Introducción a la correspondencia entre pruebas y programas:

Sistema T de Gödel y eliminación de cortes en HA

Alexandre Miquel

mayo de 2021

Kurt **Gödel** (1906–1978)

1958: *„Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes"* (Sobre una extensión todavía no usada del punto de vista finitista)

Interpretación «Dialectica» de HA $\Rightarrow$ introducción del sistema T

Plan

Plan

Sintaxis

Sistema T $=$ sistema $\lambda^{\to,\times}$ $+$ enteros primitivos (único tipo de base)

Definición (Tipos)

Tipos $\quad A, B \quad ::= \quad \mathsf{Nat} \quad | \quad A \to B \quad | \quad A \times B$

Definición (Términos)

Términos $\quad M, N, P \quad ::= \quad x \quad | \quad \lambda x : A \,.\, M \quad | \quad M\, N$
$\quad | \quad \langle M, N \rangle \quad | \quad \pi_1(M) \quad | \quad \pi_2(M)$
$\quad | \quad 0 \quad | \quad \mathtt{S}(M) \quad | \quad \mathtt{rec}(M_0, M_1, N)$

- **Notaciones:** $FV(M)$ (variables libres), $M[x := N]$ (sustitución)

  $+$ lema de sustitución (enunciado usual)

Reducción

- Relación $\succ$ de reducción definida por las 5 reglas:

$$
\begin{array}{rcl}
(\lambda x : A \,.\, M)\, N & \succ & M[x := N] \\
\pi_1(\langle M, N \rangle) & \succ & M \\
\pi_2(\langle M, N \rangle) & \succ & N \\
\mathtt{rec}(M_0,\ M_1,\ 0) & \succ & M_0 \\
\mathtt{rec}(M_0,\ M_1,\ \mathtt{S}(N)) & \succ & M_1\ N\ (\mathtt{rec}(M_0,\ M_1,\ N))
\end{array}
$$

$+$ clausura contextual

Proposición (Confluencia)

La reducción $M \succ M'$ es confluente

Demostración: Ejercicio:

(1) Definir la reducción paralela $M \Rightarrow M'$, tal que $(\succ) \subset (\Rightarrow) \subset (\overset{*}{\succ})$
(2) Demostrar que $M \Rightarrow M'$ y $N \Rightarrow N'$ implican que $M[x := N] \Rightarrow M'[x := N']$
(3) Demostrar que $\Rightarrow$ cumple la propiedad del diamante
(4) Deducir que $\succ$ es confluente

Tipado (1/2)

Contextos $\quad \Gamma, \Delta \quad ::= \quad x_1 : A_1, \ldots, x_n : A_n \qquad (x_i \not\equiv x_j \text{ si } i \neq j)$

Definición (Relación de tipado $\Gamma \vdash M : A$)

$$\frac{}{\Gamma \vdash x : A}\ \text{si } (x{:}A) \in \Gamma \qquad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x : A \,.\, M : A \to B}$$

$$\frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash MN : B}$$

$$\frac{\Gamma \vdash M : A \qquad \Gamma \vdash N : B}{\Gamma \vdash \langle M, N \rangle : A \times B} \qquad \frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \pi_1(M) : A} \qquad \frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \pi_2(M) : B}$$

$$\frac{}{\Gamma \vdash 0 : \mathrm{Nat}} \qquad \frac{\Gamma \vdash M : \mathrm{Nat}}{\Gamma \vdash \mathtt{S}(M) : \mathrm{Nat}}$$

$$\frac{\Gamma \vdash M_0 : A \qquad \Gamma \vdash M_1 : \mathrm{Nat} \to A \to A \qquad \Gamma \vdash N : \mathrm{Nat}}{\Gamma \vdash \mathtt{rec}(M_0, M_1, N) : A}$$

Tipado (2/2)

Ejercicio:

(1) Demostrar los lemas básicos (variables libres, sustitutividad, debilitamiento)

(2) Enunciar y demostrar el lema de inversión:

1. Si $\Gamma \vdash x : C$, entonces ...
2. Si $\Gamma \vdash \lambda x : A \,.\, M : C$, entonces ...
3. Si $\Gamma \vdash MN : C$, entonces ...
4. Si $\Gamma \vdash \langle M, N \rangle : C$, entonces ...
5. Si $\Gamma \vdash \pi_1(M) : C$, entonces ...
6. Si $\Gamma \vdash \pi_2(M) : C$, entonces ...
7. Si $\Gamma \vdash \mathtt{0} : C$, entonces ...
8. Si $\Gamma \vdash \mathtt{S}(M) : C$, entonces ...
9. Si $\Gamma \vdash \mathtt{rec}(M_0, M_1, N) : C$, entonces ...

(3) Deducir la propiedad de *subject reduction*

Ejemplos (1/3)

- Dados M, N : Nat, se definen:

$$\begin{array}{rcll} M + N & :\equiv & \mathtt{rec}(M,\ \lambda uz\,.\,\mathtt{S}(z),\ N) & : \ \mathrm{Nat} \\ M \times N & :\equiv & \mathtt{rec}(0,\ \lambda uz\,.\,z + M,\ N) & : \ \mathrm{Nat} \\ \mathrm{pred}(M) & :\equiv & \mathtt{rec}(0,\ \lambda uz\,.\,u,\ M) & : \ \mathrm{Nat} \end{array}$$

Se verifica que:

$$\begin{array}{rcl@{\qquad\qquad}rcl} M + 0 & \succ & M & M + \mathtt{S}(N) & \overset{+}{\succ} & \mathtt{S}(M + N) \\ M \times 0 & \succ & 0 & M \times \mathtt{S}(N) & \overset{+}{\succ} & (M \times N) + M \\ \mathrm{pred}(0) & \succ & 0 & \mathrm{pred}(\mathtt{S}(M)) & \overset{+}{\succ} & M \end{array}$$

(= mismas ecuaciones que en los términos de HA$^{\cong}$)

- **Ejercicio:** Implementar las funciones $n \mapsto n!$, $(n, m) \mapsto n^m$, $(n, m) \mapsto n \dot{-} m$, $(n, m) \mapsto \max(n, m)$, $(n, m) \mapsto \min(n, m)$

Ejemplos (2/3)

Definición (Funciones definibles en el sistema T)

Una función (total) $f : \mathbb{N}^k \to \mathbb{N}$ es definible en el sistema T cuando existe un término cerrado $M : \underbrace{\mathrm{Nat} \to \cdots \to \mathrm{Nat}}_{k} \to \mathrm{Nat}$ tal que:

$$M\,\overline{n}_1 \cdots \overline{n}_k \overset{*}{\succ} \overline{f(n_1, \ldots, n_k)}$$

para todos $n_1, \ldots, n_k \in \mathbb{N}$ (escribiendo $\overline{n} := \mathtt{S}^n(0)$ para todo $n \in \mathbb{N}$)

Proposición

Todas las funciones recursivas primitivas son definibles en el sistema T

Demostración. Por inducción sobre la definición recursiva primitiva de f. □

Recursión de tipo A cualquiera

- Todos los ejemplos anteriores sólo usan la recursión de tipo Nat:

$$\frac{\Gamma \vdash M_0 : \mathsf{Nat} \qquad \Gamma \vdash M_1 : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} \qquad \Gamma \vdash N : \mathsf{Nat}}{\Gamma \vdash \mathtt{rec}_{\mathsf{Nat}}(M_0, M_1, N) : \mathsf{Nat}}$$

= construcción de un objeto : Nat por recursión sobre otro objeto : Nat

- Recursión sobre el tipo Nat = recursión primitiva:

Teorema

Una función $f : \mathbb{N}^k \to \mathbb{N}$ es recursiva primitiva si y sólo si es definible en el sistema T con recursión restringida al tipo Nat

- Pero el sistema T permite hacer recursión con cualquier tipo A:

$$\frac{\Gamma \vdash M_0 : A \qquad \Gamma \vdash M_1 : \mathsf{Nat} \to A \to A \qquad \Gamma \vdash N : \mathsf{Nat}}{\Gamma \vdash \mathtt{rec}_{A}(M_0, M_1, N) : A}$$

= construcción de un objeto : A por recursión sobre otro objeto : Nat

Ejemplos (3/3)

Proposición

La función de Ackermann $\mathrm{ack} : \mathbb{N}^2 \to \mathbb{N}$ definida por

$$\begin{aligned} \mathrm{ack}(0,\ n) &= y+1 \\ \mathrm{ack}(m+1,\ 0) &= \mathrm{ack}(m,\ 1) \\ \mathrm{ack}(m+1,\ n+1) &= \mathrm{ack}(m,\ \mathrm{ack}(m+1, n)) \end{aligned}$$

es definible en el sistema T

Demostración: Con notaciones a la Curry:

$$\begin{array}{rcl@{\quad}c@{\quad}l} M_0 & :\equiv & \lambda y\,.\,\mathtt{S}(y) & : & \mathrm{Nat}{\to}\mathrm{Nat} \\ M_1 & :\equiv & \lambda f, y\,.\,\mathtt{rec}_{\mathrm{Nat}}(f\,\overline{1},\ \lambda u, z\,.\,f\ z,\ y) & : & (\mathrm{Nat}{\to}\mathrm{Nat}){\to}\mathrm{Nat}{\to}\mathrm{Nat} \\ \mathrm{ack} & :\equiv & \lambda x\,.\,\mathtt{rec}_{\mathrm{Nat}\to\mathrm{Nat}}(M_0,\ \lambda u\,.\,M_1,\ x) & : & \mathrm{Nat}{\to}\mathrm{Nat}{\to}\mathrm{Nat} \end{array}$$

□

Normalización fuerte

Ahora se trata de demostrar el:

Teorema (Normalización fuerte para el sistema T)

Todos los términos tipados del sistema T son fuertemente normalizantes

Arquitectura de la demostración:

(1) Se define una noción de candidato de reducibilidad adecuada para el sistema T, y se estudian sus propiedades

(2) Se asocia a cada tipo A un candidato $[\![A]\!]$...

... y a cada contexto Γ un conjunto de sustituciones $[\![\Gamma]\!]$

(3) Se demuestra el invariante de normalización:

$$\textit{Si}\ \ \Gamma \vdash M : A,\ \ \textit{entonces}\ \ M[\sigma] \in [\![A]\!]\ \ \textit{para todo}\ \sigma \in [\![\Gamma]\!]$$

(4) Se concluye que todo término bien tipado en el sistema T es fuertemente normalizante (por las propiedades de los candidatos)

Candidatos de reducibilidad (1/3)

- **SN** := conjunto de los términos fuertemente normalizantes
- $\mathrm{Red}_1(M) \ := \ \{M' \ : \ M \succ M'\}$
- Los términos en forma canónica (o constructores) son los siguientes:

$$\lambda x : A \,.\, M \qquad \langle M, N \rangle \qquad 0 \qquad \mathtt{S}(M)$$

Un término neutro es un término que no está en forma canónica

Definición (Candidato de reducibilidad)

Un conjunto de términos $C \subseteq \Lambda$ (posiblemente abiertos) es un candidato de reducibilidad cuando cumple los siguientes criterios:

(CR1) $C \subseteq \mathbf{SN}$

(CR2) Si $M \in C$, entonces $\mathrm{Red}_1(M) \subseteq C$

(CR3) Si un término neutro M es tal que $\mathrm{Red}_1(M) \subseteq C$, entonces $M \in C$

Candidatos de reducibilidad (2/3)

Lema

Un candidato de reducibilidad C contiene todas las variables: $x \in C$

Demostración. Ejercicio.

Lema (Propiedades de expansión)

Dado un candidato de reducibilidad C:

1. Si $M[x := N] \in C$ y $N \in \mathbf{SN}$, entonces $(\lambda x : A \,.\, M)N \in C$
2. Si $M \in C$ y $N \in \mathbf{SN}$, entonces $\pi_1(\langle M, N\rangle) \in C$
3. Si $M \in \mathbf{SN}$ y $N \in C$, entonces $\pi_2(\langle M, N\rangle) \in C$
4. Si $M_0 \in C$ y $M_1 \in \mathbf{SN}$, entonces $\mathtt{rec}(M_0, M_1, 0) \in C$
5. Si $M_1\, N\, (\mathtt{rec}(M_0, M_1, N)) \in C$, entonces $\mathtt{rec}(M_0, M_1, \mathtt{S}(N)) \in C$

Demostración. Ejercicio.

Candidatos de reducibilidad (3/3)

Lema (El candidato SN)

SN es un candidato de reducibilidad

Demostración. Ejercicio.

Definición (Flecha y producto de conjuntos de términos)

Dados conjuntos de términos $C, D \subseteq \Lambda$, se definen:

$$\begin{array}{rcl} C \to D & := & \{M \in \Lambda \ : \ \forall N \in C,\ MN \in D\} \\ C \times D & := & \{M \in \Lambda \ : \ \pi_1(M) \in C \ \wedge \ \pi_2(M) \in D\} \end{array}$$

Lema (Clausura de los candidatos por $\to$, $\times$ y $+$)

Si $C, D \subseteq \Lambda$ son candidatos de reducibilidad, entonces los conjuntos $C \to D$ y $C \times D$ también lo son

Demostración. Ejercicio.

Interpretación de los tipos y contextos

Definición (Interpretación de los tipos)

A cada tipo A se asocia el candidato de reducibilidad $[\![A]\!]$ definido por:

$$\begin{array}{rcl} [\![\mathrm{Nat}]\!] & := & \mathbf{SN} \\ [\![A \to B]\!] & := & [\![A]\!] \to [\![B]\!] \\ [\![A \times B]\!] & := & [\![A]\!] \times [\![B]\!] \end{array}$$

Definición (Interpretación de los contextos)

$$[\![\Gamma]\!] \;:=\; \Big\{ \sigma \text{ sustitución } \;:\; \begin{array}{l} \mathrm{dom}(\sigma) = \mathrm{dom}(\Gamma) \quad \text{y} \\ \sigma(x) \in [\![A]\!] \text{ para todo } (x : A) \in \Gamma \end{array} \Big\}$$

Normalización fuerte

Proposición (Invariante de normalización)

Si $\Gamma \vdash M : A$, entonces $M[\sigma] \in [\![A]\!]$ para todo $\sigma \in [\![\Gamma]\!]$

Demostración. Ejercicio.

Teorema (Normalización fuerte)

Si $\Gamma \vdash M : A$, entonces M es fuertemente normalizante

Demostración. Ejercicio.

Corolarios

En el sistema T:

1. Todo término tipado tiene forma normal
2. Dos términos tipados (y de mismo tipo) son convertibles si y sólo si tienen la misma forma normal
3. La relación $M_1 \cong M_2$ (entre términos de mismo tipo) es decidible

Plan

Extensión del sistema T

- En programación como en lógica, es muy cómodo trabajar con un sistema T más amplio, con al menos:
  - un tipo Unit (neutro de $\times$)
  - un tipo Bool (tipo de los booleanos)
  - tipos $A + B$ (sumas directas)
- También se pueden añadir:
  - tipos $[A]$ de listas
  - otros tipos algebraicos: árboles binarios, etc.
- Se presenta y se estudia aquí la extensión "barata" con los tipos Unit, Bool y $A + B$, y se demuestra su carácter conservativo

El tipo Unit

- Se enriquece la sintaxis del sistema T con:

Tipos	A, B	$::=$	$\cdots$	$\mid$	Unit
Términos	M, N	$::=$	$\cdots$	$\mid$	$\langle\rangle$

Intuición: Unit $=$ neutro de $\times$
$=$ tipo del objeto $\langle\rangle$ sin contenido computacional

- Nueva regla de reducción: ninguna

- Nueva regla de tipado:

$$\frac{}{\Gamma \vdash \langle\rangle : \mathsf{Unit}}$$

- Se mantienen confluencia, *subject reduction* y normalización fuerte

El tipo Bool

- Se enriquece la sintaxis del sistema T con:

$$
\begin{array}{lllllllll}
\textbf{Tipos} & A, B & ::= & \cdots & \mid & \mathsf{Bool} & & & \\
\textbf{Términos} & M, N & ::= & \cdots & \mid & \mathsf{true} & \mid & \mathsf{false} & \mid & \mathsf{if}(N, M, M')
\end{array}
$$

- Nuevas reglas de reducción:

$$
\begin{array}{rcl}
\mathsf{if}(\mathsf{true}, M, M') & \succ & M \\
\mathsf{if}(\mathsf{false}, M, M') & \succ & M'
\end{array}
$$

- Nuevas reglas de tipado:

$$
\frac{}{\Gamma \vdash \mathsf{true} : \mathsf{Bool}} \qquad \frac{}{\Gamma \vdash \mathsf{false} : \mathsf{Bool}}
$$

$$
\frac{\Gamma \vdash N : \mathsf{Bool} \qquad \Gamma \vdash M : A \qquad \Gamma \vdash M' : A}{\Gamma \vdash \mathsf{if}(N, M, M') : A}
$$

- Se mantienen confluencia, *subject reduction* y normalización fuerte

El tipo suma $A + B$

- Se enriquece la sintaxis del sistema T con:

$$
\begin{array}{llcl}
\textbf{Tipos} & A, B & ::= & \cdots \mid A + B \\
\textbf{Términos} & M, N & ::= & \cdots \mid \iota_1^{A,B}(M) \mid \iota_2^{A,B}(M) \\
& & & \mid \text{case } N \ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\}
\end{array}
$$

- Nuevas reglas de reducción:

$$
\begin{array}{lcl}
\text{case } \iota_1^{A,B}(M) \ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\} & \succ & M_1[x_1 := M] \\
\text{case } \iota_2^{A,B}(M) \ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\} & \succ & M_2[x_2 := M]
\end{array}
$$

- Nuevas reglas de tipado:

$$
\frac{\Gamma \vdash M : A}{\Gamma \vdash \iota_1^{A,B}(M) : A + B} \qquad \frac{\Gamma \vdash M : B}{\Gamma \vdash \iota_2^{A,B}(M) : A + B}
$$

$$
\frac{\Gamma \vdash N : A + B \qquad \Gamma, x_1 : A \vdash M_1 : C \qquad \Gamma, x_2 : B \vdash M_2 : C}{\Gamma \vdash \text{case } N \ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\} : C}
$$

- Se mantienen confluencia, *subject reduction* y normalización fuerte

Sistema T extendido: sintaxis

Recapitulación:

Definición (Tipos)

$$\textbf{Tipos} \quad A, B ::= \mathrm{Unit} \mid \mathrm{Bool} \mid \mathrm{Nat} \mid A \to B \mid A \times B \mid A + B$$

Definición (Términos)

$$\begin{array}{llcl}
\textbf{Términos} & M, N & ::= & x \mid \lambda x : A \,.\, M \mid M\,N \\
& & \mid & \langle M, N \rangle \mid \pi_1(M) \mid \pi_2(M) \mid \langle\rangle \\
& & \mid & \iota_1^{A,B}(M) \mid \iota_2^{A,B}(M) \\
& & \mid & \mathrm{case}\ N\ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\} \\
& & \mid & \mathrm{true} \mid \mathrm{false} \mid \mathrm{if}(N, M, M') \\
& & \mid & 0 \mid \mathtt{S}(M) \mid \mathtt{rec}(M_0, M_1, N)
\end{array}$$

Sistema T extendido: reducción

Relación $\succ$ de reducción definida por las 9 reglas:

$$(\lambda x : A \,.\, M)N \quad \succ \quad M[x := N]$$

$$\begin{array}{rcl} \pi_1(\langle M, N\rangle) & \succ & M \\ \pi_2(\langle M, N\rangle) & \succ & N \end{array}$$

$$\begin{array}{rcl} \text{case } \iota_1^{A,B}(M)\ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\} & \succ & M_1[x_1 := N] \\ \text{case } \iota_2^{A,B}(M)\ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\} & \succ & M_2[x_2 := N] \end{array}$$

$$\begin{array}{rcl} \text{if}(\text{true}, M, M') & \succ & M \\ \text{if}(\text{false}, M, M') & \succ & M' \end{array}$$

$$\begin{array}{rcl} \mathtt{rec}(M_0, M_1, \mathtt{0}) & \succ & M_0 \\ \mathtt{rec}(M_0, M_1, \mathtt{S}(N)) & \succ & M_1\ N\ (\mathtt{rec}(M_0, M_1, N)) \end{array}$$

$+$ clausura contextual

Ejercicio: Demostrar la confluencia de $\succ$

Sistema T extendido: tipado

Definición (Relación de tipado $\Gamma \vdash M : A$)

$$\frac{}{\Gamma \vdash x : A}\ \text{si } (x{:}A) \in \Gamma \qquad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x : A\,.\,M : A \to B} \qquad \frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash MN : B}$$

$$\frac{}{\Gamma \vdash \langle\rangle : \mathrm{Unit}} \qquad \frac{\Gamma \vdash M : A \qquad \Gamma \vdash N : B}{\Gamma \vdash \langle M, N\rangle : A \times B} \qquad \frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \pi_1(M) : A} \qquad \frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \pi_2(M) : B}$$

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash \iota_1^{A,B}(M) : A + B} \qquad \frac{\Gamma \vdash M : B}{\Gamma \vdash \iota_2^{A,B}(M) : A + B}$$

$$\frac{\Gamma \vdash N : A + B \qquad \Gamma, x_1 : A \vdash M_1 : C \qquad \Gamma, x_2 : B \vdash M_2 : C}{\Gamma \vdash \mathrm{case}\ N\ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\} : C}$$

$$\frac{}{\Gamma \vdash \mathrm{true} : \mathrm{Bool}} \qquad \frac{}{\Gamma \vdash \mathrm{false} : \mathrm{Bool}} \qquad \frac{\Gamma \vdash N : \mathrm{Bool} \qquad \Gamma \vdash M : A \qquad \Gamma \vdash M' : A}{\Gamma \vdash \mathrm{if}(N, M, M') : A}$$

$$\frac{}{\Gamma \vdash 0 : \mathrm{Nat}} \qquad \frac{\Gamma \vdash M : \mathrm{Nat}}{\Gamma \vdash \mathtt{S}(M) : \mathrm{Nat}}$$

$$\frac{\Gamma \vdash M_0 : A \qquad \Gamma \vdash M_1 : \mathrm{Nat} \to A \to A \qquad \Gamma \vdash N : \mathrm{Nat}}{\Gamma \vdash \mathtt{rec}(M_0, M_1, N) : A}$$

Sistema T extendido: propiedades

El sistema T extendido cumple:

- La propiedad de confluencia de la reducción
- Los lemas básicos (variables libres, debilitamiento, sustitutividad)
- El lema de inversión (Ejercicio: enunciarlo y demostrarlo)
- La *subject reduction* (Ejercicio: demostrarla)
- La normalización fuerte (véase más adelante)
- Además:

Teorema (Extensión conservativa)

El sistema T extendido es un extensión conservativa del sistema T básico, que define exactamente las mismas funciones de tipo $\mathsf{Nat}^k \to \mathsf{Nat}$

Demostración: Véase más adelante

Sistema T extendido: conservatividad (1/3)

- **Observación preliminar:** Los tipos del sistema T mínimo[1] son todos habitados. En efecto, se puede asociar a cada tipo A (del sistema mínimo) un término cerrado $\varepsilon_A : A$ definido por:

$$\varepsilon_{\mathsf{Nat}} \;:\equiv\; 0 \qquad \varepsilon_{A\to B} \;:\equiv\; \lambda x : A \,.\, \varepsilon_B \qquad \varepsilon_{A\times B} \;:\equiv\; \langle \varepsilon_A, \varepsilon_B \rangle$$

Retracción del sistema extendido adentro del sistema mínimo:

(1) A cada tipo A del sistema T extendido se asocia el tipo A^* del sistema T básico definido por:

$$\begin{array}{rcl@{\qquad}rcl}
\mathsf{Unit}^* & :\equiv & \mathsf{Nat} & (A\to B)^* & :\equiv & A^* \to B^* \\
\mathsf{Bool}^* & :\equiv & \mathsf{Nat} & (A\times B)^* & :\equiv & A^* \times B^* \\
\mathsf{Nat}^* & :\equiv & \mathsf{Nat} & (A+B)^* & :\equiv & \mathsf{Nat} \times (A^* \times B^*)
\end{array}$$

Obs.: Para todo tipo A del sistema mínimo, se tiene que $A^* \equiv A$ (retracción)

[1] Así como los tipos del sistema extendido

Sistema T extendido: conservatividad (2/3)

(2) A cada término M del sistema T extendido se asocia el término M^* del sistema T mínimo definido por:

$$
\begin{array}{rcl@{\qquad}rcl}
x^* & :\equiv & x & \langle M, N\rangle^* & :\equiv & \langle M^*, N^*\rangle \\
(\lambda x : A \,.\, M)^* & :\equiv & \lambda x : A^* \,.\, M^* & (\pi_1(M))^* & :\equiv & \pi_1(M^*) \\
(MN)^* & :\equiv & M^* N^* & (\pi_2(M))^* & :\equiv & \pi_2(M^*) \\
0^* & :\equiv & 0 & (\mathtt{S}(M))^* & :\equiv & \mathtt{S}(M^*)
\end{array}
$$

$$(\mathtt{rec}(M_0,\ M_1,\ N))^* \ :\equiv\ \mathtt{rec}(M_0^*,\ M_1^*,\ N^*)$$

$$(\langle\rangle)^* \ :\equiv\ 0$$

$$
\begin{array}{rcl@{\qquad}rcl}
\mathrm{true} & :\equiv & \mathtt{S}(0) & \mathrm{false} & :\equiv & 0
\end{array}
$$

$$\mathrm{if}(N, M, M') \ :\equiv\ \mathtt{rec}(M',\ \lambda\_,\_\,.\,M,\ N)$$

$$
\begin{array}{rcl@{\qquad}rcl}
\iota_1^{A,B}(M) & :\equiv & \langle 0, \langle M^*, \varepsilon_{B^*}\rangle\rangle & \iota_2^{A,B}(M) & :\equiv & \langle \mathtt{S}(0), \langle \varepsilon_{A^*}, M^*\rangle\rangle
\end{array}
$$

$$
\begin{array}{l}
(\mathrm{case}\ N\ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\})^* \quad :\equiv \\
\qquad \mathrm{let}\ \langle n, \langle x_1, x_2\rangle\rangle = N^*\ \mathrm{in}\ \mathtt{rec}(M_1^*,\ \lambda\_,\_\,.\,M_2^*,\ n)
\end{array}
$$

Notación: $\lambda\_\,.\,M \ :\equiv\ \lambda z\,.\,M$, con z fresca (= función constante)

Sistema T extendido: conservatividad (3/3)

(3) A cada contexto $\Gamma \equiv x_1 : A_1, \ldots, x_n : A_n$ (sistema T extendido)
se asocia el contexto $\Gamma^* :\equiv x_1 : A_1^*, \ldots, x_n : A_n^*$ (sistema T mínimo)

Propiedades de las retracciones $A \mapsto A^*$ y $M \mapsto M^*$

1. Si $A, M \in \mathscr{L}_{\text{mínimo}}$: $A^* \equiv A$ y $M^* \equiv M$ (retracción)
2. $(M[x := N])^* \equiv M^*[x := N^*]$ (sustitutividad)
3. Si $M \succ M'$ (sis. extendido), entonces $M^* \overset{+}{\succ} M'^*$ (sis. mínimo)
4. Si $\Gamma \vdash M : A$ (sis. extendido), entonces $\Gamma^* \vdash M^* : A^*$ (sis. mínimo)

Corolarios (Normalización fuerte + conservatividad)

1. El sistema T extendido cumple la propiedad de normalización fuerte
2. Dado un término $M : \mathrm{Nat}^k \to \mathrm{Nat}$ (sistema T extendido), el término $M^* : \mathrm{Nat}^k \to \mathrm{Nat}$ (sistema T mínimo) calcula la misma función

Demostración. Ejercicio.

Plan

Recordatorio: sintaxis del sistema $HA^{\cong}$ (1/2)

Términos de $HA^{\cong}$

Términos $\quad t, u \quad ::= \quad x \mid 0 \mid s(t) \mid \mathrm{pred}(t) \mid t + u \mid t \times u$

Definición (Reducción en un paso $t \succ t'$)

$$\frac{}{\mathrm{pred}(0) \succ 0} \qquad \frac{}{\mathrm{pred}(s(t)) \succ t}$$

$$\frac{}{t + 0 \succ t} \qquad \frac{}{t + s(u) \succ s(t + u)}$$

$$\frac{}{t \times 0 \succ 0} \qquad \frac{}{t \times s(u) \succ (t \times u) + t}$$

+ clausura contextual

- Relación $t \succ t'$ confluente y fuertemente normalizante
- Relación $t \cong t'$ (clausura reflexiva-simétrica-transitiva de $\succ$) decidible

Recordatorio: sintaxis del sistema HA$^{\cong}$ (2/2)

Fórmulas de HA$^{\cong}$

$$\textbf{Fórmulas} \qquad A, B, C \quad ::= \quad t = u \;\mid\; \mathrm{null}(t) \;\mid\; \top \;\mid\; \bot \;\mid\; A \wedge B \;\mid\; A \vee B \;\mid\; A \Rightarrow B \;\mid\; \forall x\, A \;\mid\; \exists x\, A$$

Definición (Reducción en un paso $t \succ t'$)

$$\frac{}{\mathrm{null}(0) \;\succ\; \top} \qquad \frac{}{\mathrm{null}(s(t)) \;\succ\; \bot} \qquad \frac{t \succ t'}{\mathrm{null}(t) \;\succ\; \mathrm{null}(t')}$$

$$\frac{t \succ t'}{t = u \;\succ\; t' = u} \qquad \frac{u \succ u'}{t = u \;\succ\; t = u'}$$

$+$ clausura contextual

- Relación $A \succ A'$ confluente y fuertemente normalizante
- Relación $A \cong A'$ (clausura reflexiva-simétrica-transitiva de $\succ$) decidible

Recordatorio: reglas de deducción de HA$^{\cong}$ (1/2)

- Secuentes asimétricos de la forma $\Gamma \vdash A$
- Reglas del cálculo proposicional intuicionista:

(Axioma) $$\frac{}{\Gamma \vdash A'} \text{ si } A' \cong A \in \Gamma$$

($\Rightarrow$) $$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

($\wedge$) $$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

($\vee$) $$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

($\top$) $$\frac{}{\Gamma \vdash C} \text{ si } C \cong \top$$ (sin regla de eliminación)

($\bot$) (sin regla de introducción) $$\frac{\Gamma \vdash C}{\Gamma \vdash A} \text{ si } C \cong \bot$$

Recordatorio: reglas de deducción de $HA^{\cong}$ (2/2)

- Reglas de introducción y de eliminación de los cuantificadores:

(∀) $$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x\, A}\ \text{si}\ x \notin FV(\Gamma) \qquad \frac{\Gamma \vdash \forall x\, A}{\Gamma \vdash A'}\ \text{si}\ A' \cong A[x:=t]$$

(∃) $$\frac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x\, A} \qquad \frac{\Gamma \vdash \exists x\, A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ \text{si}\ x \notin FV(\Gamma, B)$$

- Reglas de introducción y de eliminación de la igualdad:

(=) $$\frac{}{\Gamma \vdash t = t'}\ \text{si}\ t \cong t' \qquad \frac{\Gamma \vdash t = u \qquad \Gamma \vdash A[x := t]}{\Gamma \vdash A'}\ \text{si}\ A' \cong A[x:=u]$$

- Regla de eliminación de los enteros naturales (= inducción):

(Nat-el) $$\frac{\Gamma \vdash A[x := 0] \qquad \Gamma, A \vdash A[x := s(x)]}{\Gamma \vdash A'}\ \text{si}\ \begin{cases} x \notin FV(\Gamma) \\ A' \cong A[x:=t] \end{cases}$$

Recordatorio: reducción de los cortes lógicos (1/5)

Cortes de $\wedge$:

$$\dfrac{\dfrac{\dfrac{\vdots\, d_1}{\Gamma \vdash A} \quad \dfrac{\vdots\, d_2}{\Gamma \vdash B}}{\Gamma \vdash \color{red}{A \wedge B}}\,(\wedge\text{-in})}{\Gamma \vdash A}\,(\wedge\text{-el}_1) \quad \rightsquigarrow \quad \dfrac{\vdots\, d_1}{\Gamma \vdash A}$$

$$\dfrac{\dfrac{\dfrac{\vdots\, d_1}{\Gamma \vdash A} \quad \dfrac{\vdots\, d_2}{\Gamma \vdash B}}{\Gamma \vdash \color{red}{A \wedge B}}\,(\wedge\text{-in})}{\Gamma \vdash B}\,(\wedge\text{-el}_2) \quad \rightsquigarrow \quad \dfrac{\vdots\, d_2}{\Gamma \vdash B}$$

Recordatorio: reducción de los cortes lógicos (2/5)

Corte de $\Rightarrow$:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma, A \vdash B\end{array}}{\Gamma \vdash \color{red}{A \Rightarrow B}}\ (\Rightarrow\text{-in}) \qquad \begin{array}{c}\vdots\ d'\\ \Gamma \vdash A\end{array}}{\Gamma \vdash B}\ (\Rightarrow\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d'\\ \Gamma \vdash A\\ \vdots\ d[\mathsf{ax}(A):=d']\\ \Gamma \vdash B\end{array}$$

Recordatorio: reducción de los cortes lógicos (3/5)

Cortes de $\vee$:

$$\dfrac{\dfrac{\dfrac{\vdots\; d}{\Gamma \vdash A}}{\Gamma \vdash {\color{red}A \vee B}}\,(\vee\text{-in}_1) \qquad \dfrac{\vdots\; d_1'}{\Gamma, A \vdash C} \qquad \dfrac{\vdots\; d_2'}{\Gamma, B \vdash C}}{\Gamma \vdash C}\,(\vee\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c} \vdots\; d \\ \Gamma \vdash A \\ \vdots\; d_1'[\mathrm{ax}(A){:=}d] \\ \Gamma \vdash C \end{array}$$

$$\dfrac{\dfrac{\dfrac{\vdots\; d}{\Gamma \vdash B}}{\Gamma \vdash {\color{red}A \vee B}}\,(\vee\text{-in}_2) \qquad \dfrac{\vdots\; d_1'}{\Gamma, A \vdash C} \qquad \dfrac{\vdots\; d_2'}{\Gamma, B \vdash C}}{\Gamma \vdash C}\,(\vee\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c} \vdots\; d \\ \Gamma \vdash B \\ \vdots\; d_2'[\mathrm{ax}(B){:=}d] \\ \Gamma \vdash C \end{array}$$

Corte de $\top/\bot$: ninguno

Recordatorio: reducción de los cortes lógicos (4/5)

Corte de ∀: $\qquad$ (con $x \notin FV(\Gamma)$ y $A' \cong A[x := t]$)

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A\end{array}}{\Gamma \vdash \color{red}{\forall x\, A}}\,(\forall\text{-in})}{\Gamma \vdash A'}\,(\forall\text{-el}) \quad\leadsto\quad \dfrac{\begin{array}{c}\vdots\ d[x{:=}t]\\ \Gamma \vdash A[x := t]\end{array}}{\Gamma \vdash A'}\,(\text{Conv})$$

Corte de ∃: $\qquad$ (con $x \notin FV(\Gamma, B)$)

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A[x := t]\end{array}}{\Gamma \vdash \color{red}{\exists x\, A}}\,(\exists\text{-in}) \qquad \begin{array}{c}\vdots\ d'\\ \Gamma, A \vdash B\end{array}}{\Gamma \vdash B}\,(\exists\text{-el}) \quad\leadsto\quad \begin{array}{c}\vdots\ d\\ \Gamma \vdash A[x := t]\\ \vdots\ d'[x{:=}t][\mathrm{ax}(A[x{:=}t]){:=}d]\\ \Gamma \vdash B\end{array}$$

Reducción de los cortes lógicos (5/5)

Corte de $=$: (con $t \cong t'$ y $A' \cong A[x := t']$)

$$\dfrac{\dfrac{}{\Gamma \vdash t = t'}\,(=\text{-in}) \qquad \dfrac{\vdots\; d'}{\Gamma \vdash A[x := t]}}{\Gamma \vdash A'}\,(=\text{-el}) \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdots\; d'}{\Gamma \vdash A[x := t]}}{\Gamma \vdash A'}\,(\text{Conv})$$

Recordatorio: reducción de los cortes de inducción

Cortes de inducción: (con $x \notin FV(\Gamma)$ y $A' \cong A[x := t]$)

- Corte cuando $t \cong 0$:

$$\dfrac{\dfrac{\vdots\, d_0}{\Gamma \vdash A[x := 0]} \qquad \dfrac{\vdots\, d_s}{\Gamma, A \vdash A[x := s(x)]}}{\Gamma \vdash A' \quad (\cong A[x := 0])}\ (\text{Nat-el}) \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdots\, d_0}{\Gamma \vdash A[x := 0]}}{\Gamma \vdash A'}\ (\text{Conv})$$

- Corte cuando $t \cong s(t')$:

$$\dfrac{\dfrac{\vdots\, d_0}{\Gamma \vdash A[x := 0]} \qquad \dfrac{\vdots\, d_s}{\Gamma, A \vdash A[x := s(x)]}}{\Gamma \vdash A' \quad (\cong A[x := s(t')])}\ (\text{Nat-el}) \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{\dfrac{\vdots\, d_0}{\Gamma \vdash A[x := 0]} \qquad \dfrac{\vdots\, d_s}{\Gamma, A \vdash A[x := s(x)]}}{\Gamma \vdash A[x := t']}\ (\text{Nat-el})}{\vdots\ d_s[x{:=}t'][\mathrm{Ax}(A[x{:=}t']){:=}\ldots]}}{\dfrac{\Gamma \vdash A[x := s(t')]}{\Gamma \vdash A'}\ (\text{Conv})}$$

Eliminación de cortes en el sistema HA$^{\cong}$

Ahora, tenemos todas las herramientas para demostrar el:

Teorema (Eliminación de cortes en el sistema HA$^{\cong}$)

El sistema formado por las 10 reglas de reducción de cortes del sistema HA$^{\cong}$ es fuertemente normalizante, en el sentido de que no existe ninguna sucesión infinita de reducciones (entre derivaciones de un mismo secuente):

$$\nexists(d_0 \rightsquigarrow d_1 \rightsquigarrow d_2 \rightsquigarrow \cdots \rightsquigarrow d_i \rightsquigarrow d_{i+1} \rightsquigarrow \cdots)$$

Arquitectura de la demostración

1. Definir traducciones:

Sistema $HA^{\cong}$		**Sistema T**
término t	$\mapsto$	término t^* : Nat
fórmula A	$\mapsto$	tipo A^*
derivación d de A	$\mapsto$	término d^* : A^*

2. Verificar que cada reducción de corte (en $HA^{\cong}$) corresponde a uno o múltiples pasos de reducción (en el sistema T)
3. Normalización fuerte del sistema T $\Rightarrow$ Elim. de cortes en $HA^{\cong}$

Para ello, trabajaremos en el sistema T extendido con los tipos de base Unit, Bool y las sumas $A + B$

Traducción de los términos

Definición (Traducción $t \mapsto t^*$)

Se traduce cada término t del sistema HA$^{\cong}$ en un término $t^* : \mathrm{Nat}$ del sistema T definido por:

$$
\begin{array}{rcl}
x^* & :\equiv & x \\
0^* & :\equiv & 0 \\
s(t) & :\equiv & \mathtt{S}(t^*)
\end{array}
\qquad
\begin{array}{rcl}
(\mathrm{pred}(t))^* & :\equiv & \mathtt{rec}(0,\ \lambda xz\,.\,x,\ t^*) \\
(t+u)^* & :\equiv & \mathtt{rec}(t^*,\ \lambda xz\,.\,\mathtt{S}(z),\ u^*) \\
(t\times u)^* & :\equiv & \mathtt{rec}(0,\ \lambda xz\,.\,z+t^*,\ u^*)
\end{array}
$$

Proposición (Propiedades de la traducción $t \mapsto t^*$)

Para todo término t de HA$^{\cong}$ tal que $FV(t) \subseteq \{x_1, \ldots, x_k\}$, tenemos que

1. $x_1 : \mathrm{Nat}, \ldots, x_k : \mathrm{Nat} \vdash t^* : \mathrm{Nat}$

Además, para todos términos t, t', u de HA$^{\cong}$:

2. $(t[x := u])^* \ \equiv\ t^*[x := u^*]$
3. Si $t \succ t'$ (en HA$^{\cong}$), entonces $t^* \overset{+}{\succ} t'^*$ (en el sistema T)

Traducción de las fórmulas

Definición (Traducción $A \mapsto A^*$)

Se traduce cada fórmula A del sistema HA$^{\cong}$ en un tipo A^* del sistema T definido por:

$$\begin{array}{rcl} (t = u)^* & :\equiv & \mathrm{Unit} \\ \top^* \;\equiv\; \bot^* & :\equiv & \mathrm{Unit} \\ (A \wedge B)^* & :\equiv & A^* \times B^* \\ (A \vee B)^* & :\equiv & A^* + B^* \end{array} \qquad \begin{array}{rcl} (\mathrm{null}(t))^* & :\equiv & \mathrm{Unit} \\ (A \Rightarrow B)^* & :\equiv & A^* \to B^* \\ (\forall x\, A)^* & :\equiv & \mathrm{Nat} \to A^* \\ (\exists x\, A)^* & :\equiv & \mathrm{Nat} \times A^* \end{array}$$

De vuelta, la traducción $A \mapsto A^*$ borra todo lo que tiene que ver con los términos de primer orden. Por lo tanto:

Proposición

Para todas fórmulas A, A':

- $(A[x := t])^* \equiv A^*$
- Si $A \cong A'$, entonces $A^* \equiv A'^*$

Traducción de las derivaciones (1/9)

Definición (Traducción $d \mapsto d^*$)

A cada derivación $d : (\Gamma \vdash A)$ en $\mathrm{HA}^{\cong}$ se asocia un término d^* del sistema T tal que $FV(d^*) \subseteq \{x_1, \ldots, x_k, \xi_1, \ldots, \xi_n\}$, donde

- $x_1, \ldots x_k$ son las variables libres de la derivación d,
- $\xi_1, \ldots, \xi_n$ son nuevas variables que representan las hipótesis en Γ

Formalmente:

- **Regla axioma:**

$$\left(\overline{\Gamma \vdash A}^{\ (\mathrm{ax})}\right)^* \;:\equiv\; \xi$$

donde ξ es la variable que representa la hipótesis A en el contexto Γ

Traducción de las derivaciones

Definición (Traducción $d \mapsto d^*$, continuación)

- **Introducción de $\top$:**

$$\left(\frac{}{\Gamma \vdash \top}\ (\top\text{-in})\right)^* \;:\equiv\; \langle\rangle$$

- **Eliminación de $\perp$:**

$$\left(\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash \perp\end{array}}{\Gamma \vdash A}\ (\perp\text{-el})\right)^* \;:\equiv\; (\lambda \xi^{\mathsf{Unit}} . \varepsilon_{A^*})d^*$$

donde ξ es una variable fresca y ε_{A^*} un término cerrado de tipo A^*

Traducción de las derivaciones (3/9)

Definición (Traducción $d \mapsto d^*$, continuación)

- **Introducción de $\Rightarrow$:**

$$\left(\dfrac{\begin{array}{c} \vdots\, d \\ \Gamma, A \vdash B \end{array}}{\Gamma \vdash A \Rightarrow B}\ (\Rightarrow\text{-in}) \right)^* :\equiv \ \lambda \xi^{A^*} . \, d^*$$

donde ξ es la variable que representa la hipótesis A en el contexto Γ, A

- **Eliminación de $\Rightarrow$:**

$$\left(\dfrac{\begin{array}{c} \vdots\, d \\ \Gamma \vdash A \Rightarrow B \end{array} \quad \begin{array}{c} \vdots\, d' \\ \Gamma \vdash A \end{array}}{\Gamma \vdash B}\ (\Rightarrow\text{-el}) \right)^* :\equiv \ d^* \, {d'}^*$$

Traducción de las derivaciones (4/9)

Definición (Traducción $d \mapsto d^*$, continuación)

- **Introducción de $\wedge$:**

$$\left(\dfrac{\begin{array}{c}\vdots\ d_1\\ \Gamma, A \vdash B\end{array}\quad \begin{array}{c}\vdots\ d_2\\ \Gamma, A \vdash B\end{array}}{\Gamma \vdash A \wedge B}\ (\Rightarrow\text{-in})\right)^* :\equiv \langle d_1^*, d_2^* \rangle$$

- **Eliminación de $\wedge$:**

$$\left(\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A \wedge B\end{array}}{\Gamma \vdash A}\ (\wedge\text{-el}_1)\right)^* :\equiv \pi_1(d^*)$$

$$\left(\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A \wedge B\end{array}}{\Gamma \vdash B}\ (\wedge\text{-el}_2)\right)^* :\equiv \pi_2(d^*)$$

Traducción de las derivaciones (5/9)

Definición (Traducción $d \mapsto d^*$, continuación)

- **Introducción de $\vee$:**

$$\left(\dfrac{\begin{array}{c} \vdots\ d \\ \Gamma \vdash A \end{array}}{\Gamma \vdash A \vee B}\ (\vee\text{-in}_1) \right)^* :\equiv\ \iota_1^{A^*,B^*}(d^*)$$

$$\left(\dfrac{\begin{array}{c} \vdots\ d \\ \Gamma \vdash B \end{array}}{\Gamma \vdash A \vee B}\ (\vee\text{-in}_2) \right)^* :\equiv\ \iota_2^{A^*,B^*}(d^*)$$

- **Eliminación de $\vee$:**

$$\left(\dfrac{\begin{array}{c} \vdots\ d \\ \Gamma \vdash A \vee B \end{array} \quad \begin{array}{c} \vdots\ d_1' \\ \Gamma, A \vdash C \end{array} \quad \begin{array}{c} \vdots\ d_2' \\ \Gamma, B \vdash C \end{array}}{\Gamma \vdash C}\ (\vee\text{-el}) \right)^*$$

$$:\equiv\ \text{case } d^*\ \{\iota_1(\xi_1) \mapsto d'^*_1 \mid \iota_2(\xi_2) \mapsto d'^*_2\}$$

donde ξ_1 y ξ_2 son las variables que representan A y B en los contextos Γ, A y Γ, B

Traducción de las derivaciones (6/9)

Definición (Traducción $d \mapsto d^*$, continuación)

- **Introducción de $\forall$:** (con $x \notin FV(\Gamma)$)

$$\left(\dfrac{\begin{array}{c} \vdots\ d \\ \Gamma \vdash A \end{array}}{\Gamma \vdash \forall x\, A}\ (\forall\text{-in}) \right)^* \;:\equiv\; \lambda x^{\mathrm{Nat}} . \, d^*$$

- **Eliminación de $\forall$:** (con $A' \cong A[x := t]$)

$$\left(\dfrac{\begin{array}{c} \vdots\ d \\ \Gamma \vdash \forall x\, A \end{array}}{\Gamma \vdash A'}\ (\forall\text{-el}) \right)^* \;:\equiv\; d^*\ t^*$$

Traducción de las derivaciones (7/9)

Definición (Traducción $d \mapsto d^*$, continuación)

- **Introducción de $\exists$:**

$$\left(\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A[x := t]\end{array}}{\Gamma \vdash \exists x\, A}\ (\exists\text{-in})\right)^* \;:\equiv\; \langle t^*, d^* \rangle$$

- **Eliminación de $\exists$:** $\quad$ (con $\;x \notin FV(\Gamma, B)$)

$$\left(\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash \exists x\, A\end{array} \quad \begin{array}{c}\vdots\ d'\\ \Gamma, A \vdash B\end{array}}{\Gamma \vdash B}\ (\exists\text{-el})\right)^* \;:\equiv\; \text{let } \langle x^{\mathrm{Nat}}, \xi^{A^*} \rangle = d^* \text{ in } d'^*$$

donde ξ es la variable que representa la hipótesis A en el contexto Γ, A

Recordatorio: $\quad \text{let } \langle x^A, y^B \rangle = N \text{ in } M \quad :\equiv \quad (\lambda z^{A\times B} . (\lambda x^A . \lambda y^B . M)\, \pi_1(z)\, \pi_2(z))\, N$

Traducción de las derivaciones (8/9)

Definición (Traducción $d \mapsto d^*$, continuación)

- **Introducción de $=$:** (con $t \cong t'$)

$$\left(\dfrac{}{\Gamma \vdash t = t'}\ (=\text{-in}) \right)^* \quad :\equiv \quad \langle\rangle$$

- **Eliminación de $=$:** (con $A' \cong A[x := u]$)

$$\left(\dfrac{\begin{array}{c}\vdots\ d \\ \Gamma \vdash t = u\end{array} \quad \begin{array}{c}\vdots\ d' \\ \Gamma \vdash A[x := t]\end{array}}{\Gamma \vdash A'}\ (=\text{-el}) \right)^* \quad :\equiv \quad (\lambda \xi^{\mathsf{Unit}} \,.\, d'^*)\, d^*$$

donde ξ es una variable fresca (i.e. que no aparece en d'^*)

Traducción de las derivaciones (9/9)

Definición (Traducción $d \mapsto d^*$, fin)

- **Regla de inducción:** (con $x \notin FV(\Gamma)$ y $A' \cong A[x := t]$)

$$\left(\dfrac{\dfrac{\vdots\ d_0}{\Gamma \vdash A[x := 0]} \qquad \dfrac{\vdots\ d_1}{\Gamma, A \vdash A[x := s(x)]}}{\Gamma \vdash A'}\ \text{(Nat-el)}\right)^*$$

$$\equiv\ \mathtt{rec}(d_0^*,\ \lambda x^{\mathrm{Nat}}\,.\,\lambda \xi^{A^*}\,.\,d_1^*,\ t^*)$$

donde ξ es la variable asociada a la fórmula A en el contexto Γ, A

Ejercicio. Verificar que las 2 reglas de reducción de los cortes de inducción corresponden a las 2 reglas de reducción del recursor del sistema T (combinados con unos pasos de β-reducción)

El teorema de eliminación de cortes

Proposición (Propiedades de la traducción $d \mapsto d^*$)

1. **Invariante de tipado**

   Si $d : (A_1, \dots, A_n \vdash B)$ $(\mathrm{HA}^{\cong})$, entonces:

   $$x_1 : \mathrm{Nat}, \dots, x_k : \mathrm{Nat},\ \xi_1 : A_1^*, \dots, \xi_n : A_n^* \vdash d^* : B^* \quad \text{(sistema T)}$$

   donde $x_1, \dots, x_k$ son las variables libres de la derivación d, y $\xi_1, \dots, \xi_n$ las variables que representan las hipótesis $A_1, \dots, A_n$

2. **Invariante de reducción**

   Toda reducción de corte $d \rightsquigarrow d'$ se traduce en el sistema T por uno o múltiples pasos de reducción: $d^* \succ^+ d'^*$

Demostración. Ejercicio.

Combinando el resultado anterior con el teorema de normalización fuerte para el sistema T, se concluye inmediatamente que la reducción de los cortes es fuertemente normalizante en el sistema $\mathrm{HA}^{\cong}$ □

Extracción de programas

- **Observación:** Cada derivación $\begin{array}{c}\vdots\ d\\ \vdash \forall x\,\exists y\ A(x,y)\end{array}$ (en $HA^{\cong}$)
  se traduce en un término $d^* \ :\ \mathsf{Nat} \to \mathsf{Nat} \times A^*$ (sistema T)
- Por definición de la traducción $d \mapsto d^*$, dicho término d^* asocia a cada $n : \mathsf{Nat}$ un par $d^* n \equiv \langle p, q\rangle \ :\ \mathsf{Nat} \times A^*$ formado por:
  - un testigo $p : \mathsf{Nat}$ de la existencia $\exists y\, A(n,y)$
  - un «certificado» $q : A^*$ de la misma existencia
- Por lo tanto:

Proposición (Extracción de programas en el sistema T)

Si d es une derivación del secuente $\vdash \forall x\,\exists y\ A(x,y)$ (en $HA^{\cong}$),
entonces el término $F \ :\equiv\ \lambda x^{\mathsf{Nat}}\,.\,\pi_1(d^* x) \ :\ \mathsf{Nat} \to \mathsf{Nat}$ (sistema T)
calcula una función tal que $\vdash A(n, F(n))$ para todo $n \in \mathbb{N}$

Demostración. Ejercicio.

Teorema de representación

Más generalmente:

Proposición (Extracción de programas en el sistema T)

Si d es una derivación de $\vdash \forall \vec{x} \exists y\, A(\vec{x}, y)$ (en $\mathrm{HA}^{\cong}$), entonces el término

$$F \;:\equiv\; \lambda x_1, \ldots, x_k : \mathrm{Nat} \,.\, \pi_1(d^* x_1 \cdots x_k) \;:\; \mathrm{Nat}^k \to \mathrm{Nat} \qquad \text{(sistema T)}$$

calcula una función tal que $\vdash A(\vec{n}, F(\vec{n}))$ para todo $\vec{n} = (n_1, \ldots, n_k) \in \mathbb{N}^k$

Teorema de representación

Las funciones cuya existencia es demostrable en HA son exactamente las funciones definibles en el sistema T

Demostración. Parte directa (existencia en HA $\Rightarrow$ definible en el sistema T): cf proposición anterior.

Parte recíproca (definible en el sistema T $\Rightarrow$ existencia en HA): codificación de los términos del sistema T y de la reducción en HA (ejercicio muy técnico). $\square$

Conclusión: Sistema T $=$ lenguaje de programación de HA