Introducción a la correspondencia entre pruebas y programas:

La correspondencia de Curry-Howard

Alexandre Miquel

mayo de 2021

Sistema $\lambda^{\to,\times,+}$: sintaxis (recordatorio)

Definición (Tipos)

Tipos $\quad A, B \quad ::= \quad \alpha \mid A \to B \mid A \times B \mid A + B$

Definición (Términos)

$$
\begin{array}{llll}
\textbf{Términos} & M, N & ::= & x \mid \lambda x : A \,.\, M \mid M\, N \\
& & \mid & \langle M, N \rangle \mid \pi_1(M) \mid \pi_2(M) \\
& & \mid & \iota_1^{A,B}(M) \mid \iota_2^{A,B}(M) \\
& & \mid & \mathrm{case}\ N\ \{\iota_1(x_1) \mapsto M_1 \mid \iota_2(x_2) \mapsto M_2\}
\end{array}
$$

Definición (Contextos)

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

Sistema $\lambda^{\to,\times,+}$: reducción (recordatorio)

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

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

$$\pi_1(\langle M, N\rangle) \quad \succ \quad M$$

$$\pi_2(\langle M, N\rangle) \quad \succ \quad N$$

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

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

$+$ clausura contextual

Sistema $\lambda^{\to,\times,+}$: tipado (recordatorio)

Definición (Relación $\Gamma \vdash M : A$ en el sistema $\lambda^{\to,\times,+}$)

$$\frac{}{\Gamma \vdash x : A}\ \text{si } (x{:}A)\in\Gamma$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x : A\,.\,M : A \to B} \qquad \frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash MN : B}$$

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

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

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

Sistema $\lambda^{\rightarrow,\times,+}$: tipado sin términos

Definición (Relación $\Gamma \vdash A$ en el sistema $\lambda^{\rightarrow,\times,+}$)

$$\frac{}{\Gamma \vdash A}\ \text{si } A \in \Gamma$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \qquad \frac{\Gamma \vdash A \rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \times B} \qquad \frac{\Gamma \vdash A \times B}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \times B}{\Gamma \vdash B}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A + B} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A + B}$$

$$\frac{\Gamma \vdash A + B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}$$

Sistema $\lambda^{\to,\times,+}$: equivalencia con $\mathrm{NJ}_{\mathrm{Prop}}$

Definición (Relación $\Gamma \vdash A$ en el sistema $\mathrm{NJ}_{\mathrm{Prop}}$)

$$\frac{}{\Gamma \vdash A}\ \text{si } A \in \Gamma$$

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

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

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

¿Una coincidencia?

Plan

Plan

Interpretación de Brouwer-Heyting-Kolmogorov (1/3)

Filosofía del constructivismo: El significado de una proposición A es el conjunto $\Phi(A)$ de las "evidencias" (sentido intuitivo) que A se cumple:

Una evidencia de $A \wedge B$ es...

- un par $\langle a, b \rangle$, donde $a \in \Phi(A)$ y $b \in \Phi(B)$

... entonces $\Phi(A \wedge B) = \Phi(A) \times \Phi(B)$ (Producto cartesiano)

Una evidencia de $A \vee B$ es o bien...

- de la forma $\texttt{left}(a)$, donde $a \in \Phi(A)$, o
- de la forma $\texttt{right}(b)$, donde $b \in \Phi(B)$

... entonces $\Phi(A \vee B) = \Phi(A) + \Phi(B)$ (Suma directa)

Una evidencia de $A \Rightarrow B$ es...

- una función f que transforma cada $a \in \Phi(A)$ en algún $f(a) \in \Phi(B)$

... entonces $\Phi(A \Rightarrow B) = \Phi(A) \rightarrow \Phi(B)$ ("funciones computables")

Interpretación de Brouwer-Heyting-Kolmogorov (2/3)

Filosofía del constructivismo: El significado de una proposición A es el conjunto $\Phi(A)$ de las "evidencias" (sentido intuitivo) que A se cumple:

No hay evidencia de $\bot$...
... entonces $\Phi(\bot) = \varnothing$ (Conjunto vacío)

Una evidencia de $\forall x\, A(x)$ es...

- una función f que asocia a cada objeto $x \in D$ una evidencia $a_x \in \Phi(A(x))$

... entonces $\Phi(\forall x\, A(x)) = \prod_{x \in D} \Phi(A(x))$ ("Producto dependiente")

Una evidencia de $\exists x\, A(x)$ es...

- un par $\langle x, a \rangle$, donde $x \in D$ y $a \in \Phi(A(x))$

... entonces $\Phi(\exists x\, A(x)) = \sum_{x \in D} \Phi(A(x))$ ("Suma dependiente")

Interpretación de Brouwer-Heyting-Kolmogorov (3/3)

Filosofía del constructivismo: El significado de una proposición A es el conjunto $\Phi(A)$ de las "evidencias" (sentido intuitivo) que A se cumple:

$$
\begin{array}{rcll}
\Phi(A \land B) & = & \Phi(A) \times \Phi(B) & \text{(Producto cartesiano)} \\
\Phi(A \lor B) & = & \Phi(A) + \Phi(B) & \text{(Suma directa)} \\
\Phi(A \Rightarrow B) & = & \Phi(A) \to \Phi(B) & \text{(funciones ``computables'')} \\
\Phi(\bot) & = & \varnothing & \text{(Conjunto vacío)} \\
\Phi(\top) & = & \{\bullet\} & \text{(Conjunto unitario)} \\
\Phi(\forall x\ A(x)) & = & \prod_{x \in D} \Phi(A(x)) & \text{(Producto dependiente)} \\
\Phi(\exists x\ A(x)) & = & \sum_{x \in D} \Phi(A(x)) & \text{(Suma dependiente)}
\end{array}
$$

Ejemplo típico: $\forall x\ \exists y\ A(x, y)$

La correspondencia de Curry-Howard

Una correspondencia entre...

La teoría de la demostración	**La programación funcional**
Proposición (fórmula) Prueba (derivación)	Tipo de datos Programa (o dato)
$A \wedge B, \quad A \vee B, \quad A \Rightarrow B$	$A \times B, \quad A + B, \quad A \rightarrow B$
$\underbrace{p \ : \ A}$ p es una prueba de la fórmula A	$\underbrace{p \ : \ A}$ p es un término de tipo A
Regla de deducción Verificador de prueba	Regla de tipado Verificador de tipo
Eliminación de cortes	Normalización
Prueba de un lema Teoría (enunciados + pruebas)	Sub-programa Módulo (interfaz + implem.)

El isomorfismo de Curry-Howard (1/2)

Curry-Howard (CH) = correspondencia informal entre

- los objetos y conceptos de la teoría de la demostración y
- los objetos y conceptos de la programación funcional

En particular, la correspondencia de CH induce un isomorfismo entre

- el cálculo proposicional intuicionista (sistema $\mathrm{NJ}_{\mathrm{Prop}}$, sin $\top/\bot$) y
- el cálculo lambda simplemente tipado con $\times$ y $+$ (sistema $\lambda^{\to,\times,+}$)

a través de las identificaciones:

$$A \Rightarrow B \;\equiv\; A \to B, \qquad A \wedge B \;\equiv\; A \times B, \qquad A \vee B \;\equiv\; A + B$$

El isomorfismo de Curry-Howard (2/2)

Proposición (Isomorfismo entre $\mathrm{NJ}_{\mathbf{Prop}}$ y $\lambda^{\to,\times,+}$)

Mediante las identificaciones $(\Rightarrow) \equiv (\to)$, $(\wedge) \equiv (\times)$, $(\vee) \equiv (+)$:

1. Toda derivación de $x_1 : A_1, \ldots, x_n : A_n \vdash M : B$ $(\lambda^{\to,\times,+})$
   induce una derivación de $A_1, \ldots, A_n \vdash B$ $(\mathrm{NJ}_{\mathbf{Prop}})$

   Además, los árboles subyacentes a ambas derivaciones son isomorfos

2. Toda derivación del secuente $A_1, \ldots, A_n \vdash B$ $(\mathrm{NJ}_{\mathbf{Prop}})$
   viene de una derivación $x_1 : A_1, \ldots, x_n : A_n \vdash M : B$ $(\lambda^{\to,\times,+})$
   para algún término M (único a menos de los nombres de variables)

   M es el término de prueba de la derivación del secuente $A_1, \ldots, A_n \vdash B$

Demostración. Ejercicio.

Corolario

	una fórmula A es derivable	(en $\mathrm{NJ}_{\mathbf{Prop}}$)
sii	existe un término cerrado $M : A$	(en $\lambda^{\to,\times,+}$)

Interpretación

$$x_1 : A_1, \ldots, x_n : A_n \vdash M : B$$

- **En el cálculo lambda simplemente tipado:**
  Si $x_1, \ldots, x_n$ son variables de tipos $A_1, \ldots, A_n$,
  entonces M is un término de tipo B
- **En la deducción natural intuicionista:**
  Si $x_1, \ldots, x_n$ son pruebas abstractas de las fórmulas $A_1, \ldots, A_n$,
  entonces M is una prueba de la fórmula B

$$A_1, \; \ldots, \; A_n \vdash B$$

- **En la deducción natural intuicionista:**
  Bajo las hipótesis $A_1, \ldots, A_n$, se cumple la fórmula B
- **En el cálculo lambda simplemente tipado:**
  Si $A_1, \ldots, A_n$ son tipos habitados, entonces B también lo es

Unicidad del término de prueba

- Dos derivaciones de tipado pueden corresponder a la misma derivacíon lógica:

$$\left.\begin{array}{c}\overline{x : A,\ y : A\ \vdash\ x : A}\\[2ex] \overline{x : A,\ y : A\ \vdash\ y : A}\end{array}\right\}\quad\rightsquigarrow\quad\overline{A,\ A\ \vdash\ A}$$

- **Solución:** Remplazar la regla «Axioma» por una versión marcada:

$$\overline{\Gamma, \underline{A}, \Gamma' \vdash A}$$

para distinguir las derivaciones $\overline{\underline{A}, A \vdash A}$ y $\overline{A, \underline{A} \vdash A}$

- A menos de este cambio (menor), la correspondencia se vuelve en un isomorfismo (a menos de los nombres de variables libres y ligadas)

- **Variante:** Marcar las hipótesis con nombres de variables

Ejemplos (1/4)

$$\cfrac{\cfrac{\cfrac{\cfrac{}{A \Rightarrow B,\ B \Rightarrow C,\ A \vdash B \Rightarrow C} \qquad \cfrac{\cfrac{}{A \Rightarrow B,\ B \Rightarrow C,\ A \vdash A \Rightarrow B} \quad \cfrac{}{A \Rightarrow B,\ B \Rightarrow C,\ A \vdash A}}{A \Rightarrow B,\ B \Rightarrow C,\ A \vdash B}}{A \Rightarrow B,\ B \Rightarrow C,\ A \vdash C}}{A \Rightarrow B,\ B \Rightarrow C \vdash A \Rightarrow C}$$

$$\cfrac{\cfrac{A \Rightarrow B,\ B \Rightarrow C \vdash A \Rightarrow C}{A \Rightarrow B \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}}{\vdash (A \Rightarrow B) \Rightarrow (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}$$

$$\lambda f^{A \to B} . \lambda g^{B \to C} . \lambda x^{A} . g\ (f\ x) \quad : \quad (A \to B) \to (B \to C) \to (A \to C)$$

Ejemplos (2/4)

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}}{A \wedge B \vdash B} \qquad \dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}}{A \wedge B \vdash A}}{A \wedge B \vdash B \wedge A}}{\vdash A \wedge B \Rightarrow B \wedge A}$$

$$\lambda z^{A \times B} . \langle \pi_2(z), \pi_1(z) \rangle \quad : \quad A \times B \to B \times A$$

Ejemplos (3/4)

$$\dfrac{\dfrac{}{A \vee B \vdash A \vee B} \quad \dfrac{\dfrac{}{A \vee B,\ A \vdash A}}{A \vee B,\ A \vdash B \vee A} \quad \dfrac{\dfrac{}{A \vee B,\ B \vdash B}}{A \vee B,\ B \vdash B \vee A}}{\dfrac{A \vee B \vdash B \vee A}{\vdash A \vee B \Rightarrow B \vee A}}$$

$$\lambda z^{A+B}.\,\text{case } z\ \{\iota_1(x) \mapsto \iota_2^{B,A}(x) \mid \iota_2(y) \mapsto \iota_1^{B,A}(y)\} \quad : \quad A + B \to B + A$$

Ejemplos (4/4)

Dos pruebas distintas de la misma fórmula:

$$\dfrac{\dfrac{\dfrac{\overline{A \wedge B \;\vdash\; A \wedge B}}{A \wedge B \;\vdash\; A}}{A \wedge B \;\vdash\; A \vee B}}{\vdash\; A \wedge B \Rightarrow A \vee B} \qquad \dfrac{\dfrac{\dfrac{\overline{A \wedge B \;\vdash\; A \wedge B}}{A \wedge B \;\vdash\; B}}{A \wedge B \;\vdash\; A \vee B}}{\vdash\; A \wedge B \Rightarrow A \vee B}$$

$$\lambda z^{A \times B} \,.\, \iota_1^{A,B}(\pi_1(z)) \quad : \quad A \times B \to A + B$$

$$\lambda z^{A \times B} \,.\, \iota_2^{A,B}(\pi_2(z)) \quad : \quad A \times B \to A + B$$

Cortes y redexes

Proposición (Cortes y redexes)

A través de la correspondencia entre:

- las derivaciones lógicas en el sistema $\mathsf{NJ}_{\mathsf{Prop}}$ y
- los términos tipados en el sistema $\lambda^{\rightarrow,\times,+}$

(1) Los cortes corresponden a las redexes

(2) Los pasos de reducción de cortes corresponden a los pasos de contracción de redexes

En particular:

(3) El teorema de eliminación de cortes del sistema $\mathsf{NJ}_{\mathsf{Prop}}$ es equivalente al teorema de normalización fuerte del sistema $\lambda^{\rightarrow,\times,+}$

Cortes y redexes (2/4)

- **Un corte de $\wedge$ es...**

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

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

- **... una redex de $\times$ (y viceversa):**

$$\begin{array}{lcl}\pi_1(\langle M_1, M_2\rangle) & \succ & M_1\\ \pi_2(\langle M_1, M_2\rangle) & \succ & M_2\end{array}$$

Cortes y redexes (3/4)

- **Un corte de $\Rightarrow$ es...**

$$\dfrac{\dfrac{\genfrac{}{}{0pt}{}{\vdots\; d}{\Gamma, A \vdash B}}{\Gamma \vdash \color{red}{A \Rightarrow B}}\,(\Rightarrow\text{-in}) \qquad \genfrac{}{}{0pt}{}{\vdots\; d'}{\Gamma \vdash A}}{\Gamma \vdash B}\,(\Rightarrow\text{-el}) \qquad \rightsquigarrow \qquad \begin{array}{c} \vdots\; d' \\ \Gamma \vdash A \\ \vdots\; d[\mathrm{ax}(A){:=}d'] \\ \Gamma \vdash B \end{array}$$

- **... una redex de $\rightarrow$ (y viceversa):**

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

Cortes y redexes

- **Un corte de $\vee$ es...**

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A\end{array}}{\Gamma \vdash {\color{red}A \vee B}}\ (\vee\text{-in}_1) \quad \begin{array}{c}\vdots\ d'_1\\ \Gamma, A \vdash C\end{array} \quad \begin{array}{c}\vdots\ d'_2\\ \Gamma, B \vdash C\end{array}}{\Gamma \vdash C}\ (\vee\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d\\ \Gamma \vdash A\\ \vdots\ d'_1[\text{ax}(A){:=}d]\\ \Gamma \vdash C\end{array}$$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash B\end{array}}{\Gamma \vdash {\color{red}A \vee B}}\ (\vee\text{-in}_2) \quad \begin{array}{c}\vdots\ d'_1\\ \Gamma, A \vdash C\end{array} \quad \begin{array}{c}\vdots\ d'_2\\ \Gamma, B \vdash C\end{array}}{\Gamma \vdash C}\ (\vee\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d\\ \Gamma \vdash B\\ \vdots\ d'_2[\text{ax}(B){:=}d]\\ \Gamma \vdash C\end{array}$$

- **... una redex de $+$ (y viceversa):**

$$\text{case } \iota_1^{A,B}(M)\ \{\iota_1(x_1) \mapsto M'_1 \mid \iota_2(x_2) \mapsto M'_2\} \quad \succ \quad M'_1[x_1 := M]$$

$$\text{case } \iota_2^{A,B}(M)\ \{\iota_1(x_1) \mapsto M'_1 \mid \iota_2(x_2) \mapsto M'_2\} \quad \succ \quad M'_2[x_2 := M]$$

Extensión de la correspondencia a las unidades

- **Del lado de la lógica:**

Fórmulas: $A, B \quad ::= \quad \cdots \quad | \quad \top \quad | \quad \bot$

Permite definir la negación: $\neg A \; :\equiv \; A \Rightarrow \bot$

$+$ reglas de deducción: $\dfrac{}{\Gamma \vdash \top}\ (\top\text{-in}) \qquad \dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}\ (\bot\text{-el})$

- **Del lado de la programación:**

Tipos: $A, B \quad ::= \quad \cdots \quad | \quad \mathbf{1} \quad | \quad \mathbf{0}$

Términos: $M, N \quad ::= \quad \cdots \quad | \quad \langle\rangle \quad | \quad \mathrm{case}_A\ M\ \{\}$

$+$ reglas de tipado: $\dfrac{}{\Gamma \vdash \langle\rangle : \mathbf{1}} \qquad \dfrac{\Gamma \vdash M : \mathbf{0}}{\Gamma \vdash \mathrm{case}_A\ M\ \{\} : A}$

- **Obs.:** La extensión del sistema $\lambda^{\to,\times,+}$ con los tipos $\mathbf{0}$ y $\mathbf{1}$ no introduce ninguna nueva regla de reducción: el sistema obtenido sigue cumpliendo el teorema de normalización fuerte (Ejercicio: demostrarlo)

Plan

Recordatorio: sintaxis del sistema NJ

Dado un vocabulario $\mathcal{V}$:

Definición (Términos y fórmulas)

$$
\begin{array}{llcl}
\textbf{Términos} & t, u & ::= & x \mid f(t_1, \ldots, t_k) \\
\textbf{Fórmulas} & A, B, C & ::= & p(t_1, \ldots, t_k) \mid \top \mid \bot \\
& & & \mid A \wedge B \mid A \vee B \mid A \Rightarrow B \\
& & & \mid \forall x\, A \mid \exists x\, A
\end{array}
$$

donde x es cualquier variable,
$f \in \mathcal{V}$ es cualquier símbolo de función de aridad k y
$p \in \mathcal{V}$ es cualquier símbolo de predicado de aridad k

Abreviaturas: $\neg A \;:\equiv\; A \Rightarrow \bot, \qquad A \Leftrightarrow B \;:\equiv\; (A \Rightarrow B) \wedge (B \Rightarrow A)$

Recordatorio: reglas de deducción del sistema NJ (1/2)

- Reglas del cálculo proposicional intuicionista:

	Introducción	Eliminación
(Axioma)	$\dfrac{}{\Gamma \vdash A}$ si $A \in \Gamma$	
$(\Rightarrow)$	$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$	$\dfrac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}$
$(\wedge)$	$\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$	$\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$ $\quad$ $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$
$(\vee)$	$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$ $\quad$ $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$	$\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$
$(\top)$	$\dfrac{}{\Gamma \vdash \top}$	(sin regla de eliminación)
$(\bot)$	(sin regla de introducción)	$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}$

Recordatorio: reglas de deducción del sistema NJ (2/2)

- Reglas de introducción y de eliminación de los cuantificadores:

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

- Reglas de introducción y de eliminación de la igualdad:

$(=)$	$\dfrac{}{\Gamma \vdash t = t}$	$\dfrac{\Gamma \vdash t = u \qquad \Gamma \vdash A[x := t]}{\Gamma \vdash A[x := u]}$

Recordatorio: reducción de los cortes en NJ (1/5)

Cortes de $\wedge$:

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

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

Recordatorio: reducción de los cortes en NJ (2/5)

Corte de $\Rightarrow$:

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

Recordatorio: reducción de los cortes en NJ (3/5)

Cortes de $\vee$:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\; d\\ \Gamma \vdash A\end{array}}{\Gamma \vdash \color{red}{A \vee B}}\,(\vee\text{-in}_1) \qquad \begin{array}{c}\vdots\; d'_1\\ \Gamma, A \vdash C\end{array} \qquad \begin{array}{c}\vdots\; d'_2\\ \Gamma, B \vdash C\end{array}}{\Gamma \vdash C}\,(\vee\text{-el}) \qquad \rightsquigarrow \qquad \begin{array}{c}\vdots\; d\\ \Gamma \vdash A\\ \vdots\; d'_1[\mathsf{ax}(A){:=}d]\\ \Gamma \vdash C\end{array}$$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\; d\\ \Gamma \vdash B\end{array}}{\Gamma \vdash \color{red}{A \vee B}}\,(\vee\text{-in}_2) \qquad \begin{array}{c}\vdots\; d'_1\\ \Gamma, A \vdash C\end{array} \qquad \begin{array}{c}\vdots\; d'_2\\ \Gamma, B \vdash C\end{array}}{\Gamma \vdash C}\,(\vee\text{-el}) \qquad \rightsquigarrow \qquad \begin{array}{c}\vdots\; d\\ \Gamma \vdash B\\ \vdots\; d'_2[\mathsf{ax}(B){:=}d]\\ \Gamma \vdash C\end{array}$$

Corte de $\top/\bot$: ninguno

Recordatorio: reducción de los cortes en NJ (4/5)

Corte de $\forall$: $(\text{con} \quad x \notin FV(\Gamma))$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash A\end{array}}{\Gamma \vdash \color{red}{\forall x\, A}}\ (\forall\text{-in})}{\Gamma \vdash A[x := t]}\ (\forall\text{-el}) \quad \rightsquigarrow \quad \begin{array}{c}\vdots\ d[x{:=}t]\\ \Gamma \vdash A[x := t]\end{array}$$

Corte de $\exists$: $(\text{con} \quad x \notin FV(\Gamma, B))$

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

Recordatorio: reducción de los cortes en NJ (5/5)

Corte de $=$:

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

Eliminación de cortes en el sistema NJ

Ahora, tenemos todas las herramientas para demostrar el:

Teorema (Eliminación de cortes en NJ)

El sistema formado por las 8 reglas de reducción de cortes del sistema NJ 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 NJ		**Sistema $\lambda^{\to,\times,+}$**
fórmula A	$\mapsto$	tipo A^*
derivación d de A	$\mapsto$	término $d^* : A^*$

2. Verificar que cada reducción de corte (en NJ) corresponde a uno o múltiples pasos de reducción (en $\lambda^{\to,\times,+}$)
3. Normalización fuerte de $\lambda^{\to,\times,+}$ $\Rightarrow$ Eliminación de cortes en NJ

Para ello, trabajaremos en el sistema $\lambda^{\to,\times,+}$ enriquecido con:

- una constante inerte $\boldsymbol{c} : \alpha$ (donde α es el único tipo de base)
- una constante inerte $\boldsymbol{r}_A : \alpha \to A$ para cada tipo A

Obs.: Introducir constantes inertes (i.e. sin reglas de reducción) nunca afecta la propiedad de normalización fuerte de un sistema. Siempre se pueden ver tales constantes como variables declaradas implícitamente "en el origen del mundo"

Traducción de las fórmulas

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

$$
\begin{array}{rcl}
(p(t_1,\ldots,t_k))^* & :\equiv & \alpha \\
\top^* \ \equiv \ \bot^* & :\equiv & \alpha \\
(A \wedge B)^* & :\equiv & A^* \times B^* \\
(A \vee B)^* & :\equiv & A^* + B^* \\
(A \Rightarrow B)^* & :\equiv & A^* \to B^* \\
(\forall x\, A)^* & :\equiv & \alpha \to A^* \\
(\exists x\, A)^* & :\equiv & \alpha \times A^*
\end{array}
$$

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

Proposición

Para toda fórmula A: $(A[x := t])^* \equiv A^*$

Traducción de las derivaciones

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

A cada derivación $d : (\Gamma \vdash A)$ en el sistema NJ se asocia un término d^* del sistema $\lambda^{\to,\times,+}$ tal que $FV(d^*) \subseteq \{\xi_1, \ldots, \xi_n\}$, donde $\xi_1, \ldots, \xi_n$ son variables que representan las hipótesis en Γ

- **Regla axioma:**

$$\left(\frac{}{\Gamma \vdash A}\,(\text{ax})\right)^* \;:\equiv\; \xi$$

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

- **Introducción de $\top$:**

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

- **Eliminación de $\bot$:**

$$\left(\frac{\begin{array}{c}\vdots\, d\\ \Gamma \vdash \bot\end{array}}{\Gamma \vdash A}\,(\bot\text{-el})\right)^* \;:\equiv\; \boldsymbol{r}_{A^*}\; d^*$$

Traducción de las derivaciones (2/7)

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 (3/7)

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 (4/7)

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 (5/7)

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

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

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

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

- **Eliminación de $\forall$:**

$$\left(\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash \forall x\, A\end{array}}{\Gamma \vdash A[x := t]}\ (\forall\text{-el})\right)^* :\equiv\ d^*\ \boldsymbol{c}$$

Traducción de las derivaciones (6/7)

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

- **Introducción de $\exists$:**

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

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

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

donde z es una variable fresca (i.e. que no aparece en d'^*), y donde ξ es la variable que representa la hipótesis A en el contexto Γ, A

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

Traducción de las derivaciones (7/7)

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

- **Introducción de $=$:**

$$\left(\overline{\Gamma \vdash t = t}\ {}^{(=\text{-in})} \right)^* \;:\equiv\; \boldsymbol{c}$$

- **Eliminación de $=$:**

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

donde ξ es una variable que no aparece en d'^*

El teorema de eliminación de cortes

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

1. **Invariante de tipado**

   Para toda derivación $d : (A_1, \ldots, A_n \vdash B)$ (en NJ)
   tenemos que $\xi_1 : A_1^*, \ldots, \xi_n : A_n^* \vdash d^* : B^*$ (en $\lambda^{\to,\times,+}$)

   donde $\xi_1, \ldots, \xi_n$ son las variables que representan las hipótesis $A_1, \ldots, A_n$

2. **Invariante de reducción**

   Toda reducción de corte $d \rightsquigarrow d'$ se traduce en el sistema $\lambda^{\to,\times,+}$ 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 $\lambda^{\to,\times,+}$, se concluye inmediatamente que la reducción de los cortes es fuertemente normalizante en el sistema NJ $\square$