) \qquad \Diamond A = \mu X.(A \vee \bigcirc X)$$

$$\begin{cases} \nu X.F[X] \to F[\nu X.F[X]] \\ \dfrac{B \to F[B]}{B \to \nu X.F[X]} \end{cases} \qquad \begin{cases} F[\mu X.F[X]] \to \mu X.F[X] \\ \dfrac{F[B] \to B}{\mu X.F[X] \to B} \end{cases}$$

Formellement

$$A, B ::= X \mid X^\perp \mid A \otimes B \mid A \parr B \mid \mathbf{1} \mid \bot \mid A \oplus B \mid A \,\&\, B$$
$$\mid \mu X.A[X]^{(*)} \mid \nu X.A[X]^{(*)}$$

- μ et ν sont des lieurs
- (*) $\mu X.A[X]$ et $\nu X.A[X]$ ne peuvent être formés que si X apparaît en position covariante dans $A[X]$

Exemples

- $\mu X.(\mathbf{1} \oplus X)$: Ok.
- $\mu X.(\mathbf{1} \oplus X^\perp)$: Nope !

Formellement

Et une négation involutive étendue par :

$$(\mu X.A[X])^\perp := \nu X.A[X^\perp]^\perp \quad \text{noté} \quad \nu X.A^\perp[X]$$

et symétriquement pour le ν

Exemples

- On ne pourrait pas former $\nu X.A[X]^\perp$: X est en position *contravariante* dans $A[X]^\perp$
- $(\mu X.X)^\perp = \nu X.(X^\perp)^\perp = \nu X.X$
- $\underbrace{(\mu X.(\mathbf{1} \oplus X))^\perp}_{\text{type des entiers}} = \underbrace{\nu X.(\perp \,\&\, X)}_{\approx \perp\&(\perp\&(\perp\&\cdots))}$

Première école : $\mu MALL$

- les règles habituelles de MALL
- plus :

$$\frac{\vdash \Gamma, A[\mu X.A[X]]}{\vdash \Gamma, \mu X.A[X]}\,\mu \qquad \frac{\vdash \Delta, S \quad \vdash S^{\perp}, A[S]}{\vdash \Delta, \nu X.A[X]}\,\nu_{\mathrm{inv}}$$

Le problème de $\mu MALL$: la réduction

$$\dfrac{\dfrac{\vdash \Gamma, A^{\perp}[\mu X.A^{\perp}[X]]}{\vdash \Gamma, \mu X.A^{\perp}[X]}\,\mu \qquad \dfrac{\vdash \Delta, S \quad \vdash S^{\perp}, A[S]}{\vdash \Delta, \nu X.A[X]}\,\nu_{\mathrm{inv}}}{\vdash \Gamma, \Delta}\,\mathsf{cut} \longrightarrow$$

Le problème de $\mu MALL$: la réduction

$$\dfrac{\dfrac{\dfrac{\vdash \Gamma, A^{\perp}[\mu X.A^{\perp}[X]]}{\vdash \Gamma, \mu X.A^{\perp}[X]}\,\mu \qquad \dfrac{\vdash \Delta, S \quad \vdash S^{\perp}, A[S]}{\vdash \Delta, \nu X.A[X]}\,\nu_{\text{inv}}}{\vdash \Gamma, \Delta}\,\text{cut}}{\longrightarrow}$$

$$\dfrac{\vdash \Gamma, A^{\perp}[\mu X.A^{\perp}[X]] \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A[S], S^{\perp} \quad \vdash S, S^{\perp}}\,\text{id}}{\vdash \nu X.A[X], S^{\perp}}\,\nu_{\text{inv}}}{\vdash A[\nu X.A[X]], A[S]^{\perp}}\,A[\cdot] \qquad \vdash A[S], S^{\perp}}{\vdash A[\nu X.A[X]], S^{\perp}}\,\text{cut}}{\vdash \Gamma, S^{\perp}}\,\text{cut} \qquad \vdash \Delta, S}{\vdash \Gamma, \Delta}\,\text{cut}$$

$\mu MALL$: la fonctorialité par l'exemple

$$\frac{\vdash X^{\perp}, Y}{\vdash A[X]^{\perp}, A[Y]}\, A[\cdot]$$

Ex : $A[X] = \mathbf{1} \oplus (X \otimes B \otimes X)$

$$\dfrac{\dfrac{}{\vdash \bot, \mathbf{1}}\,\mathrm{id}}{\vdash \bot, \mathbf{1} \oplus (Y \otimes B \otimes Y)}\,\oplus^{1} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash X^{\perp}, Y}\,\mathrm{id} \quad \dfrac{}{\vdash B^{\perp}, B}\,\mathrm{id} \quad \dfrac{}{\vdash X^{\perp}, Y}\,\mathrm{id}}{\vdash X^{\perp}, B^{\perp}, X^{\perp}, Y \otimes B \otimes Y}\,\otimes, \otimes}{\vdash X^{\perp} \parr B^{\perp} \parr X^{\perp}, Y \otimes B \otimes Y}\,\parr, \parr}{\vdash X^{\perp} \parr B^{\perp} \parr X^{\perp}, \mathbf{1} \oplus (Y \otimes B \otimes Y)}\,\oplus^{2}}{\vdash \bot \,\&\, (X^{\perp} \parr B^{\perp} \parr X^{\perp}), \mathbf{1} \oplus (Y \otimes B \otimes Y)}\,\parr$$

Deuxième école : $\mu MALL^\infty$

- les règles habituelles de MALL
- plus

$$\frac{\vdash \Gamma, A[\mu X.A[X]]}{\vdash \Gamma, \mu X.A[X]}\,\mu \qquad \frac{\vdash \Delta, A[\nu X.A[X]]}{\vdash \Delta, \nu X.A[X]}\,\nu$$

- et les arbres de preuves peuvent être *infinis* !

Avantage de $\mu MALL^\infty$: la réduction de tes rêves

$$\dfrac{\dfrac{\dfrac{\vdash \Gamma, A[\mu X.A[X]]}{\vdash \Gamma, \mu X.A[X]}\,\mu \qquad \dfrac{\vdash \Delta, A[\nu X.A[X]]}{\vdash \Delta, \nu X.A[X]}\,\nu}{\vdash \Gamma, \Delta}\,\mathsf{cut}}{} \longrightarrow \dfrac{\vdash \Gamma, A[\mu X.A[X]] \quad \vdash \Delta, A[\nu X.A[X]]}{\vdash \Gamma, \Delta}\,\mathsf{cut}$$

Inconvénient de $\mu MALL^\infty$: un nécessaire critère de correction

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}}{\vdash \mu X.X}\mu \quad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, \Gamma}}{\vdash \nu X.X, \Gamma}\nu}{\dfrac{\vdash \mu X.X}{\vdash \mu X.X}\mu \quad \dfrac{\vdash \nu X.X, \Gamma}{\vdash \nu X.X, \Gamma}\nu}\,\mathsf{cut}$$
$$\vdash \Gamma$$

Inconvénient de $\mu MALL^{\infty}$: un nécessaire critère de correction

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}}{\vdash \mu X.X}\mu \quad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, \Gamma}}{\vdash \nu X.X, \Gamma}\nu}{\vdash \Gamma}\mathsf{cut} \longrightarrow \dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}}{\vdash \mu X.X}\mu \quad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, \Gamma}}{\vdash \nu X.X, \Gamma}\nu}{\vdash \Gamma}\mathsf{cut}$$

Quel lien entre $\mu MALL$ et $\mu MALL^\infty$

- Une traduction $\mu MALL \to \mu MALL^\infty$
- qui consiste essentiellement en

$$\dfrac{\vdash \Gamma, S^\perp \quad \vdash S^\perp, A[S]}{\vdash \Gamma, \nu XA}\,\nu_{\text{inv}} \rightsquigarrow$$

$$\dfrac{\vdots}{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\vdash S^\perp, \nu XA}}{\vdash S^\perp, A[S] \quad \vdash A^\perp[S^\perp], A[\nu XA]}\,[A]}{\vdash S^\perp, A[\nu XA]}\,\text{cut}}{\vdash \Gamma, S^\perp \quad \vdash S^\perp, \nu XA}\,\nu}\,\text{cut}$$

$$\vdash \Gamma, \nu XA$$

Quel lien entre $\mu MALL$ et $\mu MALL^\infty$

$\mu MALL^\infty$	$\mu MALL$
$\sim$« les vraies choses »	une représentation d'un fragment de $\mu MALL^\infty$
arbres infinis	arbres finis
critère de fils global et non trivial	pas de critère spécial
réduction rêvée	réduction lourde

- $\mu MALL$ = des représentations finies mal adaptées à l'étude de l'opérationnalité, conçues à partir de considérations sémantiques
- concevons des représentations finies à partir de l'opérationnalité !

$\mu MALL^*$: la conception

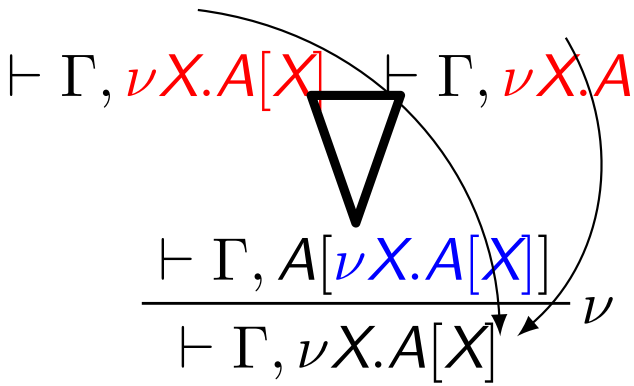
Parmis les fragments de $\mu MALL^\infty$ représentables finiment : les preuves circulaires :

- $=$ preuves ayant un nombre fini de sous-arbres
- représentables par des arbres finis avec des *back-edges*

$\mu MALL^{*}$: la conception

On prend un fragment des preuves circulaires en ajoutant deux contraintes sur les *back-edges* :

- la cible d'une *back-edge* doit être la conclusion d'une règle (ν)



- chaque occurrence $\nu X.A[X]$ doit être une des occurrences $\nu X.A[X]$

$\mu MALL^*$: exemples

$$\dfrac{\dfrac{\vdash \nu X.X}{\vdash \nu X.X}\,\nu \quad \dfrac{\vdash \nu X.X}{\vdash \nu X.X}\,\nu}{\vdash \nu X.X}\,\nu$$

deux représentations différentes de la même preuve infinie

$$\dfrac{\dfrac{\dfrac{\vdash \nu X.(\mathbf{1}\oplus X), \mathbf{1}\oplus \nu X.(\mathbf{1}\oplus X)}{\vdash \mathbf{1}\oplus \nu X.(\mathbf{1}\oplus X), \nu X.(\mathbf{1}\oplus X)}\,\text{exc}}{\vdash \mathbf{1}\oplus \nu X.(\mathbf{1}\oplus X), \mathbf{1}\oplus \nu X.(\mathbf{1}\oplus X)}\,\oplus^2}{\vdash \nu X.(\mathbf{1}\oplus X), \mathbf{1}\oplus \nu X.(\mathbf{1}\oplus X)}\,\nu$$

Nope ! Pas la bonne occurrence.

$$\dfrac{\dfrac{\vdash \nu X.X}{\vdash \nu X.X}\,\nu}{\vdash \nu X.X}\,\nu$$

Nope ! Trop de dépliages.

$\mu MALL^{*}$: la réduction de tes rêves... après dépliage

$$\dfrac{\dfrac{\vdash \Gamma, A[\mu X.A[X]]}{\vdash \Gamma, \mu X.A[X]}\,\mu \qquad \dfrac{\vdash \Delta, A[\nu X.A[X]]}{\vdash \Delta, \nu X.A[X]}\,\nu}{\vdash \Gamma, \Delta}\,\text{cut} \longrightarrow$$

$$\dfrac{\dfrac{\vdash \Gamma, A[\mu X.A[X]]}{\vdash \Gamma, \mu X.A[X]}\,\mu \qquad \dfrac{\dfrac{\vdash \Delta, A[\nu X.A[X]]}{\vdash \Delta, \nu X.A[X]}\,\nu}{\vdots}}{\vdash \Gamma, \Delta}\,\text{cut}$$

Conjectures

1. la traduction naturelle $\mu MALL^* \to \mu MALL^\infty$ est correcte pour le critère de fils
2. et elle factorise $\mu MALL \to \mu MALL^\infty$ en $\mu MALL \to \mu MALL^* \to \mu MALL^\infty$
3. il existe une traduction $\mu MALL^* \to \mu MALL$, ils ont donc la même expressivité

Bilan : $\mu MALL \leftrightarrow \mu MALL^*$

$\mu MALL^\infty$	$\mu MALL$	$\mu MALL^*$
$\sim$« les vraies choses »	une représentation d'un fragment de $\mu MALL^\infty$	une représentation d'un fragment de $\mu MALL^\infty$, de même expressivité que $\mu MALL$
arbres infinis	arbres finis	arbres finis avec *back-edges*
critère de fils global et non trivial	pas de critère spécial	critère d'occurences pour les *back-edges*, local à chaque boucle
réduction rêvée	réduction lourde	réduction simple, éventuels déroulages de boucles

Bilan : $\mu MALL^{*}$: preuves $\leftrightarrow$ programmes

$\mu MALL^{*}$	
une représentation d'un fragment de $\mu MALL^{\infty}$	une extension de système L ?
arbres finis avec *back-edges*	$\approx$ termes avec lieurs
critère d'occurences pour les *back-edges*, local à chaque boucle	$\approx$ appels récursifs restreints aux sous-termes immédiats
réduction simple, éventuels déroulages de boucles	$\approx Y\,(\lambda a.p) \to p\left[{}^{Y\,(\lambda a.p)}/_{a}\right]$

Bilan : travaux futurs

1. s'appuyer sur cette représentation pour concevoir un vrai langage de termes pour la correspondance preuves-programmes

Bilan : travaux futurs

1. s'appuyer sur cette représentation pour concevoir un vrai langage de termes pour la correspondance preuves-programmes
2. relacher la contrainte d'occurrences sur les *back-edges* pour autoriser plusieurs dépliages avant un appel récursif

Bilan : travaux futurs

1. s'appuyer sur cette représentation pour concevoir un vrai langage de termes pour la correspondance preuves-programmes
2. relacher la contrainte d'occurrences sur les *back-edges* pour autoriser plusieurs dépliages avant un appel récursif
3. se servir de ce langage pour explorer la correspondance entre logique temporelle et programmation fonctionnelles réactive dans le cas du temps discret ; en particulier concevoir une LTL classique constructive en ajoutant du controle de continuations dans FRP