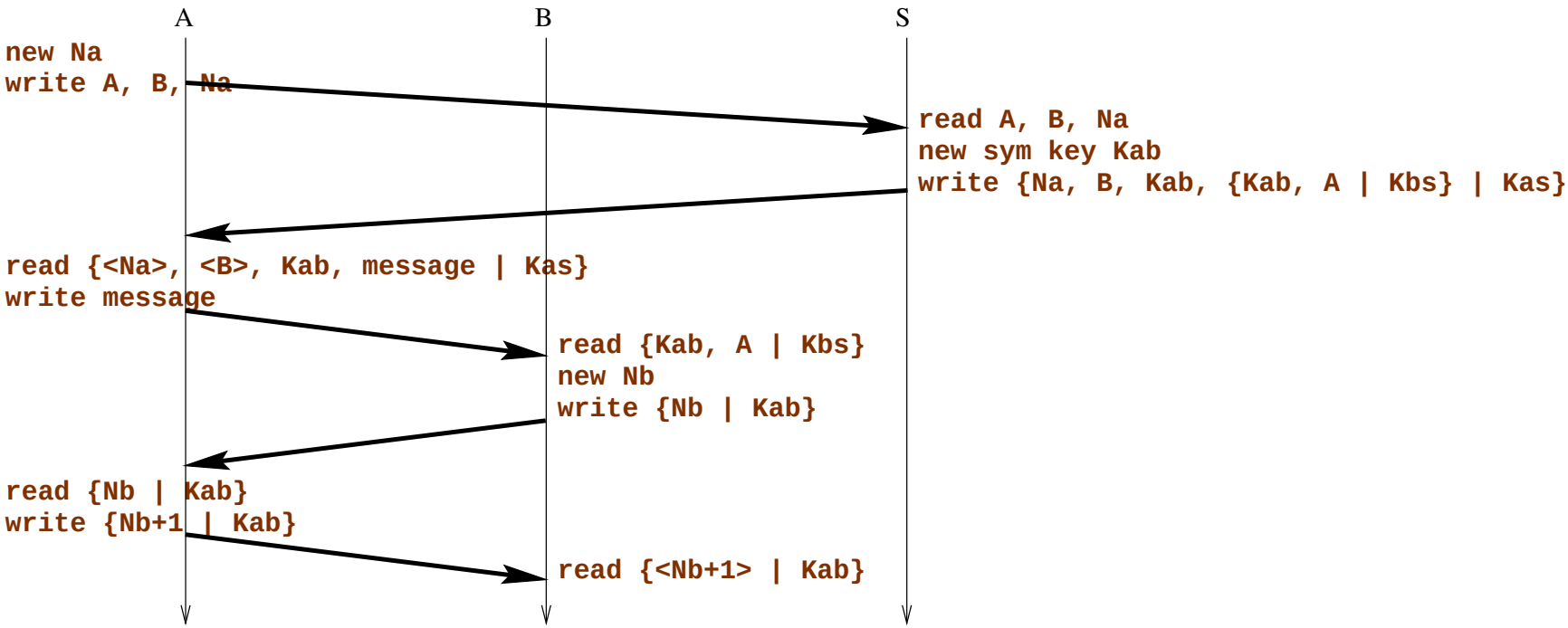
Relations logiques

pour types monadiques

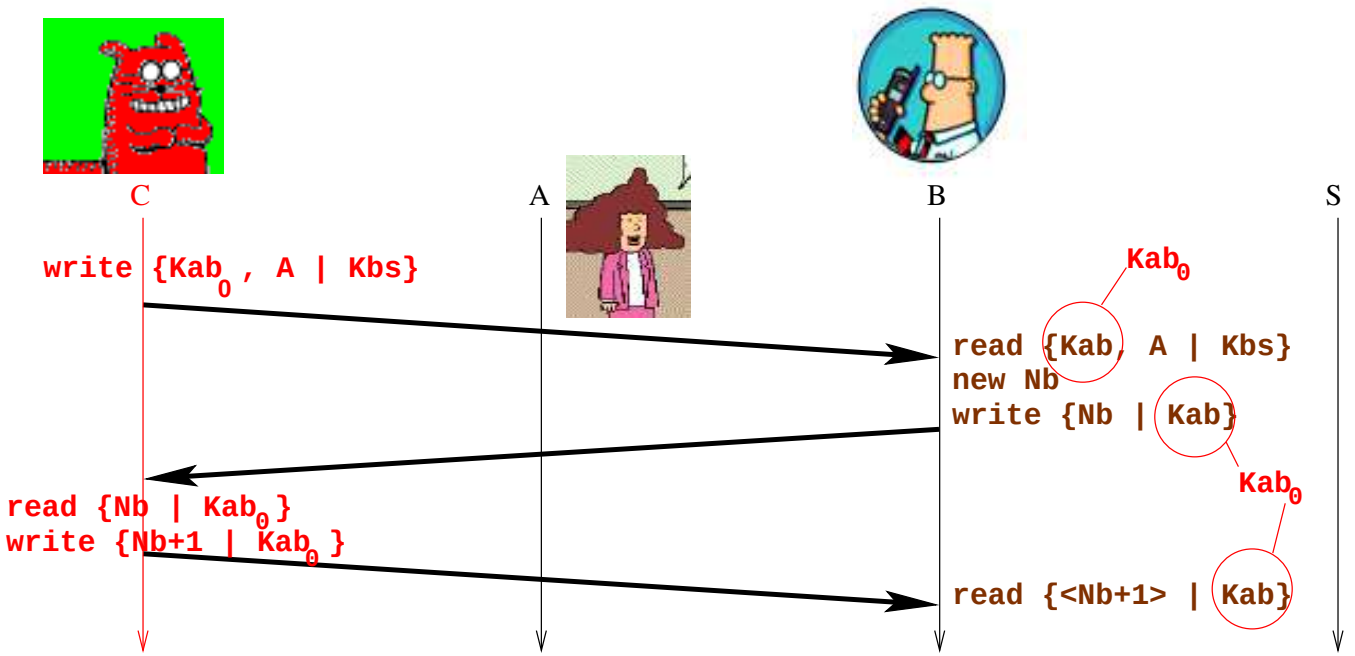
... et homologie?

Jean Goubault-Larrecq,
LSV/CNRS UMR 8643 & INRIA Futurs projet SECSI & ENS Cachan

Motivations (1): le protocole de Needham-Schroeder à clés privées



Motivations (2): ... une attaque



Le λ-calcul cryptographique [Sumii et Pierce, CSFW'2001]

Un langage de modélisation des protocoles cryptographiques:

e	$::=$	x	variables
	$\mid$	$e_1\, e_2$	application de la fonction e_1 à e_2
	$\mid$	$\lambda x \cdot e$	abstraction: fonction $x \mapsto e$
	$\mid$	$\pi_i e$	projection ($i = 1, 2$)
	$\mid$	$\langle e_1, e_2 \rangle$	paire
	$\mid$	$()$	rien (!)
	$\mid$	$(\nu x) e$	création de noms frais x
	$\mid$	$\{e_1\}_{e_2}$	chiffrement
	$\mid$	$\texttt{let}\ \{x\}_{e_2} = e_1\ \texttt{in}\ e_3\ \texttt{else}\ e_4$	déchiffrement
	$\mid$	$\ldots$	

... sert à programmer des protocoles cryptographiques

(avec quelques mensonges...)

$$
\begin{aligned}
A \quad := \quad & (\nu N_a)\texttt{send}\,(A, B, N_a); \\
& \texttt{read}\,(\lambda x \cdot \texttt{let}\,\{n, b, kab, m\}_{K_{as}} = x\,\texttt{in} \\
& \texttt{if}\; n = N_a \wedge b = B\;\texttt{then} \\
& \texttt{send}\,(m); \ldots)
\end{aligned}
$$

... sert surtout à vérifier des protocoles cryptographiques

Équivalence observationnelle:

$$e \cong e' \text{ ssi } \forall \mathcal{C}[] \cdot \mathcal{C}[e] \to^* \texttt{true} \Leftrightarrow \mathcal{C}[e'] \to^* \texttt{true}$$

Exemples [Pitts & Stark, MFCS'1993]:

$(\nu n)\lambda x \cdot (x = n) \cong \lambda x \cdot \texttt{false}$ $\qquad$ $(\nu n)(\nu n')\lambda f \cdot (fn = fn') \cong \lambda f \cdot \texttt{true}$

Typage

En fait, les termes sont typés:

$$\frac{}{\Gamma, x : \tau \vdash x : \tau}\ (Var) \qquad \frac{\Gamma, n : \mathtt{name} \vdash e : \tau}{\Gamma \vdash (\nu n)e : \tau}\ (New)$$

$$\frac{\Gamma, x : \tau \vdash e : \tau'}{\Gamma \vdash \lambda x \cdot e : \tau \to \tau'}\ (Abs) \qquad \frac{\Gamma \vdash e_1 : \tau \to \tau' \quad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1 e_2 : \tau'}\ (App)$$

et l'on demande que

$$\Gamma \vdash e \cong_\tau e'$$

Plan

Mon but (à terme): trouver des critères calculables d'équivalence observationnelle.

Idée: "il y a des monades alors il y a de l'homologie" (enfin, il devrait...)

- Relations logiques dans le λ-calcul (pas crypto);
- Relations logiques dans le λ-calcul monadique; (avec David Nowak et Slawek Lasota)
- Passage aux objects co-simpliciaux;
- Passage à la cohomologie.

Plan

- Relations logiques dans le λ-calcul (pas crypto);
- Relations logiques dans le λ-calcul monadique; (avec David Nowak et Slawek Lasota)
- Passage aux objects co-simpliciaux;
- Passage à la cohomologie.

Relations logiques pour le λ-calcul (pas crypto)

Une relation logique R est une famille de relations R_τ, une pour chaque type τ, telle que:

$$\begin{aligned} f\ R_{\tau\to\tau'}\ f' &\quad\Leftrightarrow\quad \forall a\ R_\tau\ a' \cdot f a\ R_{\tau'}\ f' a' \\ a\ R_{\tau\times\tau'}\ a' &\quad\Leftrightarrow\quad \pi_1 a\ R_\tau\ \pi_1 a' \wedge \pi_2 a\ R_{\tau'}\ \pi_2 a' \\ a\ R_1\ a' & \end{aligned}$$

Prop ("Basic Lemma") si $x_1 : \tau_1, \ldots, x_n : \tau_n \vdash e : \tau$,

et $a_1\ R_{\tau_1}\ a'_1, \ldots, a_n\ R_{\tau_n}\ a'_n$,

alors $e[x_1 := a_1, \ldots, x_n := a_n]\ R_\tau\ e[x_1 := a'_1, \ldots, x_n := a'_n]$.

Corollaire: si $a\ R_\tau\ a'$ alors $\vdash a \cong_\tau a'$.

Comment étendre ceci au cas des noms?

Avant de continuer, généralisons: la sémantique

On interprète les λ-termes typés dans une catégorie cartésienne close $\boldsymbol{C}$.

$\boldsymbol{C}[\![\tau]\!], \boldsymbol{C}[\![\Gamma]\!]$: objet $\quad$ $\boldsymbol{C}[\![\Gamma \vdash e : \tau]\!]$: morphisme $\boldsymbol{C}[\![\Gamma]\!] \to \boldsymbol{C}[\![\tau]\!]$

$$\boldsymbol{C}[\![\ldots, x_i : \tau_i, \ldots \vdash x_i : \tau_i]\!] \quad = \quad \ldots \times \boldsymbol{C}[\![\tau_i]\!] \times \ldots \xrightarrow{\pi_i} \boldsymbol{C}[\![\tau_i]\!]$$

$$\boldsymbol{C}[\![\Gamma \vdash e_1 e_2 : \tau']\!] \quad = \quad \boldsymbol{C}[\![\Gamma]\!] \xrightarrow[\boldsymbol{C}[\![e_2]\!]]{\boldsymbol{C}[\![e_1]\!]} \overbrace{\boldsymbol{C}[\![\tau \to \tau']\!]}^{\mathbf{hom}(\boldsymbol{C}[\![\tau]\!], \boldsymbol{C}[\![\tau']\!])} \times \boldsymbol{C}[\![\tau]\!] \xrightarrow{App} \boldsymbol{C}[\![\tau']\!]$$

$$\boldsymbol{C}[\![\Gamma \vdash \lambda x \cdot e : \tau \to \tau']\!] \quad = \quad \boldsymbol{C}[\![\Gamma]\!] \xrightarrow{\Lambda(\boldsymbol{C}[\![\Gamma, x:\tau \vdash e:\tau']\!])} \mathbf{hom}(\boldsymbol{C}[\![\tau]\!], \boldsymbol{C}[\![\tau']\!])$$

$$\left(\begin{array}{ll} \boldsymbol{C}[\![\Gamma, x : \tau]\!] & \xrightarrow{\boldsymbol{C}[\![e]\!]} \boldsymbol{C}[\![\tau']\!] \\ = \boldsymbol{C}[\![\Gamma]\!] \times \boldsymbol{C}[\![\tau]\!] & \end{array} \right)$$

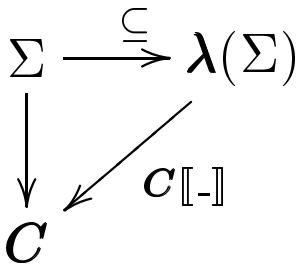
L'usage des CCC est bien une généralisation

Lemme Pour tout ensemble Σ (vu comme une catégorie), il existe une CCC libre $\boldsymbol{\lambda}(\Sigma)$ au-dessus de B:

$$\begin{aligned}
\text{Objets} \quad & = \text{types } \tau ::= \Sigma | \tau \to \tau | \tau \times \tau \\
\text{Morphismes} \quad & = \lambda\text{-termes modulo } \beta\eta\text{-équivalence } =_{\beta\eta} \\
& \tau_1 \times \ldots \times \tau_n \xrightarrow{e} \tau \\
& \text{où } x_1 : \tau_1, \ldots, x_n : \tau_n \vdash e : \tau, \\
& \text{mod } (\lambda x \cdot e) e' =_{\beta\eta} e[x := e'], \\
& \qquad \lambda x \cdot ex =_{\beta\eta} e \quad (x \text{ non libre dans } e)
\end{aligned}$$

La sémantique, en diagrammes

Pour toute CCC $\mathcal{C}$, la sémantique est entièrement décrite par le diagramme suivant dans $\mathcal{C}at$:



où $\mathcal{C}\,[\![_]\!]$ est donc une représentation de CCC.

Relations logiques, catégoriquement [Mitchell&Scedrov, CSL'1992]

Soit $\mathbb{C}$ une catégorie avec produits finis et pullbacks, (penser $\boldsymbol{Set}$)

$|_| : \boldsymbol{C} \to \mathbb{C}$ un foncteur préservant les produits. (penser $\boldsymbol{C}(1, _)$)

Le sous-scone $\boldsymbol{C} \downarrow \mathbb{C}$ est la catégorie: ($\sim$ comma-catégorie)

Objets = triplets $\langle S \in \mathbb{C}, m, A \in \boldsymbol{C} \rangle$,

où $S \overset{m}{\hookrightarrow} |A|$ (m mono) (penser sous-ensemble)

Morphismes = couples (u, v) de morphismes dans C

$\langle S, m, A \rangle \xrightarrow{(u,v)} \langle S', m', A' \rangle$ tels que

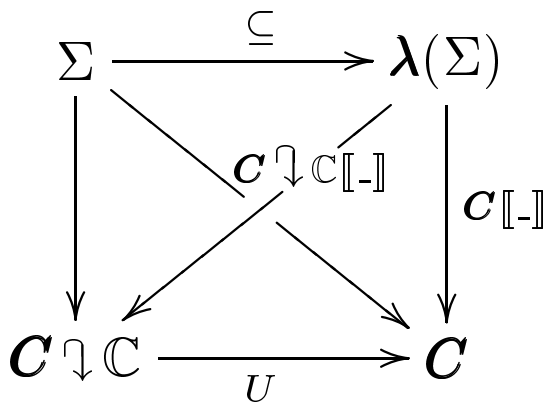
$$\begin{array}{ccc} S & \overset{m}{\hookrightarrow} & |A| \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle |v|} \\ S' & \overset{m'}{\hookrightarrow} & |A'| \end{array}$$

Trivial mais important: $U : \boldsymbol{C} \downarrow \mathbb{C} \to \boldsymbol{C}$ (oubli).

$$U\langle S, m, A \rangle = A \qquad U(u, v) = v$$

Le “Basic Lemma”, catégoriquement

Si on arrive à montrer que $\boldsymbol{C}\downarrow\mathbb{C}$ est une CCC, alors:



Exercice Vérifier que ça donne les relations logiques du début de cette présentation... $(\boldsymbol{C} = \mathbb{C} = \boldsymbol{\lambda}(\Sigma), |_| = \mathrm{id})$

La construction d'une structure de CCC sur $\mathcal{C}\downarrow\mathbb{C}$

On commence par le trivial:

- Objet terminal

$$\langle 1_{\mathbb{C}}, \mathrm{id}, 1_{\mathcal{C}}\rangle$$

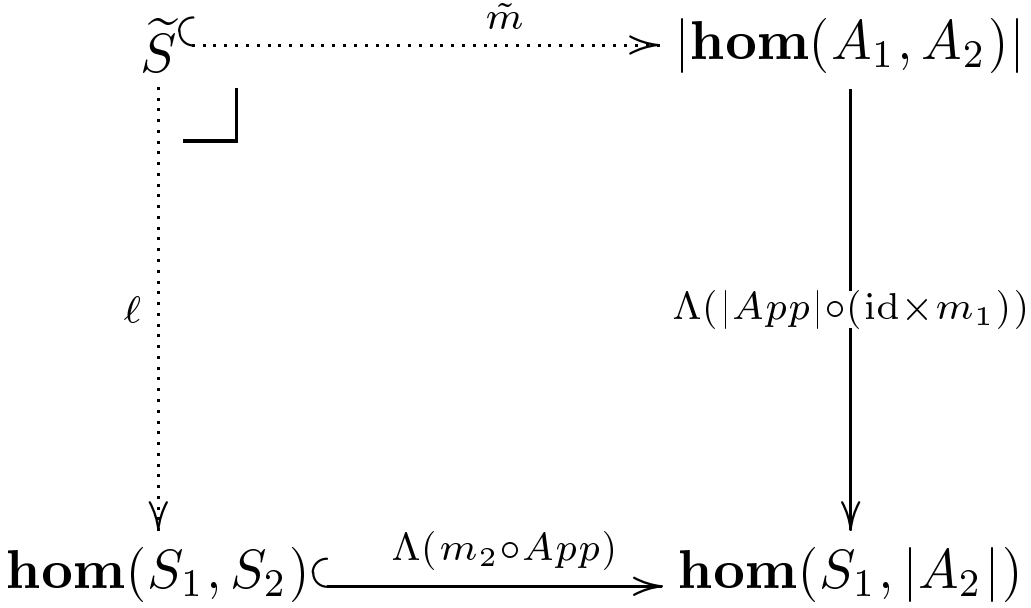
$$1_{\mathbb{C}} \hookrightarrow^{\mathrm{id}} |1_{\mathcal{C}}| = 1_{\mathbb{C}}$$

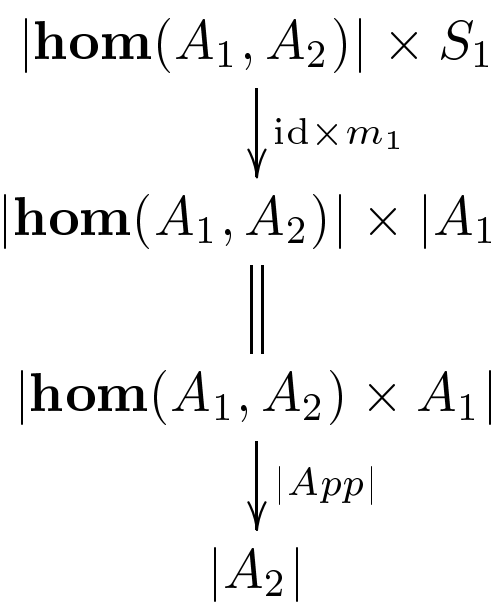
- Produit $\langle S_1, m_1, A_1\rangle \times \langle S_2, m_2, A_2\rangle = \langle S_1 \times S_2, m_1 \times m_2, A_1 \times A_2\rangle$

$$S_1 \times S_2 \hookrightarrow^{m_1 \times m_2} |A_1| \times |A_2| = |A_1 \times A_2|$$

- L'exponentielle se construit grâce aux pullbacks de $\mathbb{C}$...

$$\widetilde{S} \xhookrightarrow{\tilde{m}} |\mathbf{hom}(A_1, A_2)| \;=\; \mathbf{hom}\Big(S_1 \xhookrightarrow{m_1} |A_1| \;,\; S_2 \xhookrightarrow{m_2} |A_2| \Big)$$





$$\mathbf{hom}(S_1, S_2) \times S_1 \xrightarrow{App} S_2 \xrightarrow{m_2} |A_2|$$

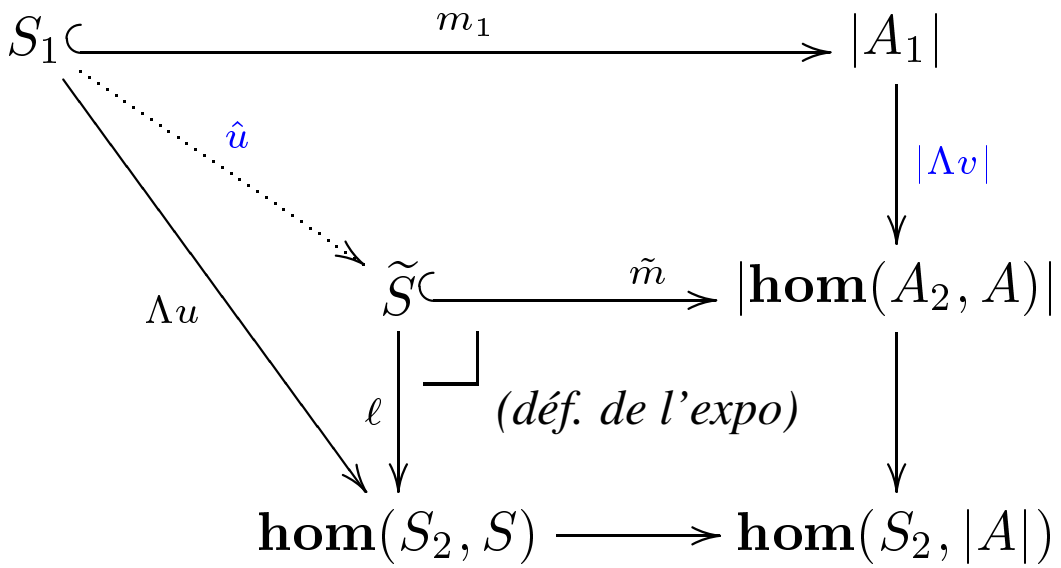
Application

$$\mathbf{hom}(\ S_1 \overset{m_1}{\hookrightarrow} |A_1|\ ,\ S_2 \overset{m_2}{\hookrightarrow} |A_2|\ ) \times (\ S_1 \overset{m_1}{\hookrightarrow} |A_1|\ )$$

$$\begin{array}{ccccc}
\widetilde{S} \times S_1 & \xrightarrow{\tilde{m}\times \mathrm{id}} & |\mathbf{hom}(A_1, A_2)| \times S_1 & \xrightarrow{\mathrm{id}\times m_1} & |\mathbf{hom}(A_1, A_2)| \times |A_1 \\
\downarrow{\scriptstyle \ell\times \mathrm{id}} & \textit{(déf. de l'expo)} & \downarrow & & \| \\
\mathbf{hom}(S_1, S_2) \times S_1 & \longrightarrow & \mathbf{hom}(S_1, |A_2|) \times S_1 & \textit{(calcul)} & \| \\
\downarrow{\scriptstyle App} & \textit{(calcul)} & \downarrow{\scriptstyle App} & & \| \\
S_2 & \underset{m_2}{\hookrightarrow} & |A_2| & \xleftarrow{|App|} & |\mathbf{hom}(A_1, A_2) \times A_1|
\end{array}$$

Abstraction ($\Lambda(\ldots)$)

Soit $\langle S_1, m_1, A_1\rangle \times \langle S_2, m_2, A_2\rangle \xrightarrow{\quad (u,v) \quad} \langle S, m, A\rangle$,
on définit $\Lambda(u, v) = (\hat{u}, \Lambda v)$ tel que:



Voilà, le sous-scone est une CCC!

Plan

- Relations logiques dans le λ-calcul (pas crypto);
- Relations logiques dans le λ-calcul monadique; (avec David Nowak et Slawek Lasota)
- Passage aux objects co-simpliciaux;
- Passage à la cohomologie.

Le λ-calcul monadique, syntaxiquement

Un nouveau type: $\tau ::= \Sigma | \tau \to \tau | \boldsymbol{T}\tau$.

$$\frac{}{\Gamma, x : \tau \vdash x : \tau}\ (Var)$$

$$\frac{\Gamma, x : \tau \vdash e : \tau'}{\Gamma \vdash \lambda x \cdot e : \tau \to \tau'}\ (Abs) \qquad \frac{\Gamma \vdash e_1 : \tau \to \tau' \quad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1 e_2 : \tau'}\ (App)$$

$$\frac{\Gamma \vdash u : \tau}{\Gamma \vdash \mathtt{val}\, u : \boldsymbol{T}\tau}\ (\boldsymbol{T}I) \qquad \frac{\Gamma \vdash u : \boldsymbol{T}\tau \quad \Gamma, x : \tau \vdash v : \boldsymbol{T}\tau'}{\Gamma \vdash \mathtt{let\ val}\, x = u\, \mathtt{in}\, v : \boldsymbol{T}\tau'}\ (\boldsymbol{T}E)$$

La création de noms, en λ-calcul monadique

Idée: étant donné A, $\boldsymbol{T}A \sim \{(\nu n_1, ..., n_k)v | n_1, ..., n_k : \texttt{name}, v \in A\}$.

On se donne une constante $\texttt{new} : \boldsymbol{T}\texttt{name}$ $\sim (\nu n)n$

Alors:

$$(\nu n)e \quad \sim \quad \texttt{let val}\ n = \texttt{new in}\ e$$

Sémantique

On se donne maintenant une CCC $\boldsymbol{C}$ avec une monade forte $(\boldsymbol{T}, \boldsymbol{\eta}, \boldsymbol{\mu}, \boldsymbol{t})$ (une let-catégorie).

$$\boldsymbol{C}[\![\boldsymbol{T}\tau]\!] = \boldsymbol{T}\boldsymbol{C}[\![\tau]\!]$$

$$\boldsymbol{C}[\![\Gamma \vdash \mathtt{val}\, e : \boldsymbol{T}\tau]\!] \quad = \quad \boldsymbol{C}[\![\Gamma]\!] \xrightarrow{\boldsymbol{C}[\![e]\!]} \boldsymbol{C}[\![\tau]\!] \xrightarrow{\boldsymbol{\eta}} \boldsymbol{T}\boldsymbol{C}[\![\tau]\!]$$

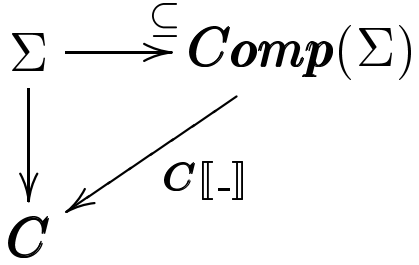
$$\boldsymbol{C}[\![\Gamma \vdash \mathtt{let\ val}\, x = e\ \mathtt{in}\, e' : \boldsymbol{T}\tau']\!] \quad = \quad \boldsymbol{C}[\![\Gamma]\!] \xrightarrow{\langle \mathrm{id},\, \boldsymbol{C}[\![e]\!] \rangle} \boldsymbol{C}[\![\Gamma]\!] \times \boldsymbol{T}\boldsymbol{C}[\![\tau]\!] \xrightarrow{\boldsymbol{t}} \boldsymbol{T}(\boldsymbol{C}[\![\Gamma]\!] \times \boldsymbol{C}[\![\tau]\!]) \xrightarrow{\boldsymbol{T}\boldsymbol{C}[\![e']\!]} \boldsymbol{T}^2\boldsymbol{C}[\![\tau']\!] \xrightarrow{\boldsymbol{\mu}} \boldsymbol{T}\boldsymbol{C}[\![\tau']\!]$$

La sémantique, catégoriquement

Prop Le λ-calcul monadique typé forme la let-catégorie libre $\boldsymbol{Comp}(\Sigma)$.

$$\begin{aligned}
\boldsymbol{\eta}_\tau &= x : \tau \vdash \mathtt{val}\, x : \boldsymbol{T}\tau \\
\boldsymbol{\mu}_\tau &= x : \boldsymbol{T}^2\tau \vdash \mathtt{let\,val}\, y = x\, \mathtt{in}\, y : \boldsymbol{T}\tau \\
\boldsymbol{t}_{\tau,\tau'} &= x : \tau, y : \boldsymbol{T}\tau' \vdash \mathtt{let\,val}\, z = y\, \mathtt{in}\, \langle x, z\rangle : \boldsymbol{T}\tau \times \tau'
\end{aligned}$$

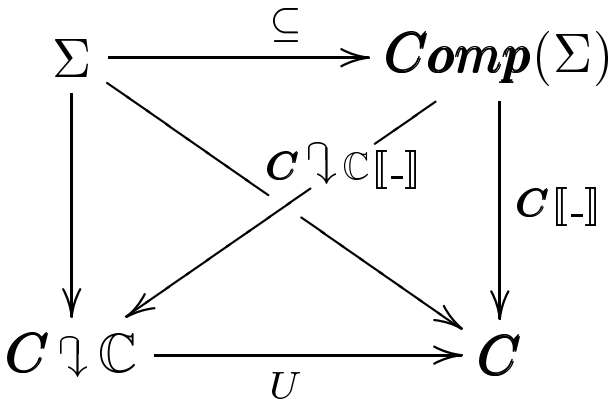
Pour toute let-catégorie $\boldsymbol{C}$, sémantique=:



où $\boldsymbol{C}\,[\![_]\!]$ est donc une représentation de let-catégorie.

Comment fabriquer des relations logiques avec des monades

Si on arrive à montrer que $\boldsymbol{C} \downarrow \mathbb{C}$ est une let-catégorie, alors:



où $\boldsymbol{C} \downarrow \mathbb{C}\,[\![_]\!]$ et $\boldsymbol{C}\,[\![_]\!]$ sont des représentations de let-catégories...
Il n'y a plus qu'à trouver une structure de monade forte sur $\boldsymbol{C} \downarrow \mathbb{C}\,[\![_]\!]$.

Pour ça, on suppose qu'on a déjà une monade forte (T, η, μ, t) sur $\mathbb{C}$

+ 7 (!) autres hypothèses...

Les ingrédients nécessaires (dans $\mathbb{C}$): 1. factorisation mono

Un système de factorisation mono est la donnée de deux classes de morphismes de $\mathbb{C}$,
celle des pseudoepis $\twoheadrightarrow$, celle monos pertinents $\hookrightarrow$.

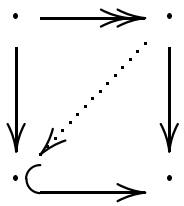
(a) tout mono pertinent est mono;

(on demande aussi que les monos pertinents soient préservés par pullbacks)

(b) tout iso est à la fois $\twoheadrightarrow$ et $\hookrightarrow$;

(c) les deux classes sont stables par composition avec les isos;

(d) Propriété de relèvement:

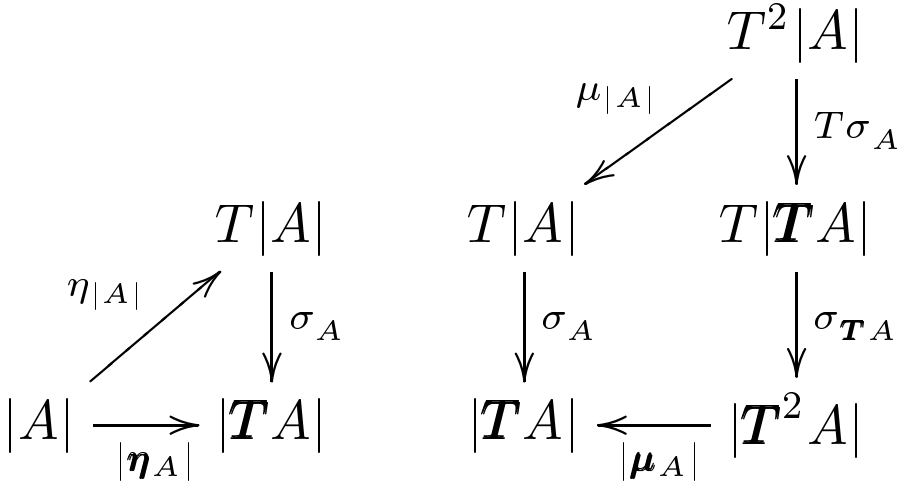


Les ingrédients nécessaires (dans $\mathbb{C}$): 2. distributivité

Il nous faut une transformation naturelle

$$\sigma : T|_| \Rightarrow |\boldsymbol{T}|$$

telle que



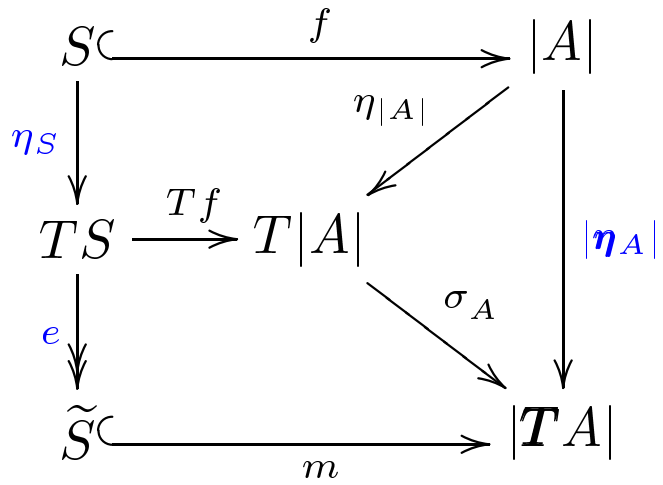
... autrement dit, un morphisme de monades.

Construction de $\widetilde{T}$

$$\widetilde{T}\big(\ S \overset{m}{\hookrightarrow} |A|\ \big) \quad = \quad \begin{array}{ccc} TS & \xrightarrow{Tm} & T|A| \\ {\scriptstyle e}\downarrow & & \downarrow{\scriptstyle \sigma_A} \\ \widetilde{S} & \underset{m}{\hookrightarrow} & |\boldsymbol{T}A| \end{array}$$

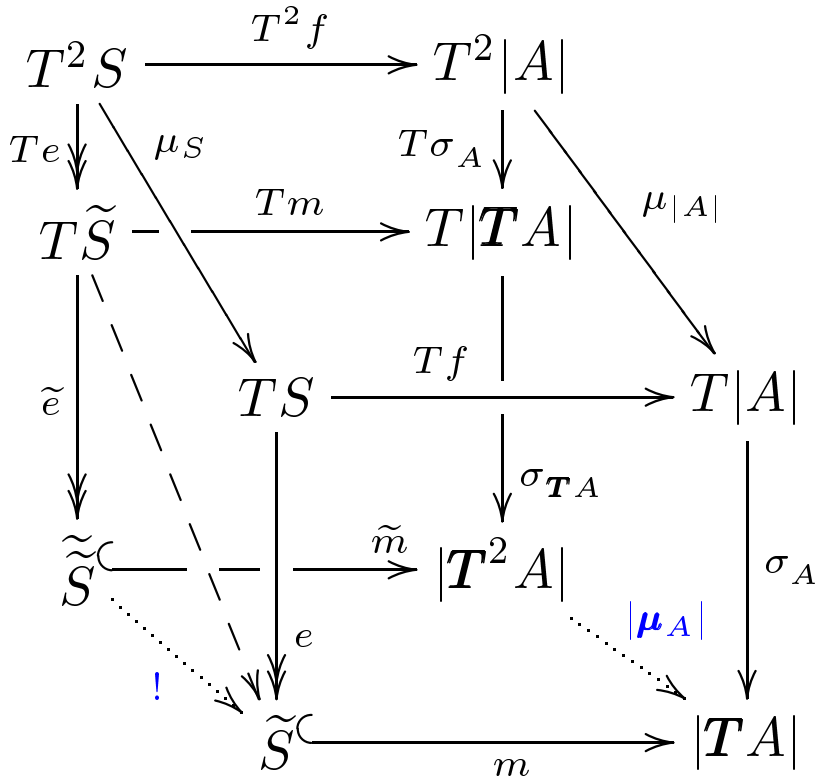
$$\widetilde{T}\left(\begin{array}{ccccc} S & \overset{m}{\hookrightarrow} & |A| & & \\ & {\scriptstyle u}\searrow & & \searrow{\scriptstyle |v|} & \\ & & S' & \underset{m'}{\hookrightarrow} & |A'| \end{array} \right) \quad = \quad \begin{array}{ccccc} TS & & \xrightarrow{Tm} & & T|A| \\ & \searrow^{Tu} & & & \downarrow{\scriptstyle |\boldsymbol{T}v|} \\ {\scriptstyle e}\downarrow & & TS' & \xrightarrow{Tm'} & T|A'| \\ & & \downarrow{\scriptstyle \sigma_A} & & \\ \widetilde{S} & \overset{m}{\hookrightarrow} & |\boldsymbol{T}A| & & \downarrow{\scriptstyle \sigma_{A'}} \\ & \searrow^{\hat{u}} & {\scriptstyle e'}\downarrow & \searrow{\scriptstyle |\boldsymbol{T}v|} & \\ & & \widetilde{S}' & \underset{m'}{\hookrightarrow} & |\boldsymbol{T}A'| \end{array}$$

Construction de l'unité $\widetilde{\eta}_{S \overset{f}{\hookrightarrow} |A|}$



Construction de la multiplication $\widetilde{\mu}$

$S \overset{f}{\hookrightarrow} |A|$



à condition que T préserve les pseudoepis (on peut demander un peu moins...)

Construction de la force

... je vous l'épargne!

La morale: tout se fait naturellement.

Mais qu'est-ce que ça donne en vrai?

Le cas de la création de noms, dans $\mathbb{C} = \boldsymbol{Set}^{\mathcal{I}}$ [Moggi]

- $\mathcal{I}$: objets=ensembles finis [de noms], morphismes=injections;
- $\boldsymbol{T}A = \mathrm{colim}_{s'}\, A(_ + s') : \mathcal{I} \to \boldsymbol{Set}$;

  ... les éléments de $\boldsymbol{T}As$ sont des "$(\nu s')a$", où:
  - s' est un ensemble de noms;
  - tous les noms de s' sont *liés* dans a;
  - tout nom utilisé par a est dans $s + s'$;
  - $(\nu s', s'')a \equiv (\nu s')a$ si aucun des nouveaux noms de s'' n'est utilisé par a.
- $\boldsymbol{\eta}_A s : As \to \boldsymbol{T}As$ est défini par: $\boldsymbol{\eta}_A sa = (\emptyset, a)$; "$(\nu\emptyset)a$"
- $\boldsymbol{\mu}_A s : \boldsymbol{T}^2 As \to \boldsymbol{T}As$ est défini par $\boldsymbol{\mu}_A s(s', (s'', a)) = (s' + s'', a)$;

  "$(\nu s')(\nu s'')a \mapsto (\nu s', s'')a$"

La relation logique obtenue

$$(\nu s_1)a_1 \ \widetilde{S}s \ (\nu s_2)a_2 \quad \Longleftrightarrow \quad \exists s_0 \in \mathcal{I} \cdot \exists i_1 : s_1 \to s_0 \in \mathcal{I} \cdot \exists i_2 : s_2 \to s_0 \in \mathcal{I} \cdot$$
$$a_1[s_1 := i_1(s_1)] \ S(s + s_0) \ a_2[s_2 := i_2(s_2)]$$

- ressemble au traitement des noms en bisimulation cadrée [Abadi & Gordon, NJC'1998]
- ressemble aux relations logiques de [Pitts & Stark, MFCS'1993]
- est en fait moins précise [Zhang 2002]
  ... il faut passer à $\boldsymbol{Set}^{\mathcal{I},\mathcal{I}}$ [Nowak 2003],
  ... mais c'est déjà assez compliqué pour cet exposé, non?

Autres applications

- Monade $\mathbb{P}$ dans $\boldsymbol{Set}$: $A \to \boldsymbol{T}A$ est le type des systèmes de transitions,

  ... on retrouve les bisimulations fortes.

- Monade de l'espace des mesures dans $\boldsymbol{C} = \boldsymbol{Mes}$, $\mathbb{C} = \boldsymbol{Set}$: $A \to \boldsymbol{T}A$ est le type des chaînes de Markov,

  ... on retrouve les bisimulations probabilistes [Larsen & Skou, I&C'1991]

  ... en fait, ça marche mieux avec l'espace des valuations continues dans $\boldsymbol{C} = \mathbb{C} = \boldsymbol{Cpo}$.

Plan

- Relations logiques dans le λ-calcul (pas crypto);
- Relations logiques dans le λ-calcul monadique; (avec David Nowak et Slawek Lasota)
- Passage aux objects co-simpliciaux;
- Passage à la cohomologie.

Que peut-on faire ici?

La question à résoudre est:

Étant donnés deux termes e, e' de type τ, existe-t-il une relation logique R telle que $e\ R_\tau\ e'$?

Je fais le pari que c'est indécidable, ou trop compliqué en pratique.
Je souhaite donc trouver un critère d'existence [ou de non-existence] de telles relations logiques.
Comme on a des monades, la (co)homologie de Barr-Beck semble une voie toute tracée, non?

Une fausse piste (pour les noms)

Dans $\boldsymbol{Set}^{\mathcal{I}}$, on a déjà une structure co-semi-simpliciale.

En vrai, $\boldsymbol{Set}^{\mathcal{I}} \cong \boldsymbol{Set}^{\Delta^-}$, où Δ^- est la catégorie semi-simpliciale (on a juste les faces).

Ça suffit pour définir un complexe de cochaînes (donc une cohomologie):

- $C_n[\tau] = \mathbb{Z}\boldsymbol{Set}\,[\![\tau]\!]\,([n])$,
- $d : C_n[\tau] \to C_{n+1}[\tau], x \mapsto \sum_{i=0}^{n+1} (-1)^i \partial^i x$.

Mais tout se dégrade très vite:

- On n'a pas Eilenberg-Zilber, donc pas Künneth non plus.

  (Hum, on a peut-être Künneth... merci à l'assistance de me l'avoir signalé...)

- Une homotopie (co)simpliciale ne fournit pas en général d'homotopie de chaînes dans $C_\bullet$ (!)

Prenons la monade au sérieux...

Plongement $(_)^*$ de $\mathbb{C}$ dans $\mathbb{C}^\Delta$, via la monade [Barr & Beck, STCHT'1969]:

- $A^* = (T^{n+1}A)_{n\geq -1}$;
- $\partial^i : A^*_n \to A^*_{n+1} = T^i\eta_{T^{n+1-i}A}$, $\quad s^i : A^*_{n+1} \to A^*_n = T^i\mu_{T^{n-i}A}$.

Si $\mathbb{C} = \boldsymbol{Set}$ce que vous voulez, $\mathbb{C}^\Delta$ est une CCC avec pullbacks, il y a une factorisation epi-mono, il y a même une monade forte:

- $T^*K = K[-1]$ (co-décalage, $K[-1]_n = K_{n-1}$)
  Note: $T^*A^* = (TA)^*$;
- ${\eta_K}^* = \partial^0$, ${\mu_K}^* = s^0$.

On peut (a priori) refaire le sous-scone dans $\mathbb{C}^\Delta$ au lieu de $\mathbb{C}$ (c'est même plus précis!), en composant $|_|^* = (_)^* \circ |_|$, mais...

Problème: $(_)^*$ ne préserve pas les produits finis!

... parce que T ne préserve pas en général les produits finis.

Si $T = \mathbb{P}$, ça voudrait dire $\mathbb{P}(A \times B) = \mathbb{P}A \times \mathbb{P}B$.

Dans le cas de la monade des noms, ça reviendrait à mettre en bijection

$$\text{les } (\nu s)(a, b) \equiv (\nu s, s')(a, b) \ (s' \text{ non utilisé ni par } a \text{ ni par } b)$$

et

$$\text{les } (\nu s)a, (\nu s)b \equiv (\nu s, s')a, (\nu s, s'')b \ (s' \text{ non utilisé par } a \text{ mais peut-être par } b, \text{ et symétriquement})$$

Catégoriquement, $(_)^*$ préserverait $\times$ si $\mathcal{I}$ était une catégorie filtrante (conjecture), mais ce n'est pas le cas...

On s'en sort quand même!

On refait toute la construction du sous-scone en supposant seulement que $|_|^*$ est monoïdal:

$$|A_1|^* \times |A_2|^* \xrightarrow{\theta_{A_1,A_2}} |A_1 \times A_2|^*$$
$$1 \xrightarrow{\iota} |1|^*$$

avec θ naturel + conditions de cohérence.

Nécessite en plus une factorisation mono dans $\mathbb{C}^\Delta$ . . mais on en a déjà une!

Parenthèse: $(_)^*$ est monoïdal dans $\mathbb{C}^\Delta$

... car T est une monade forte.

$$\begin{array}{ccc} TA_1 \times TA_2 & \xrightarrow{t} & T(TA_1 \times A_2) \\ & & \downarrow{\scriptstyle T(\leftrightharpoons)} \\ T^2(A_2 \times A_1) & \xleftarrow[Tt]{} & T(A_2 \times TA_1) \\ \downarrow{\scriptstyle T^2(\leftrightharpoons)} & & \\ T^2(A_1 \times A_2) & \xrightarrow[\mu]{} & T(A_1 \times A_2) \end{array}$$

On en déduit que T est monoïdal dans $\mathbb{C}$, donc $(_)^*$ monoïdal dans $\mathbb{C}^\Delta$, donc aussi $|_|^*$.

La construction d'une structure de CCC sur $\mathcal{C}\downarrow\mathbb{C}^{\Delta}$

On commence par le [un peu moins] trivial:

- Objet terminal

$$\langle 1_{\mathbb{C}}, \iota, 1_{\mathcal{C}}\rangle$$

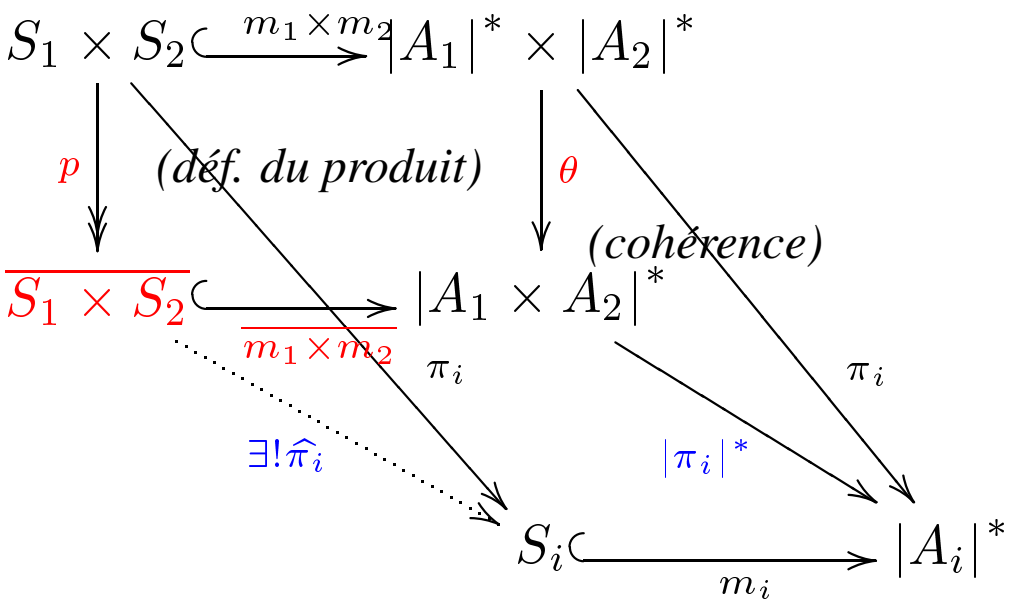
$$1_{\mathbb{C}} \overset{\iota}{\hookrightarrow} |1_{\mathcal{C}}|^*$$

- Produit $\langle S_1, m_1, A_1\rangle \times \langle S_2, m_2, A_2\rangle = \langle \overline{S_1 \times S_2}, \overline{m_1 \times m_2}, A_1 \times A_2\rangle$

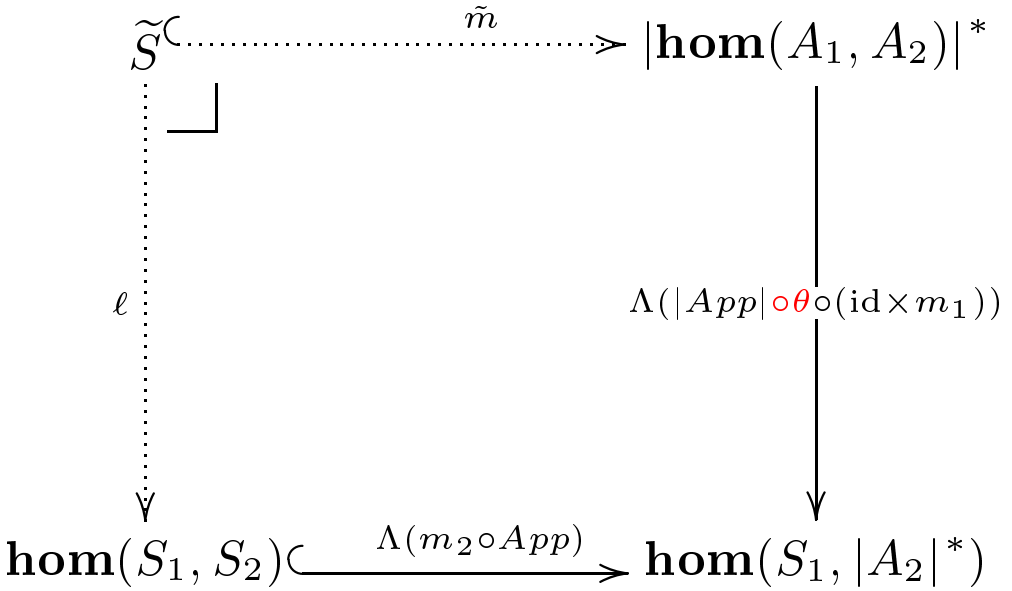
$$\begin{array}{ccc} S_1 \times S_2 & \overset{m_1\times m_2}{\hookrightarrow} & |A_1|^* \times |A_2|^* \\ \downarrow p & & \downarrow \theta \\ \overline{S_1 \times S_2} & \underset{\overline{m_1\times m_2}}{\hookrightarrow} & |A_1 \times A_2|^* \end{array}$$

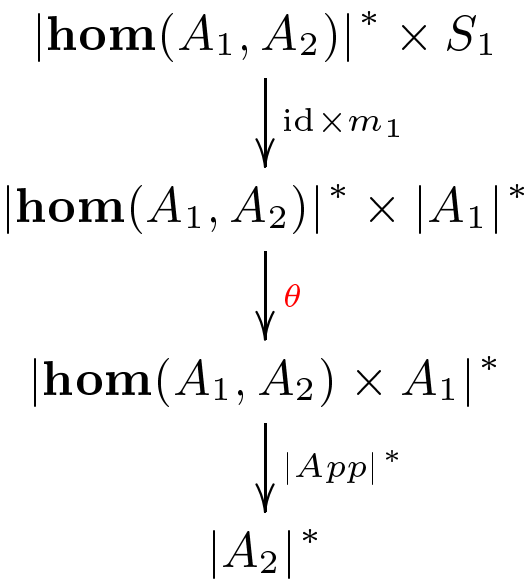
- Les projections se construisent par relèvement (transparent suivant);
- L'exponentielle se construit grâce aux pullbacks de $\mathbb{C}$... (à suivre)

Projections, par relèvement



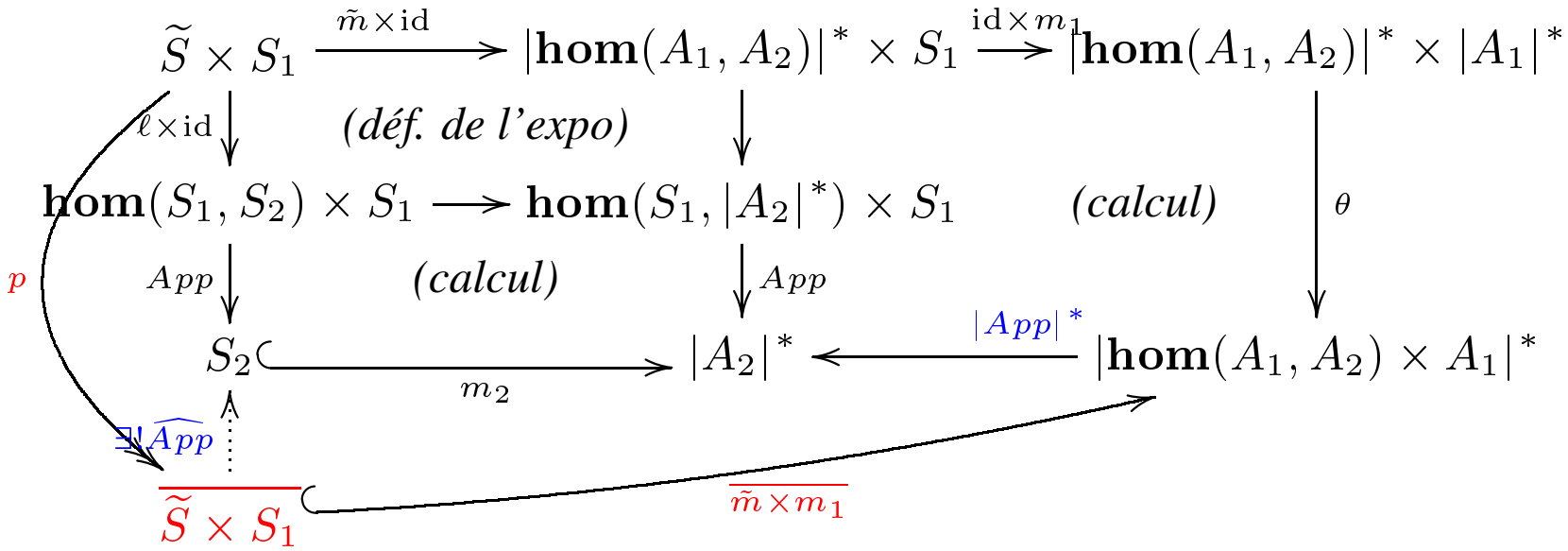
$$\widetilde{S} \overset{\tilde{m}}{\hookrightarrow} |\mathbf{hom}(A_1, A_2)|^* = \mathbf{hom}(\, S_1 \overset{m_1}{\hookrightarrow} |A_1|^* \,,\; S_2 \overset{m_2}{\hookrightarrow} |A_2|^* \,)$$





$$\mathbf{hom}(S_1, S_2) \times S_1 \overset{App}{\longrightarrow} S_2 \overset{m_2}{\longrightarrow} |A_2|^*$$

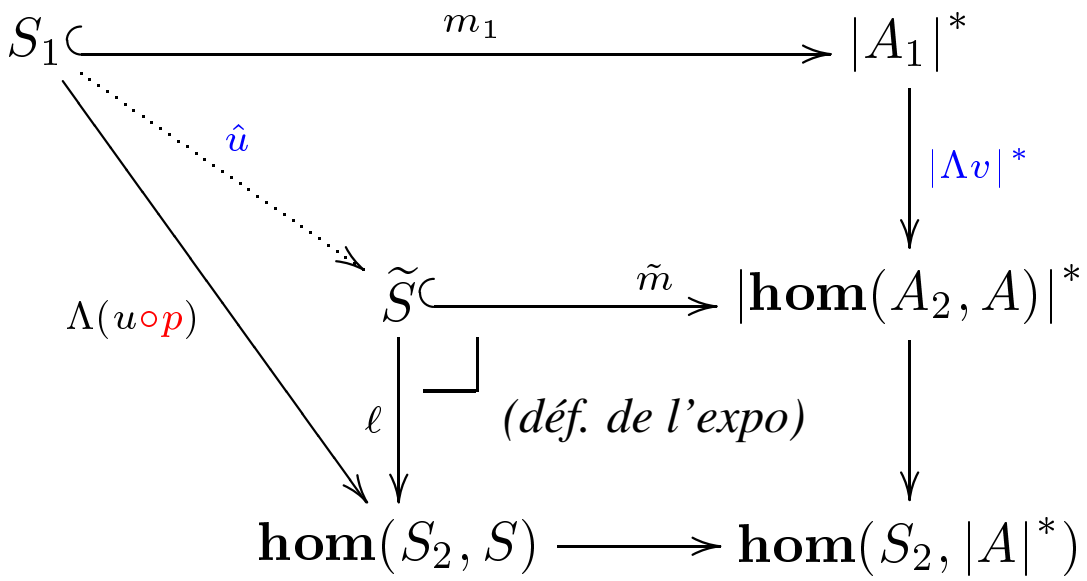
Application



$$\mathbf{hom}(\ S_1 \overset{m_1}{\hookrightarrow} |A_1|^*\ ,\ S_2 \overset{m_2}{\hookrightarrow} |A_2|^*\ ) \times (\ S_1 \overset{m_1}{\hookrightarrow} |A_1|^*\ )$$

Abstraction ($\Lambda(\ldots)$)

Soit $\langle S_1, m_1, A_1\rangle \times \langle S_2, m_2, A_2\rangle \xrightarrow{(u,v)} \langle S, m, A\rangle$,
on définit $\Lambda(u, v) = (\hat{u}, \Lambda v)$ tel que:



Voilà, le sous-scone est une CCC, et pourtant $|_|^*$ ne préserve pas les produits. (Pour les monades, aucune modification.)

Résumé

On a fabriqué un sous-scone $\boldsymbol{C} \downarrow \mathbb{C}^{\Delta}$, qui fournit une relation logique de Kripke du λ-calcul monadique.

Fonctionne pour toute monade forte.

Nécessite juste que $\mathbb{C}^{\Delta}$ soit une CCC avec pullbacks:

- pas vrai en général;
- OK si $\mathbb{C} = \boldsymbol{Set}^{\mathcal{I}}$ (car $\mathbb{C}^{\Delta} \cong \boldsymbol{Set}^{\mathcal{I} \times \Delta}$ topos élémentaire).

Plan

- Relations logiques dans le λ-calcul (pas crypto);
- Relations logiques dans le λ-calcul monadique; (avec David Nowak et Slawek Lasota)
- Passage aux objects co-simpliciaux;
- Passage à la cohomologie. (beaucoup plus prospectif!)

Note: les transparents suivants sont complètement remaniés comparés à ma présentation du 14 février 2003.

Rappel: complexes de cochaînes (bornés par le bas)

Soit $\mathcal{A}$ une catégorie abélienne. (par ex., groupes abéliens $\boldsymbol{Ab}$)

Un complexe de cochaînes dans $\mathcal{A}$ est une suite d'objets C_n de $\mathcal{A}$

$$\cdots \longrightarrow 0 \longrightarrow \cdots \longrightarrow 0 \longrightarrow C_{-k} \xrightarrow{d_{-k+1}} C_{-k+1} \xrightarrow{d_{-k}} \cdots \xrightarrow{d_n} C_n \xrightarrow{d_{n+1}} \cdots$$

tels que $d_{n+1} \circ d_n = \mathbf{0}$. (en abrégé, $d^2 = \mathbf{0}$)

La catégorie $\boldsymbol{CoCh}(\mathcal{A})$ des complexes de cochaînes a comme morphismes les $(f_n)_{n\in\mathbb{Z}}$ qui font commuter:

$$\begin{array}{ccccccccccccc}
\cdots & \longrightarrow & 0 & \longrightarrow & \cdots & \longrightarrow & 0 & \longrightarrow & C_{-k} & \xrightarrow{d_{-k+1}} & C_{-k+1} & \xrightarrow{d_{-k}} & \cdots \xrightarrow{d_n} C_n \xrightarrow{d_{n+1}} \cdots \\
 & & \downarrow & & & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\cdots & \longrightarrow & 0 & \longrightarrow & \cdots & \longrightarrow & 0 & \longrightarrow & C'_{-k} & \xrightarrow{d_{-k+1}} & C'_{-k+1} & \xrightarrow{d_{-k}} & \cdots \xrightarrow{d_n} C'_n \xrightarrow{d_{n+1}} \cdots
\end{array}$$

f_{-k-1} f_{-k} f_{-k+1} f_n

Note: $\boldsymbol{CoCh}(\mathcal{A})$ est de nouveau une catégorie abélienne.

Rappel: objets cosimpliciaux et complexes de cochaînes (Barr-Beck)

La catégorie des objets cosimpliciaux de $\mathcal{C}$ est $\mathcal{C}^{\Delta}$.

Tout foncteur $E : \mathcal{C} \to \mathcal{A}$ induit un foncteur $C(\bullet, E) : \mathcal{C}^{\Delta} \to \boldsymbol{CoCh}(\mathcal{A})$:

- $C(K, E) =$

$$\cdots \longrightarrow 0 \longrightarrow \cdots \longrightarrow E(K_{-1}) \xrightarrow{d_0} E(K_0) \xrightarrow{d_1} \cdots \xrightarrow{d_n} E(K_n) \xrightarrow{d_{n+1}} \cdots$$

$d_n : E(K_{n-1}) \to E(K_n) = \sum_{i=0}^{n} (-1)^i E(\partial_n^i)$

- si $f : K \to L$, $C(f, E)$ est:

$$\begin{array}{ccccccccccccc}
\cdots & \longrightarrow & 0 & \longrightarrow & \cdots & \longrightarrow & E(K_{-1}) & \xrightarrow{d_0} & E(K_0) & \xrightarrow{d_1} & \cdots & \xrightarrow{d_n} & E(K_n) & \xrightarrow{d_{n+1}} & \cdots \\
 & & \downarrow{\scriptstyle 0} & & & & \downarrow{\scriptstyle E(f_{-1})} & & \downarrow{\scriptstyle E(f_0)} & & & & \downarrow{\scriptstyle E(f_n)} & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & \cdots & \longrightarrow & E(L_{-1}) & \xrightarrow{d_0} & E(L_0) & \xrightarrow{d_1} & \cdots & \xrightarrow{d_n} & E(L_n) & \xrightarrow{d_{n+1}} & \cdots
\end{array}$$

En fait, $C(\bullet, E)$ est même défini sur les objets co-semi-simpliciaux (cf. p. 37).

Cohomologie de Barr-Beck

Soit $H^n(K, E) = \ker d_{n+1}/\text{im } d_n$, $n \in \mathbb{N}$.

Définit une famille de foncteurs $H^\bullet(_, E) : \mathcal{C}^\Delta \to \mathcal{A}$,

$H^n(_, E)$ est la $n$ième cohomologie à coefficients dans E.

Exemples:

- $\mathcal{A} = \boldsymbol{Ab}$, $\mathcal{C} = \boldsymbol{Set}^{op}$, E foncteur groupe abélien libre
  (co)homologie des ensembles (co)simpliciaux;
- $\mathcal{A} = A\boldsymbol{Mod}$ (A anneau), $\mathcal{C} = \boldsymbol{Grp}^{op}$, E foncteur $_ \otimes_A N$
  homologie des A-modules M à coefficients dans N ($\text{Tor}^A_\bullet(M, N)$)

Cochaînes et structure cartésienne

On a:

- $C(K \times L, E) = C(K, E) \otimes C(L, E)$,
  où $(C \otimes C')_n = \coprod_{p+q=n} C_p \otimes C'_q$;
  $d(x_p \otimes y_q) = dx_p + dy_q$

- $C(\mathbf{hom}(K, L), E) = \mathbf{hom}(C(K, E), C(L, E))$,
  où $\mathbf{hom}(C, C')_n = \prod_{p+q=n} \mathbf{hom}(C_p, C'_q)$,
  $d(f \in \mathbf{hom}(C_p, C'_q)) = d_{q+1} \circ f + (-1)^{p+q+1} f \circ d_p$.

- $_ \otimes K \dashv \mathbf{hom}(K, _)$, on a donc une structure symétrique monoïdale close sur $\boldsymbol{CoCh}(\mathcal{A})$,
  et le foncteur $C(_, E)$ préserve la structure symétrique monoïdale close de la CCC $\mathcal{C}$.

Homologie et structure cartésienne

Si $\mathcal{A}$ est la catégorie des k-espaces vectoriels,
$H^\bullet(K \times L, E) = H^\bullet(K, E) \otimes H^\bullet(L, E)$, et
$H^\bullet(\mathbf{hom}(K, L), E) = \mathbf{hom}(H^\bullet(K, E), H^\bullet(L, E))$.

En général ($\mathcal{A}$ catégorie des groupes abéliens ou des R-modules par ex.), s'ajoutent des Tor (...) aux premiers et des Ext (...) aux seconds. (Théorème des coefficients universels.)

Coefficients dans le cas de la monade des noms

On cherche un foncteur $E : \mathbb{C} = \boldsymbol{Set}^{\mathcal{I}} \to \mathcal{A}$, où $\mathcal{A}$ est une catégorie abélienne bien choisie.

Il y a un choix canonique:

- $\mathcal{A} = \boldsymbol{CoCh}(A\boldsymbol{Mod})$ (complexes de cochaînes de A-modules)

  (ma préférence personnelle: $A = \mathbb{F}_p$ corps fini...)

- E envoie chaque $(K_n)_{n\geq -1}$ objet de $\boldsymbol{Set}^{\mathcal{I}}$ vers le complexe des $C_n = A[K_n]$ (A-module libre au-dessus de K_n), avec la différentielle évidente (cf. p. 37).

Piste 1: le sous-scone dans les complexes de cochaînes

On avait une sémantique dans $\mathbb{C}$, puis une dans $\mathbb{C}^{\Delta}$, donc on pourrait passer à une sémantique dans $\boldsymbol{CoCh}(\mathcal{A})$, via un foncteur coefficients E;

Naturellement, E envoie:

- des produits cartésiens $\times$ vers des produits tensoriels $\otimes$;
- des exponentielles (cartésiennes) vers des exponentielles (tensorielles).

En fait, dans $A\boldsymbol{Mod}$, on a même les projections $\pi_i : A_1 \otimes A_2 \to A_i$. (Conjecture: ça passe à $\boldsymbol{CoCh}(A\boldsymbol{Mod})$.)

On peut refaire toute la théorie des sous-scones pratiquement sans modification! (Remplacer $\times$ par $\otimes$ partout...)

Mais que serait une catégorie-symétrique-monoïdale-avec-monades-etc. libre? (Nécessaire pour obtenir un diagramme similaire à la p. 25.)

Piste 2: Comment bien algébriser les sous-scones

Remarque fondamentale: $S \overset{m}{\hookrightarrow} |A|^*$ est essentiellement la donnée d'une inclusion de S dans $|A|^*$.

(Attention: tout mono n'est pas en général une inclusion [un mono régulier]...)

Il y a donc un sens à passer à la cohomologie en considérant la cohomologie relative de $|A|^*$ par rapport à S dans $\mathbb{C}^\Delta$.

En somme, au lieu de définir un sous-scone $\boldsymbol{C}\downarrow \boldsymbol{CoCh}(A\boldsymbol{Mod})$ des complexes de chaînes, on définit une homologie relative au-dessus du sous-scone $\boldsymbol{C}\downarrow \mathbb{C}^\Delta$.

Cohomologie relative sur $S \overset{m}{\hookrightarrow} |A|^*$

On demande que l'image par E d'un mono pertinent dans $\mathbb{C}^\Delta$ soit un mono de $\mathcal{A}$. (C'est vrai pour le E canonique de la p. 54.)

On a alors la suite exacte courte:

$$0 \longrightarrow E(S) \xrightarrow{E(m)} E(|A|^*) \xrightarrow{q} \text{coker } E(m) \longrightarrow 0$$

où q est l'application quotient, coker $E(m) = |A|^*/\text{im } E(m)$ ("$= |A|^*/S$")

On en déduit la suite exacte longue classique de cohomologie:

$$\cdots \longrightarrow H^n(S) \xrightarrow{E(m)} H^n(|A|^*) \xrightarrow{q} H^n(|A|^*/S) \overset{\widetilde{d}}{\dashrightarrow} H^{n+1}(S) \xrightarrow{E(m)} \cdots$$

(On abrège $H^\bullet(_, E)$ en $H^\bullet(_)$.)

Produits, exponentielles, monades, etc.

Peut-on calculer:

- $H^\bullet(|A_1 \times A_2|^*/\overline{S_1 \times S_2})$ en fonction des $H^\bullet(|A_i|^*/S_i)$, $i = 1, 2$?
  (Notations: cf. p. 42)

  à trouver (Künneth, i.e., coefficients universels?)...

- $H^\bullet(|\mathbf{hom}(A_1, A_2)|^*/\widetilde{S})$ en fonction des $H^\bullet(|A_i|^*/S_i)$, $i = 1, 2$?
  (Notations: cf. p. 44)

  à trouver (coefficients universels?)...

- $H^\bullet(|TA|/\widetilde{S})$? (Notations: cf. p. 28)

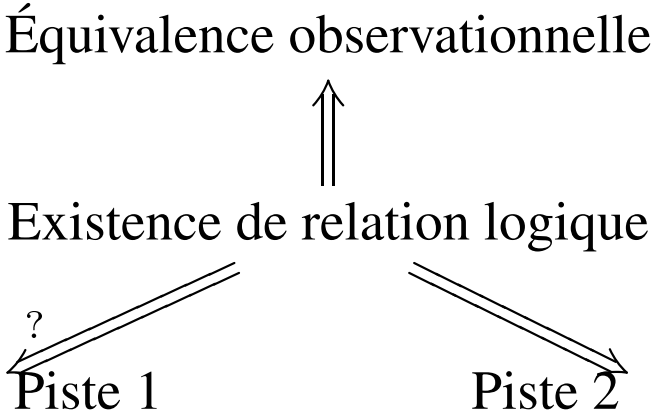
  Ça, c'est facile: $H^n(|TA|/\widetilde{S}) = H^{n-1}(A/S)$.

Et finalement: tout ceci répond-il à la question de l'approximation de l'existence d'une relation logique reliant deux termes donnés?

à trouver...

Conclusion

Il y a du travail... et les implications sont a priori dans le mauvais sens:



existence d'objet dans $\boldsymbol{C}\downharpoonright\boldsymbol{CoCh}(A\boldsymbol{Mod})$

existence d'objet dans $H^{\bullet}(\boldsymbol{C}\downharpoonright\mathbb{C}^{\Delta}, E)$

... il manque une implication du bas vers le haut (Hurewicz?)

Peut toujours servir à montrer l'inexistence d'une preuve d'équivalence observationnelle par relation logiques;

donc à l'inéquivalence observationnelle si relations logiques complètes.