Una prueba constructiva del axioma de elección dependiente en lógica clásica

Hugo Herbelin[1], Étienne Miquey[1,2]

[1]Team πr^2 (INRIA), PPS, Université Paris-Diderot
[2]Fac. de Ingeniería, Universidad de la República, Uruguay

29 de Marzo 2016

En el capítulo anterior...

La meta

1. **Objetivo :** definir un sistema de tipos para tener una **prueba** del axioma de elección dependiente
2. **Bonus :** corrección del sistema sin meta-uso del axioma de elección
3. **Super-bonus :** equiconsistencia con otro sistema lógico

Teoría de tipos de Martin-Löf (1973)

Ingredientes

$$\frac{\Gamma, a : A \vdash p : B}{\Gamma \vdash \lambda a.p : A \to B} \to_I \qquad \frac{\Gamma, x : T \vdash p : A}{\Gamma \vdash \lambda x.p : \forall x^T A} \forall_I$$

$$\frac{\Gamma \vdash p : A[t/x] \quad \Gamma \vdash t : T}{\Gamma \vdash (t, p) : \exists x^T A} \exists_I \qquad \frac{\Gamma \vdash p : \exists x^T A(x)}{\Gamma \vdash \mathtt{prf}\ p : A(\mathtt{wit}\ p)} \exists_E$$

Martin-Löf'73

$$\begin{array}{lll} AC_A & := & \lambda H.(\lambda x.\mathtt{wit}(Hx), \lambda x.\mathtt{prf}(Hx)) \\ & : & \forall x^A \exists y^B P(x,y) \to \exists f^{A\to B} \forall x^A P(x, f(x)) \end{array}$$

Herbelin'12

$$\begin{array}{lll} AC_{\mathbb{N}} & := & \lambda H.\mathtt{let}\ H_\infty = \mathtt{cofix}^0_{fn}(H\ n, f(S(n)))\ \mathtt{in} \\ & & (\lambda n.\mathtt{nth}\ n\ H_\infty, \lambda n.\mathtt{nth}\ n\ H_\infty) \\ & : & \forall x^{\mathbb{N}} \exists y^B P(x,y) \to \exists f^{\mathbb{N}\to B} \forall x^{\mathbb{N}} P(x, f(x)) \end{array}$$

Teoría de tipos de Martin-Löf (1973)

Ingredientes

$$\frac{\Gamma, a : A \vdash p : B}{\Gamma \vdash \lambda a.p : A \to B} \to_I \qquad \frac{\Gamma, x : T \vdash p : A}{\Gamma \vdash \lambda x.p : \forall x^T A} \forall_I$$

$$\frac{\Gamma \vdash p : A[t/x] \quad \Gamma \vdash t : T}{\Gamma \vdash (t, p) : \exists x^T A} \exists_I \qquad \frac{\Gamma \vdash p : \exists x^T A(x)}{\Gamma \vdash \mathtt{prf}\, p : A(\mathtt{wit}\, p)} \exists_E$$

Martin-Löf'73

$$\begin{array}{lll} AC_A & := & \lambda H.(\lambda x.\mathtt{wit}(Hx), \lambda x.\mathtt{prf}(Hx)) \\ & : & \forall x^A \exists y^B P(x,y) \to \exists f^{A\to B} \forall x^A P(x, f(x)) \end{array}$$

Herbelin'12

$$\begin{array}{lll} AC_{\mathbb{N}} & := & \lambda H.\mathtt{let}\, H_\infty = \mathtt{cofix}^0_{fn}(H\ n, f(S(n)))\, \mathtt{in} \\ & & \quad (\lambda n.\mathtt{nth}\ n\ H_\infty, \lambda n.\mathtt{nth}\ n\ H_\infty) \\ & : & \forall x^{\mathbb{N}} \exists y^B P(x,y) \to \exists f^{\mathbb{N}\to B} \forall x^{\mathbb{N}} P(x, f(x)) \end{array}$$

dPA^ω

Ref : Hugo Herbelin (LICS'12)

A Constructive Proof of Dependent Choice, Compatible with Classical Logic

Un sistema formal :

- **clásico** : $p, q ::= \dots \mid \mathtt{catch}_\alpha\, p \mid \mathtt{throw}_\alpha\, p$
- con **tipos dependientes** :
  - fórmulas : $A, B ::= \dots \mid [a : A] \to B \mid t = u$,
  - términos : $t, u ::= \dots \mid \mathtt{wit}\, p$,
  - pruebas : $p, q ::= \dots \mid \mathtt{prf}\, p$
- una **compartimentación** :

$$\frac{\Gamma \vdash p : \exists x^T A(x) \quad p \text{ Nef}}{\Gamma \vdash \mathtt{prf}\, p : A(\mathtt{wit}\, p)} \qquad \frac{\Gamma \vdash p : \exists x^T A(x) \quad \Gamma, x : T, a : A \vdash q : B}{\Gamma \vdash \mathtt{dest}\, p\, \mathtt{as}\, ((x, a))\, \mathtt{in}\, q : B}$$

- call-by-value y **sharing** : $p, q ::= \dots \mid \mathtt{let}\, a = q\, \mathtt{in}\, p$
- con constructores inductivos y **coinductivos** :
  $p, q ::= \dots \mid \mathtt{ind}\ t\ \mathtt{of}\ [p \mid (x, a).q] \mid \mathtt{cofix}^t_{bn}\ p$
- **pereza** para el $\mathtt{cofix}$

Propiedades

Subject reduction

Si $\Gamma \vdash p : A$ y $p \triangleright q$, entonces $\Gamma \vdash q : A$.

Normalización

Si $\Gamma \vdash p : A$ entonces p se normaliza.

Conservatividad

If A is $\rightarrow$-ν-$\texttt{wit}$-$\forall$-free, and $\vdash_{dPA^\omega} p : A$, then $\vdash_{HA^\omega} p : A$

Corrección

$$\nvdash_{dPA^\omega} \bot$$

Continuación : aspecto lógico

Lógica clásica :

- lógica intuicionista + axioma clásica
- Encaje en lógica intuicionista :
  ↬ traducción negativa :

$$A \mapsto (A \to \bot) \to \bot$$

Cálculo clásico :

- cálculo intuicionista + manipulación explicita de continuaciones
- "compilación" en un cálculo intuicionista :
  ↬ traducción **CPS** :

$$t : A \mapsto [\![t]\!] : (A \to \bot) \to \bot$$

Normalización por CPS

- **Lenguaje 1 :** λ-coso, reducción, tipaje
- **Lenguaje 2 :** λ-cosa, reducción, tipaje, normalización

Normalización

$$\Gamma \vdash_1 p : A \qquad \Rightarrow \qquad p \text{ normaliza.}$$

Proof :

1. Si $\Gamma \vdash_1 p : A$ entonces $[\![\Gamma]\!] \vdash_2 [\![p]\!] : [\![A]\!]$
2. Si $p \to_1 q$ entonces $[\![p]\!] \xrightarrow{+}_2 [\![q]\!]$

$\looparrowright$ si p no normalizaba, tampoco normalizaría $[\![p]\!]$, absurdo !

Semantic artefacts

CPS : Ariola et al (FLOPS'12)

Classical Call-by-Need Sequent Calculi : The Unity of Semantic Artifacts

Semántica operacional :

- Cálculo big-step : *variante del $\bar{\lambda}\mu\tilde{\mu}$-cálculo ?*
- Definición small-step
  $\looparrowright$ reducción *context-free*
- Traducción CPS : *variante del λ-cálculo ?*
- Corrección computacional

Normalización :

- Tipaje de la traducción : *sistema F ?*
- Happy end ?

$\bar{\lambda}\mu\tilde{\mu}$: un cálculo de secuentes

(Nuestra arma principal)

$\bar{\lambda}\mu\tilde{\mu}$

Ventajas :

- Lenguaje de comandos : $\langle p \mid e \rangle$
- Manipulación atómica de las continuaciones : $\mu\alpha.c$
- Permite varias estrategias de reducción

Definición

Pruebas	p	$::=$	$a \mid \lambda a.p \mid \mu\alpha.c$
Contextos	e	$::=$	$\alpha \mid p \cdot e \mid \tilde{\mu}a.c$
Comandos	c	$::=$	$\langle p \mid e \rangle$

Reducción

$$\begin{array}{rcl} \langle \mu\alpha.c \mid e \rangle & \rightsquigarrow & c[e/\alpha] \\ \langle p \mid \tilde{\mu}a.c \rangle & \rightsquigarrow & c[p/a] \\ \langle \lambda a.p \mid q \cdot e \rangle & \rightsquigarrow & \langle q \mid \tilde{\mu}a.\langle p \mid e \rangle\rangle \end{array}$$

Tipaje

$$\frac{\Gamma \vdash p : A \mid \Delta \quad \Gamma \mid e : A \vdash \Delta}{\langle p \mid e \rangle : \Gamma \vdash \Delta}\ \text{CUT}$$

$$\frac{c : (\Gamma \vdash \Delta, \alpha : A)}{\Gamma \vdash \mu\alpha.c : A \mid \Delta}\ \mu \qquad \frac{c : (\Gamma, a : A \vdash \Delta)}{\Gamma \mid \tilde{\mu}a.c : A \vdash \Delta}\ \tilde{\mu}$$

$$\frac{\Gamma, a : A \vdash p : B \mid \Delta}{\Gamma \vdash \lambda a.p : A \to B \mid \Delta}\ \to_I \qquad \frac{\Gamma \vdash q : A \mid \Delta \quad \Gamma \mid e : B \vdash \Delta}{\Gamma \mid q \cdot e : A \to B \vdash \Delta}\ \to_E$$

Tipaje

Cálculo de secuentes :

$$\frac{\Gamma \vdash A \mid \Delta \quad \Gamma \mid A \vdash \Delta}{\Gamma \vdash \Delta}\ \textsc{cut}$$

$$\frac{(\Gamma \vdash \Delta, A)}{\Gamma \vdash A \mid \Delta}\ \mu \qquad \frac{(\Gamma, A \vdash \Delta)}{\Gamma \mid A \vdash \Delta}\ \tilde{\mu}$$

$$\frac{\Gamma, A \vdash B \mid \Delta}{\Gamma \vdash A \to B \mid \Delta}\ \to_I \qquad \frac{\Gamma \vdash A \mid \Delta \quad \Gamma \mid B \vdash \Delta}{\Gamma \mid A \to B \vdash \Delta}\ \to_E$$

Extendiendo para tipos dependientes

Definición

Términos	t	$::=$	$x \mid n \in \mathbb{N} \mid \texttt{wit}\ V$
Pruebas	p	$::=$	$a \mid \lambda a.p \mid \mu\alpha.c$
		$\mid$	$(t,p) \mid \texttt{prf}\ V$
Contextos	e	$::=$	$\alpha \mid p \cdot e \mid \tilde{\mu}a.c$
Comandos	c	$::=$	$\langle p \mid e \rangle$

Reducción

$$
\begin{array}{ccc}
\langle \mu\alpha.c \mid e \rangle & \rightsquigarrow & c[e/\alpha] \\
\langle V \mid \tilde{\mu}a.c \rangle & \rightsquigarrow & c[V/a] \\
\langle \lambda a.p \mid q \cdot e \rangle & \rightsquigarrow & \langle q \mid \tilde{\mu}a.\langle p \mid e \rangle\rangle \\
\langle (t,p) \mid e \rangle & \rightsquigarrow & \langle p \mid \tilde{\mu}a.\langle (t,a) \mid e \rangle\rangle \\
\langle \texttt{prf}(t,V) \mid e \rangle & \rightsquigarrow & \langle V \mid e \rangle \\
\langle \texttt{prf}\ p \mid e \rangle & \rightsquigarrow & \langle p \mid \tilde{\mu}a.\langle \texttt{prf}\ a \mid e \rangle\rangle
\end{array}
$$

Extendiendo para tipos dependientes

Definición

Términos	t	$::=$	$x \mid n \in \mathbb{N} \mid \texttt{wit}\ V$
Pruebas	p	$::=$	$a \mid \lambda a.p \mid \mu\alpha.c$
		$\mid$	$(t,p) \mid \texttt{prf}\ V$
Contextos	e	$::=$	$\alpha \mid p \cdot e \mid \tilde{\mu}a.c$
Comandos	c	$::=$	$\langle p \mid e \rangle$

Reducción

$$\langle \mu\alpha.c \mid e \rangle \rightsquigarrow c[e/\alpha]$$
$$\langle V \mid \tilde{\mu}a.c \rangle \rightsquigarrow c[V/a]$$
$$\langle \lambda a.p \mid q \cdot e \rangle \rightsquigarrow \langle q \mid \tilde{\mu}a.\langle p \mid e \rangle \rangle$$
$$\langle (t,p) \mid e \rangle \rightsquigarrow \langle p \mid \tilde{\mu}a.\langle (t,a) \mid e \rangle \rangle$$
$$\langle \texttt{prf}(t,V) \mid e \rangle \rightsquigarrow \langle V \mid e \rangle$$
$$\langle \texttt{prf}\ p \mid e \rangle \rightsquigarrow \langle p \mid \tilde{\mu}a.\langle \texttt{prf}\ a \mid e \rangle \rangle$$

Extendiendo para tipos dependientes

Definición

Términos	t	$::=$	$x \mid n \in \mathbb{N} \mid \texttt{wit}\ V$
Pruebas	p	$::=$	$a \mid \lambda a.p \mid \mu\alpha.c$
		$\mid$	$(t,p) \mid \texttt{prf}\ V$
Contextos	e	$::=$	$\alpha \mid p \cdot e \mid \tilde{\mu}a.c$
Comandos	c	$::=$	$\langle p \mid e \rangle$

Reducción

$$\langle \mu\alpha.c \mid e \rangle \rightsquigarrow c[e/\alpha]$$
$$\langle V \mid \tilde{\mu}a.c \rangle \rightsquigarrow c[V/a]$$
$$\langle \lambda a.p \mid q \cdot e \rangle \rightsquigarrow \langle q \mid \tilde{\mu}a.\langle p \mid e \rangle\rangle$$
$$\langle (t,p) \mid e \rangle \rightsquigarrow \langle p \mid \tilde{\mu}a.\langle (t,a) \mid e \rangle\rangle$$
$$\langle \texttt{prf}(t,V) \mid e \rangle \rightsquigarrow \langle V \mid e \rangle$$
$$\langle \texttt{prf}\ p \mid e \rangle \rightsquigarrow \langle p \mid \tilde{\mu}a.\langle \texttt{prf}\ a \mid e \rangle\rangle$$

Extendiendo para tipos dependientes

Definición

Términos	t	$::=$	$x \mid n \in \mathbb{N} \mid \texttt{wit}\ V$
Pruebas	p	$::=$	$a \mid \lambda a.p \mid \mu\alpha.c$
		$\mid$	$(t,p) \mid \texttt{prf}\ V$
Contextos	e	$::=$	$\alpha \mid p \cdot e \mid \tilde{\mu}a.c$
Comandos	c	$::=$	$\langle p \mid e \rangle$

Reducción

$$\begin{array}{ccc}
\langle \mu\alpha.c \mid e \rangle & \rightsquigarrow & c[e/\alpha] \\
\langle V \mid \tilde{\mu}a.c \rangle & \rightsquigarrow & c[V/a] \\
\langle \lambda a.p \mid q \cdot e \rangle & \rightsquigarrow & \langle q \mid \tilde{\mu}a.\langle p \mid e \rangle\rangle \\
\langle (t,p) \mid e \rangle & \rightsquigarrow & \langle p \mid \tilde{\mu}a.\langle (t,a) \mid e \rangle\rangle \\
\langle \texttt{prf}(t,V) \mid e \rangle & \rightsquigarrow & \langle V \mid e \rangle \\
\langle \texttt{prf}\ p \mid e \rangle & \rightsquigarrow & \langle p \mid \tilde{\mu}a.\langle \texttt{prf}\ a \mid e \rangle\rangle
\end{array}$$

Tipaje (bis)

$$\frac{\Gamma \vdash p : A \mid \Delta \quad \Gamma \mid e : A \vdash \Delta}{\langle p \mid e \rangle : \Gamma \vdash \Delta}\ \textsc{Cut}$$

$$\frac{c : (\Gamma \vdash \Delta, \alpha : A)}{\Gamma \vdash \mu\alpha.c : A \mid \Delta}\ \mu \qquad \frac{c : (\Gamma, a : A \vdash \Delta)}{\Gamma \mid \tilde{\mu}a.c : A \vdash \Delta}\ \tilde{\mu}$$

$$\frac{\Gamma, a : A \vdash p : B \mid \Delta}{\Gamma \vdash \lambda a.p : [a : A] \to B \mid \Delta}\ \to_I \qquad \frac{\Gamma \vdash q : A \mid \Delta \quad \Gamma \mid e : B[q/a] \vdash \Delta \qquad q \notin V \Rightarrow a \notin B}{\Gamma \mid q \cdot e : [a : A] \to B \vdash \Delta}\ \to_E$$

$$\frac{\Gamma \vdash t : \mathbb{N} \mid \Delta \quad \Gamma \vdash p : A(t) \mid \Delta}{\Gamma \vdash (t, p) : \exists x A(x) \mid \Delta}\ \exists_I \qquad \frac{\Gamma \vdash V : \exists x A(x) \mid \Delta}{\Gamma \vdash \texttt{prf}\ V : A(\texttt{wit}\ V) \mid \Delta}\ \texttt{prf}$$

$$\frac{\Gamma \vdash p : \exists x A(x) \mid \Delta}{\Gamma \vdash \texttt{wit}\ V : \mathbb{N} \mid \Delta}\ \texttt{wit} \qquad \frac{\Gamma \vdash p : A \mid \Delta \quad A \equiv B}{\Gamma \vdash p : B \mid \Delta}\ \textsc{Conv} \qquad \frac{\Gamma \mid e : A \vdash \Delta \quad A \equiv B}{\Gamma \mid e : B \vdash \Delta}\ \textsc{Conv}$$

Otra vez, un problema...

$$\dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta}{\Gamma \vdash \lambda a.p : [a:A] \to B \mid \Delta} \qquad \dfrac{\Gamma \vdash q : A \mid \Delta \qquad \Gamma \mid e : B[q] \vdash \Delta \qquad q \in V}{\Gamma \mid q \cdot e : [a:A] \to B \vdash \Delta}}{\langle \lambda a.p \mid q \cdot e \rangle : \Gamma \vdash \Delta}\ \mathrm{CUT}$$

$$\rightsquigarrow$$

$$\dfrac{\Gamma \vdash q : A \mid \Delta \qquad \dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta \qquad \Gamma, a : A \mid e : B[q] \vdash \Delta}{\langle p \mid e \rangle : \Gamma, a : A \vdash \Delta}\ \mathrm{CUT}}{\Gamma \mid \tilde{\mu} a.\langle p \mid e \rangle : A \vdash \Delta}\ \tilde{\mu}}{\langle q \mid \tilde{\mu} a.\langle p \mid e \rangle \rangle : \Gamma \vdash \Delta}\ \mathrm{CUT}$$

Otra vez, un problema...

$$\dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta}{\Gamma \vdash \lambda a.p : [a:A] \to B \mid \Delta} \quad \dfrac{\Gamma \vdash q : A \mid \Delta \qquad \Gamma \mid e : B[q] \vdash \Delta \quad q \in V}{\Gamma \mid q \cdot e : [a:A] \to B \vdash \Delta}}{\langle \lambda a.p \mid q \cdot e \rangle : \Gamma \vdash \Delta}\ \text{CUT}$$

$$\rightsquigarrow$$

$$\dfrac{\Gamma \vdash q : A \mid \Delta \qquad \dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta \qquad \Gamma, a : A \mid e : B[q] \vdash \Delta}{\langle p \mid e \rangle : \Gamma, a : A \vdash \Delta}\ \text{CUT}}{\Gamma \mid \tilde{\mu}a.\langle p \mid e \rangle : A \vdash \Delta}\ \tilde{\mu}}{\langle q \mid \tilde{\mu}a.\langle p \mid e \rangle \rangle : \Gamma \vdash \Delta}\ \text{CUT}$$

Otra vez, un problema...

$$\dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta}{\Gamma \vdash \lambda a.p : [a : A] \to B \mid \Delta} \qquad \dfrac{\Gamma \vdash q : A \mid \Delta \qquad \Gamma \mid e : B[q] \vdash \Delta \quad q \in V}{\Gamma \mid q \cdot e : [a : A] \to B \vdash \Delta}}{\langle \lambda a.p \mid q \cdot e \rangle : \Gamma \vdash \Delta}\ \mathrm{CUT}$$

$$\rightsquigarrow$$

$$\dfrac{\Gamma \vdash q : A \mid \Delta \qquad \dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta \qquad \Gamma, a : A \mid e : B[q] \vdash \Delta}{\langle p \mid e \rangle : \Gamma, a : A \vdash \Delta}\ \mathrm{CUT}}{\Gamma \mid \tilde{\mu}a.\langle p \mid e \rangle : A \vdash \Delta}\ \tilde{\mu}}{\langle q \mid \tilde{\mu}a.\langle p \mid e \rangle \rangle : \Gamma \vdash \Delta}\ \mathrm{CUT}$$

Otra vez, un problema...

$$\dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta}{\Gamma \vdash \lambda a.p : [a : A] \to B \mid \Delta} \qquad \dfrac{\Gamma \vdash q : A \mid \Delta \qquad \Gamma \mid e : B[q] \vdash \Delta \qquad q \in V}{\Gamma \mid q \cdot e : [a : A] \to B \vdash \Delta}}{\langle \lambda a.p \mid q \cdot e \rangle : \Gamma \vdash \Delta}\ \text{CUT}$$

$$\rightsquigarrow$$

$$\dfrac{\Gamma \vdash q : A \mid \Delta \qquad \dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta \qquad \Gamma, a : A \mid e : B[q] \vdash \Delta}{\langle p \mid e \rangle : \Gamma, a : A \vdash \Delta}\ \text{CUT}}{\Gamma \mid \tilde\mu a.\langle p \mid e \rangle : A \vdash \Delta}\ \tilde\mu}{\langle q \mid \tilde\mu a.\langle p \mid e \rangle \rangle : \Gamma \vdash \Delta}\ \text{CUT}$$

Otra vez, un problema...

$$\dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta}{\Gamma \vdash \lambda a.p : [a : A] \to B \mid \Delta} \qquad \dfrac{\Gamma \vdash q : A \mid \Delta \qquad \Gamma \mid e : B[q] \vdash \Delta \quad q \in V}{\Gamma \mid q \cdot e : [a : A] \to B \vdash \Delta}}{\langle \lambda a.p \mid q \cdot e \rangle : \Gamma \vdash \Delta}\ \text{CUT}$$

$$\rightsquigarrow$$

$$\dfrac{\Gamma \vdash q : A \mid \Delta \qquad \dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta \qquad \Gamma, a : A \mid e : B[q] \vdash \Delta}{\langle p \mid e \rangle : \Gamma, a : A \vdash \Delta}\ \text{CUT}}{\Gamma \mid \tilde{\mu}a.\langle p \mid e \rangle : A \vdash \Delta}\ \tilde{\mu}}{\langle q \mid \tilde{\mu}a.\langle p \mid e \rangle \rangle : \Gamma \vdash \Delta}\ \text{CUT}$$

Otra vez, un problema...

$$\dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta}{\Gamma \vdash \lambda a.p : [a:A] \to B \mid \Delta} \qquad \dfrac{\Gamma \vdash q : A \mid \Delta \qquad \Gamma \mid e : B[q] \vdash \Delta \quad q \in V}{\Gamma \mid q \cdot e : [a:A] \to B \vdash \Delta}}{\langle \lambda a.p \mid q \cdot e \rangle : \Gamma \vdash \Delta}\ \text{CUT}$$

$$\rightsquigarrow$$

$$\dfrac{\Gamma \vdash q : A \mid \Delta \qquad \dfrac{\dfrac{\Gamma, a : A \vdash p : B[a] \mid \Delta \qquad \Gamma, a : A \mid e : B[q] \vdash \Delta; \{a|q\}}{\langle p \mid e \rangle : \Gamma, a : A \vdash \Delta; \{a|q\}}\ \text{CUT}}{\Gamma \mid \tilde{\mu}a.\langle p \mid e \rangle : A \vdash \Delta; \{.|q\}}\ \tilde{\mu}}{\langle q \mid \tilde{\mu}a.\langle p \mid e \rangle\rangle : \Gamma \vdash \Delta; \{\cdot|\cdot\}}\ \text{CUT}$$

Tipaje (ter)

$$\frac{\Gamma \vdash p : A_{\varepsilon^+} \mid \Delta; \varepsilon \quad \Gamma \mid e : A_{\varepsilon^-} \vdash \Delta; \{\cdot|p\}\varepsilon}{\langle p \mid e \rangle : \Gamma \vdash \Delta; \varepsilon}\ \textsc{Cut}$$

$$\frac{c : (\Gamma \vdash \Delta, \alpha : A; \varepsilon)}{\Gamma \vdash \mu\alpha.c : A \mid \Delta; \varepsilon}\ \mu \qquad \frac{c : (\Gamma, a : A \vdash \Delta; \{a|p\}\varepsilon)}{\Gamma \mid \tilde{\mu}a.c : A \vdash \Delta; \{\cdot|p\}\varepsilon}\ \tilde{\mu}$$

$$\frac{\Gamma, a : A \vdash p : B \mid \Delta; \varepsilon}{\Gamma \vdash \lambda a.p : [a : A] \to B \mid \Delta; \varepsilon}\ \to_I \qquad \frac{\Gamma \vdash q : A \mid \Delta \quad \Gamma \mid e : B[q] \vdash \Delta; \{\cdot|\mu\alpha.\langle p \mid q \cdot \alpha\rangle\}\varepsilon}{\Gamma \mid q \cdot e : [a : A] \to B \vdash \Delta; \{\cdot|p\}\varepsilon}\ \to_E$$

$$\frac{\Gamma \vdash t : \mathbb{N} \mid \Delta \quad \Gamma \vdash p : A(t) \mid \Delta; \varepsilon}{\Gamma \vdash (t, p) : \exists x A(x) \mid \Delta; \varepsilon}\ \exists_I \qquad \frac{\Gamma \vdash V : \exists x A(x) \mid \Delta; \varepsilon}{\Gamma \vdash \mathtt{prf}\ V : A(\mathtt{wit}\ V) \mid \Delta; \varepsilon}\ \mathtt{prf}$$

$$\frac{\Gamma \vdash V : \exists x A(x) \mid \Delta; \varepsilon}{\Gamma \vdash \mathtt{wit}\ V : \mathbb{N} \mid \Delta; \varepsilon}\ \mathtt{wit} \qquad \frac{\Gamma \vdash p : A \mid \Delta; \varepsilon \quad A \equiv B}{\Gamma \vdash p : B \mid \Delta; \varepsilon}\ \textsc{Conv}$$

Subject reduction

Si $c : \Gamma \vdash \Delta; \{\cdot \mid \cdot\}$ y $c \rightsquigarrow c'$, entonces $c' : \Gamma \vdash \Delta; \{\cdot \mid \cdot\}$

Tipaje (ter)

$$\frac{\Gamma \vdash p : A_{\varepsilon^+} \mid \Delta; \varepsilon \quad \Gamma \mid e : A_{\varepsilon^-} \vdash \Delta; \{\cdot|p\}\varepsilon}{\langle p \mid e\rangle : \Gamma \vdash \Delta; \varepsilon}\ \textsc{Cut}$$

$$\frac{c : (\Gamma \vdash \Delta, \alpha : A; \varepsilon)}{\Gamma \vdash \mu\alpha.c : A \mid \Delta; \varepsilon}\ \mu \qquad \frac{c : (\Gamma, a : A \vdash \Delta; \{a|p\}\varepsilon)}{\Gamma \mid \tilde{\mu}a.c : A \vdash \Delta; \{\cdot|p\}\varepsilon}\ \tilde{\mu}$$

$$\frac{\Gamma, a : A \vdash p : B \mid \Delta; \varepsilon}{\Gamma \vdash \lambda a.p : [a : A] \to B \mid \Delta; \varepsilon}\ \to_I \qquad \frac{\Gamma \vdash q : A \mid \Delta \quad \Gamma \mid e : B[q] \vdash \Delta; \{\cdot|\mu\alpha.\langle p \mid q \cdot \alpha\rangle\}\varepsilon}{\Gamma \mid q \cdot e : [a : A] \to B \vdash \Delta; \{\cdot|p\}\varepsilon}\ \to_E$$

$$\frac{\Gamma \vdash t : \mathbb{N} \mid \Delta \quad \Gamma \vdash p : A(t) \mid \Delta; \varepsilon}{\Gamma \vdash (t, p) : \exists x A(x) \mid \Delta; \varepsilon}\ \exists_I \qquad \frac{\Gamma \vdash V : \exists x A(x) \mid \Delta; \varepsilon}{\Gamma \vdash \texttt{prf}\ V : A(\texttt{wit}\ V) \mid \Delta; \varepsilon}\ \texttt{prf}$$

$$\frac{\Gamma \vdash V : \exists x A(x) \mid \Delta; \varepsilon}{\Gamma \vdash \texttt{wit}\ V : \mathbb{N} \mid \Delta; \varepsilon}\ \texttt{wit} \qquad \frac{\Gamma \vdash p : A \mid \Delta; \varepsilon \quad A \equiv B}{\Gamma \vdash p : B \mid \Delta; \varepsilon}\ \textsc{Conv}$$

Subject reduction

Si $c : \Gamma \vdash \Delta; \{\cdot \mid \cdot\}$ y $c \rightsquigarrow c'$, entonces $c' : \Gamma \vdash \Delta; \{\cdot \mid \cdot\}$

Otra vez, un problema... (bis)

- Hicimos un "bricolaje" para solucionar eso :

$$\langle \lambda a.p \mid q \cdot e \rangle : \Gamma \vdash \Delta \quad \rightsquigarrow \quad \langle q \mid \tilde{\mu}a.\langle p \mid e \rangle\rangle : \Gamma \vdash \Delta$$

- Pero en la CPS, seguimos teniendo el problema :

$$\begin{aligned} [\![\langle q \mid \tilde{\mu}a.\langle p \mid e \rangle\rangle]\!] &:= [\![q]\!]\,[\![\tilde{\mu}a.\langle p \mid e \rangle]\!] \\ &= [\![q]\!]\,(\lambda a.\underbrace{[\![p]\!]}_{\neg\neg A[a]}\ \underbrace{[\![e]\!]}_{\neg A[q]}) \end{aligned}$$

- Nos gustaría tener algo como :

$$[\![\langle q \mid \tilde{\mu}a.\langle p \mid e \rangle\rangle]\!] := ([\![q]\!]\,(\lambda a.[\![p]\!]))[\![e]\!]$$

↬ explicación en el pizarrón

Otra vez, un problema... (bis)

- Hicimos un "bricolaje" para solucionar eso :

$$\langle \lambda a.p \mid q \cdot e \rangle : \Gamma \vdash \Delta \qquad \rightsquigarrow \qquad \langle q \mid \tilde{\mu} a.\langle p \mid e \rangle \rangle : \Gamma \vdash \Delta$$

- Pero en la CPS, seguimos teniendo el problema :

$$\begin{aligned} [\![\langle q \mid \tilde{\mu} a.\langle p \mid e \rangle \rangle]\!] &:= [\![q]\!]\, [\![\tilde{\mu} a.\langle p \mid e \rangle]\!] \\ &= [\![q]\!]\, (\lambda a. \underbrace{[\![p]\!]}_{\neg\neg A[a]} \underbrace{[\![e]\!]}_{\neg A[q]}) \end{aligned}$$

- Nos gustaría tener algo como :

$$[\![\langle q \mid \tilde{\mu} a.\langle p \mid e \rangle \rangle]\!] := ([\![q]\!]\, (\lambda a.[\![p]\!]))[\![e]\!]$$

$\looparrowright$ explicación en el pizarrón

Otra vez, un problema... (bis)

- Hicimos un "bricolaje" para solucionar eso :

$$\langle \lambda a.p \mid q \cdot e \rangle : \Gamma \vdash \Delta \quad \rightsquigarrow \quad \langle q \mid \tilde{\mu} a.\langle p \mid e \rangle\rangle : \Gamma \vdash \Delta$$

- Pero en la CPS, seguimos teniendo el problema :

$$\begin{aligned} [\![\langle q \mid \tilde{\mu} a.\langle p \mid e \rangle\rangle]\!] &:= [\![q]\!]\, [\![\tilde{\mu} a.\langle p \mid e \rangle]\!] \\ &= [\![q]\!]\, (\lambda a. \underbrace{[\![p]\!]}_{\neg\neg A[a]} \ \underbrace{[\![e]\!]}_{\neg A[q]}) \end{aligned}$$

- Nos gustaría tener algo como :

$$[\![\langle q \mid \tilde{\mu} a.\langle p \mid e \rangle\rangle]\!] := ([\![q]\!]\, (\lambda a.[\![p]\!]))[\![e]\!]$$

$\looparrowright$ explicación en el pizarrón

Extendiendo una última vez

Definición

Términos	t	$::=$	$x \mid n \in \mathbb{N} \mid \texttt{wit}\ V$
Pruebas	p	$::=$	$a \mid \lambda a.p \mid \mu\alpha.c \mid (t,p) \mid \texttt{prf}\ V$
		$\mid$	$\mu\hat{\texttt{tp}}.c_{\hat{\texttt{tp}}}$
Contextos	e	$::=$	$\alpha \mid p \cdot e \mid \tilde{\mu}a.c \mid$
Comandos	c	$::=$	$\langle p \mid e \rangle$
	$c_{\hat{\texttt{tp}}}$	$::=$	$\langle p \mid \hat{\texttt{tp}} \rangle \mid \langle V \mid \tilde{\mu}a.c_{\hat{\texttt{tp}}} \rangle$

Reducción

$$\langle \lambda a.p \mid V \cdot e \rangle \rightsquigarrow \langle \mu\hat{\texttt{tp}}.\langle V \mid \tilde{\mu}a.\langle p \mid \hat{\texttt{tp}} \rangle\rangle \mid e \rangle$$

$$\langle \lambda a.p \mid q \cdot e \rangle \rightsquigarrow \langle q \mid \tilde{\mu}a.\langle p \mid e \rangle\rangle$$

$$\langle \mu\hat{\texttt{tp}}.\langle p \mid \hat{\texttt{tp}} \rangle \mid e \rangle \rightsquigarrow \langle p \mid e \rangle$$

$\bar{\lambda}\mu\tilde{\mu}$, pereza y sistema F

(La última dificultad)

Introduciendo pereza

Reducción CbV

$$\begin{array}{lcl}
\langle \mu\alpha.c \mid e\rangle & \rightsquigarrow & c[e/\alpha] \\
\langle V \mid \tilde{\mu}a.c\rangle & \rightsquigarrow & c[p/a] \\
\langle \lambda a.p \mid q \cdot e\rangle & \rightsquigarrow & \langle q \mid \tilde{\mu}a.\langle p \mid e\rangle\rangle
\end{array}$$

$\looparrowright$ pizarrón

Introduciendo pereza

Términos	p	$::=$	$V \mid \mu\alpha.c$
Valores	V	$::=$	$v \mid a$
Funciones	v	$::=$	$\lambda a.p$
Contextos	e	$::=$	$E \mid \tilde{\mu}a.c$
Co-valores	E	$::=$	$F \mid \alpha \mid \tilde{\mu}[a].\langle a \mid F\rangle\tau$
Contextos forzadores	F	$::=$	$\alpha \mid p \cdot E$
Comandos	c	$::=$	$\langle p \mid e\rangle$
Entorno	τ	$::=$	$\epsilon \mid \tau[a := t]$

Reducción CbN

$$
\begin{array}{rcl}
\langle p \mid \tilde{\mu}a.c\rangle\tau & \rightsquigarrow & c\tau[a := p] \\
\langle \mu\alpha.c \mid E\rangle\tau & \rightsquigarrow & (c[E/\alpha])\tau \\
\langle a \mid F\rangle\tau[a := p]\tau' & \rightsquigarrow & \langle p \mid \tilde{\mu}[a].\langle a \mid F\rangle\tau'\rangle\tau \\
\langle V \mid \tilde{\mu}[a].\langle a \mid F\rangle\tau'\rangle\tau & \rightsquigarrow & \langle V \mid F\rangle\tau[a := V]\tau' \\
\langle \lambda a.p \mid q \cdot E\rangle\tau & \rightsquigarrow & \langle q \mid \tilde{\mu}a.\langle p \mid E\rangle\rangle\tau
\end{array}
$$

CPS para el $\bar{\lambda}\mu\tilde{\mu}$ perezoso

Pasos chicos :

$$
\begin{array}{rcl}
\langle p \mid \tilde{\mu}a.c\rangle_e\tau & \rightsquigarrow & c_e\tau[a := p] \\
\langle p \mid E\rangle_e\tau & \rightsquigarrow & \langle p \mid E\rangle_p\tau \\
\langle \mu\alpha.c \mid E\rangle_p\tau & \rightsquigarrow & (c[E/\alpha])\tau \\
\langle V \mid E\rangle_p\tau & \rightsquigarrow & \langle V \mid E\rangle_E\tau \\
\langle V \mid \tilde{\mu}[a].\langle a \mid F\rangle\tau'\rangle_E\tau & \rightsquigarrow & \langle V \mid F\rangle_V\tau[a := V]\tau' \\
\langle V \mid F\rangle_E\tau & \rightsquigarrow & \langle V \mid F\rangle_V\tau \\
\langle a \mid F\rangle_V\tau[a := p]\tau' & \rightsquigarrow & \langle p \mid \tilde{\mu}[a].\langle a \mid F\rangle\tau'\rangle_p\tau \\
\langle \lambda a.p \mid F\rangle_V\tau & \rightsquigarrow & \langle \lambda a.p \mid F\rangle_F\tau \\
\langle \lambda a.p \mid q \cdot E\rangle_F\tau & \rightsquigarrow & \langle q \mid \tilde{\mu}a.\langle p \mid E\rangle\rangle_e\tau
\end{array}
$$

CPS para el $\bar{\lambda}\mu\tilde{\mu}$ perezoso

CPS :

$$
\begin{array}{rcl}
[\![\langle p \mid e\rangle\tau]\!] & := & [\![e]\!]_e\,[\![\tau]\!]_\tau\,[\![p]\!]_p \\
[\![\tilde{\mu}a.c]\!]_e\,\tau\,p & := & [\![c]\!]\,\tau[a := p] \\
[\![E]\!]_e\,\tau\,p & := & p\,\tau\,[\![E]\!]_E \\
[\![\mu\alpha.c]\!]_p\,\tau\,E & := & ([\![c]\!]_c\,\tau)[E/\alpha] \\
[\![V]\!]_p\,\tau\,E & := & E\,\tau\,[\![V]\!]_v \\
[\![\tilde{\mu}[a].\langle a \mid F\rangle\tau']\!]_E\,\tau\,V & := & V\,\tau[a := V]\tau'\,[\![F]\!]_F \\
[\![F]\!]_E\,\tau\,V & := & V\,\tau\,[\![F]\!]_F \\
[\![a]\!]_v\,\tau\,F & := & \tau(a)\,\tau\,(\lambda\tau V.V\,\tau[a := V]\tau'\,[\![F]\!]_F) \\
[\![\lambda a.p]\!]_v\,\tau\,F & := & F\,\tau\,(\lambda q\tau E.[\![p]\!]_p\,\tau[a := q]\,E) \\
[\![q \cdot E]\!]_F\,\tau\,v & := & v\,[\![q]\!]_p\,\tau\,[\![E]\!]_E
\end{array}
$$

↬ Tipaje ?

CPS para el $\bar{\lambda}\mu\tilde{\mu}$ perezoso

CPS :

$$
\begin{array}{rcl}
[\![\langle p \mid e\rangle\tau]\!] & := & [\![e]\!]_e\,[\![\tau]\!]_\tau\,[\![p]\!]_p \\
[\![\tilde{\mu}a.c]\!]_e\,\tau\,p & := & [\![c]\!]\,\tau[a := p] \\
[\![E]\!]_e\,\tau\,p & := & p\,\tau\,[\![E]\!]_E \\
[\![\mu\alpha.c]\!]_p\,\tau\,E & := & ([\![c]\!]_c\,\tau)[E/\alpha] \\
[\![V]\!]_p\,\tau\,E & := & E\,\tau\,[\![V]\!]_v \\
[\![\tilde{\mu}[a].\langle a \mid F\rangle\tau']\!]_E\,\tau\,V & := & V\,\tau[a := V]\tau'\,[\![F]\!]_F \\
[\![F]\!]_E\,\tau\,V & := & V\,\tau\,[\![F]\!]_F \\
[\![a]\!]_v\,\tau\,F & := & \tau(a)\,\tau\,(\lambda\tau V.V\,\tau[a := V]\tau'\,[\![F]\!]_F) \\
[\![\lambda a.p]\!]_v\,\tau\,F & := & F\,\tau\,(\lambda q\tau E.[\![p]\!]_p\,\tau[a := q]\,E) \\
[\![q \cdot E]\!]_F\,\tau\,v & := & v\,[\![q]\!]_p\,\tau\,[\![E]\!]_E
\end{array}
$$

↬ Tipaje ?

Tipaje

Notas / cuestiones :

- Pasaje de continuacion **y** entorno
- 5 niveles :

$$\begin{array}{rl} [\![A]\!]_e & : \tau \to ([\![A]\!]_p \to \bot) \to \bot \\ [\![A]\!]_p & : \tau \to ([\![A]\!]_E \to \bot) \to \bot \\ [\![A]\!]_E & : \tau \to ([\![A]\!]_v \to \bot) \to \bot \\ & \vdots \end{array}$$

- Como tipar el entorno τ ?
- Resultado ?

Tipaje

Indices de De Bruijn :

$$\frac{\Gamma, a_n : A \vdash p : B \mid \Delta \qquad |\Gamma| = n}{\Gamma \vdash \lambda a_n.p : A \to B \mid \Delta} \qquad \frac{c : (\Gamma, a_n : A \vdash \Delta) \quad |\Gamma| = n}{\Gamma \mid \tilde{\mu} a_n.c : A \vdash \Delta}$$

$$\frac{\Gamma, a_n : A, \Gamma' \mid F : A \vdash \Delta \quad \Gamma \vdash \Delta; \tau : \Gamma' \quad |\Gamma| = n}{\Gamma \mid \tilde{\mu}[a_n].\langle a_n \mid F\rangle\tau : A \vdash \Delta} \qquad \frac{\Gamma(i) = a_i : A}{\Gamma \vdash a_i : A \mid \Delta}$$

$$\frac{c : (\Gamma \vdash \Delta, \alpha_n : A) \qquad |\Delta| = n}{\Gamma \vdash \mu\alpha_n.c : A \mid \Delta} \qquad \frac{\Delta(i) = \alpha_i : A}{\Gamma \mid \alpha_i : A \vdash \Delta}$$

Tipaje

Tipaje del entorno :

$$\frac{\Gamma \vdash p : A \mid \Delta \qquad \Gamma \mid e : A \vdash \Delta}{\langle p \mid e \rangle : (\Gamma \vdash \Delta)} \qquad \frac{c : (\Gamma, \Gamma' \vdash \Delta) \qquad \Gamma \vdash \Delta; \tau : \Gamma'}{c\tau : (\Gamma \vdash \Delta)}$$

$$\frac{}{\Gamma \vdash \Delta; \epsilon : \epsilon} \qquad \frac{\Gamma \vdash \Delta; \tau : \Gamma' \qquad \Gamma, \Gamma' \vdash p : A \mid \Delta}{\Gamma \vdash \Delta; \tau[a := p] : \Gamma', a : A}$$

Corrección de la CPS

Pizarrón : tipaje del entorno en la CPS ?

Corrección de la CPS

Enriqueciendo la CPS con todas las informaciones de tipaje,

Teorema

La traducción es bien tipada, i.e.

$$
\begin{array}{lll}
\Gamma \vdash_v \Delta; v : A & \text{implica} & [\![\Gamma \vdash_v \Delta; v : A]\!]^{\vec{T}} \\
\Gamma; F : A \vdash_F \Delta & \text{implica} & [\![\Gamma; F : A \vdash_F \Delta]\!]^{\vec{T}} \\
\Gamma \vdash_V \Delta; V : A & \text{implica} & [\![\Gamma \vdash_V \Delta; V : A]\!]^{\vec{T}} \\
\Gamma; E : A \vdash_E \Delta & \text{implica} & [\![\Gamma; E : A \vdash_E \Delta]\!]^{\vec{T}} \\
\Gamma \vdash_p \Delta; p : A & \text{implica} & [\![\Gamma \vdash_p \Delta; p : A]\!]^{\vec{T}} \\
\Gamma; e : A \vdash_e \Delta & \text{implica} & [\![\Gamma; e : A \vdash_e \Delta]\!]^{\vec{T}} \\
c : (\Gamma \vdash_c \Delta) & \text{implica} & [\![c : (\Gamma \vdash_c \Delta)]\!]^{\vec{T}}
\end{array}
$$

Final feliz

Vimos cómo :

- definir un cálculo de secuentes con tipos dependientes
- definir un cálculo de secuentes perezoso
- definir su traducción tipada por CPS y demostrar así su normalización

Mezclando esos ingredientes y dPA^ω, conseguimos :

- un lenguaje $dLPA^\omega$ con una prueba de $AC_\mathbb{N}$ y DC
- una traducción CPS **tipada** desde $dLPA^\omega$ hacia HA^ω

Teorema

$PA^2 + DC$ es equi-consistente con HA^2

Demostración : sin meta-uso de DC o $AC_\mathbb{N}$! !

Final feliz

Vimos cómo :

- definir un cálculo de secuentes con tipos dependientes
- definir un cálculo de secuentes perezoso
- definir su traducción tipada por CPS y demostrar así su normalización

Mezclando esos ingredientes y dPA^ω, conseguimos :

- un lenguaje $dLPA^\omega$ con una prueba de $AC_{\mathbb{N}}$ y DC
- una traducción CPS **tipada** desde $dLPA^\omega$ hacia HA^ω

Teorema

$PA^2 + DC$ es equi-consistente con HA^2

Demostración : sin meta-uso de DC o $AC_{\mathbb{N}}$! !

Final feliz

Vimos cómo :

- definir un cálculo de secuentes con tipos dependientes
- definir un cálculo de secuentes perezoso
- definir su traducción tipada por CPS y demostrar así su normalización

Mezclando esos ingredientes y dPA^ω, conseguimos :

- un lenguaje $dLPA^\omega$ con una prueba de $AC_\mathbb{N}$ y DC
- una traducción CPS **tipada** desde $dLPA^\omega$ hacia HA^ω

Teorema

$$PA^2 + DC \text{ es equi-consistente con } HA^2$$

Demostración : sin meta-uso de DC o $AC_\mathbb{N}$! !