Paradigmas de Programación

Correspondencia de Curry-Howard Puntos fijos y recursión

1er cuatrimestre de 2025 Departamento de Computación Facultad de Ciencias Exactas y Naturales Universidad de Buenos Aires

Sistema de tipos para el cálculo- λ^b

Vamos a omitir las reglas para booleanos.

Sistema de tipos para el cálculo- λ

```
Reglas de tipadoDeducción natural
    \overline{\Gamma, x}: \quad \tau \vdash x: \quad \tau T-VARax
     \frac{\Gamma, x: \quad \tau \vdash M: \quad \sigma}{\Gamma \vdash \lambda x: \sigma.M: \quad \tau \to \sigma} \text{T-ABS} \to_{i}
     \frac{\Gamma \vdash M : \qquad \tau \to \sigma \qquad \qquad \Gamma \vdash N : \qquad \tau}{\Gamma \vdash MN : \qquad \sigma} \text{T-APP} \to_{e}
```

- ► Ignoremos los términos
- Las reglas de tipado se corresponden con reglas de deducción natural.

Correspondencia de Curry

Curry y Feys observaron que si se lee el tipo $au o \sigma$ como una implicación $au \Rightarrow \sigma$:

la regla de tipado de la aplicación de una función es la regla **modus ponens**

Pruebas y Programas

```
\begin{array}{ccc} \mathsf{F\acute{o}rmulas} & \leftrightarrow & \mathsf{T\acute{i}pos} \\ \mathsf{Demostraciones} & \leftrightarrow & \mathsf{T\acute{e}rminos} \end{array}
```

Un juicio $\vdash \sigma$ es derivable si y sólo si el tipo σ está habitado, esto es, existe un término M tal que $\vdash M : \tau$ es derivable.

Ejemplo

¿Es derivable $\vdash \sigma \Rightarrow \sigma$?

Si, por ejemplo:

$$\frac{\overline{\sigma \vdash \sigma}^{\mathsf{ax}}}{\vdash \sigma \Rightarrow \sigma} \Rightarrow_{\mathsf{i}}$$

Corresponde al siguiente juicio de tipado:

$$\frac{\overline{x:\sigma \vdash x:\sigma}^{\text{T-VAR}}}{\vdash \lambda x:\sigma.x:\sigma \rightarrow \sigma}^{\text{T-ABS}}$$

El **término** $\lambda x : \sigma.x$ se asocia con la **prueba** de $\sigma \Rightarrow \sigma$ que se muestra en la parte superior

Ejemplo

¿Es derivable $\vdash \sigma \Rightarrow \sigma$?

También existe la siguiente prueba

$$\frac{\overline{\sigma \Rightarrow \sigma \vdash \sigma \Rightarrow \sigma}^{\mathsf{ax}}}{\vdash (\sigma \Rightarrow \sigma) \Rightarrow \sigma \Rightarrow \sigma} \Rightarrow_{i} \frac{\overline{\sigma \vdash \sigma}^{\mathsf{ax}}}{\vdash \sigma \Rightarrow \sigma} \Rightarrow_{i} \\ \vdash \sigma \Rightarrow \sigma$$

Corresponde al siguiente juicio de tipado:

$$\frac{\frac{}{x:\sigma \to \sigma \vdash x:\sigma \to \sigma}^{\text{T-VAR}}}{\vdash \lambda x:\sigma \to \sigma.x:(\sigma \to \sigma) \to \sigma \to \sigma}^{\text{T-ABS}} \quad \frac{\frac{}{y:\sigma \vdash y:\sigma}^{\text{T-VAR}}}{\vdash \lambda y:\sigma \to \sigma}^{\text{T-ABS}}}{\vdash \lambda y:\sigma \to \sigma}^{\text{T-ABS}}$$

$$\vdash (\lambda x:\sigma \to \sigma.x)(\lambda y:\sigma.y):\sigma \to \sigma$$

El **término** $(\lambda x : \sigma \to \sigma.x)(\lambda y : \sigma.y)$ se asocia con la **prueba** que se muestra en la parte superior.

Ejemplo

; Es derivable $\vdash \sigma \Rightarrow \sigma$?

También existe la siguiente prueba

$$\frac{\overline{\sigma \vdash \sigma} \stackrel{\mathsf{ax}}{\Rightarrow}_{i}}{\sigma \vdash \sigma \Rightarrow \sigma} \Rightarrow_{i} \frac{\overline{\sigma \vdash \sigma} \stackrel{\mathsf{ax}}{\Rightarrow}_{e}}{\sigma \vdash \sigma} \Rightarrow_{e} \\
 \frac{\sigma \vdash \sigma \Rightarrow \sigma}{\vdash \sigma \Rightarrow \sigma} =$$

$$\frac{\overline{x : \sigma, y : \sigma \vdash y : \sigma}^{\text{T-VAR}}}{x : \sigma \vdash \lambda y : \sigma \cdot y : \sigma \to \sigma}^{\text{T-ABS}} \qquad \overline{x : \sigma \vdash x : \sigma}^{\text{T-VAR}}$$

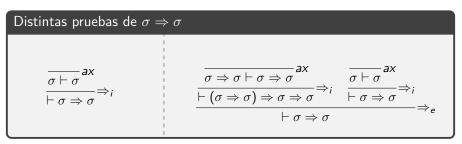
$$\frac{x : \sigma \vdash \lambda y : \sigma \cdot y : \sigma \to \sigma}{x : \sigma \vdash (\lambda y : \sigma \cdot y) x : \sigma}^{\text{T-APP}}$$

$$\vdash \lambda x : \sigma \cdot (\lambda y : \sigma \cdot y) x : \sigma \to \sigma$$

El **término** $\lambda x : \sigma.(\lambda y : \sigma.y)x$ se asocia con la **prueba** que se muestra en la parte superior.

Pruebas vs términos

- Una fórmula puede tener muchas pruebas distintas.
- ▶ Distintas pruebas corresponden a distintos juicios de tipado, es decir distintos términos.
- Notar que algunas pruebas de la misma proposición son mas complejas que otras:



Correspondencia de Curry-Howard

William Alvin Howard extendió la correspondencia:

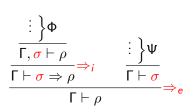
- Tratando los restantes conectivos lógicos.
- lacktriangle Usando el cálculo- λ en lugar de la lógica combinatoria.
- Mostrando una correspondencia entre la simplificación de pruebas y la computación.

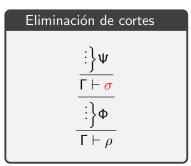
Simplificación de pruebas

Corte (cut)

Un corte es una "vuelta" innecesaria en una demostración.

- Está dado por una regla de introducción seguida inmediatamente de una regla de eliminación.
- Involucra a una fórmula de corte que no es subfórmula de la tesis.





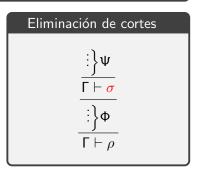
Simplificación de pruebas

Eliminación de cortes (cut-elimination)

Reescribir una prueba de manera tal que no tenga cortes:

▶ Eliminamos σ reemplazando cada uso σ en la prueba de ρ por una copia de la prueba de σ .

$$\frac{\vdots }{\Gamma, \sigma \vdash \rho} \xrightarrow{\vdots} \qquad \vdots \\ \frac{\Gamma \vdash \sigma \Rightarrow \rho}{\Gamma \vdash \rho} \Rightarrow_{i} \qquad \vdots \\ \frac{\vdots}{\Gamma \vdash \sigma} \Rightarrow_{e}$$



Computación como simplificación de pruebas

Eliminación de cortes y reducción β

Un paso de eliminación de cortes se corresponde con un paso de cómputo (aplicación de la regla β o E-APPABS).

$$\frac{\vdots}{\Gamma, \tau \vdash M : \rho} \\
\frac{\Gamma \vdash \lambda x : \tau.M : \tau \to \rho}{\Gamma \vdash (\lambda x : \tau.M) N : \rho} \xrightarrow{\Gamma \vdash ABS} \frac{\vdots}{\Gamma \vdash N : \tau} \\
\frac{\vdots}{\Gamma \vdash (\lambda x : \tau.M) N : \rho} \\
\frac{\vdots}{\Gamma \vdash M \{x := N\} : \rho}$$

Conjunción

$$\frac{\Gamma \vdash \quad \tau \quad \Gamma \vdash \quad \sigma}{\tau \vdash \quad \tau \land \sigma} \land_{i}$$

$$\frac{\Gamma \vdash \quad \tau \land \sigma}{\Gamma \vdash \quad \tau} \land_{e_{1}} \quad \frac{\Gamma \vdash \quad \tau \land \sigma}{\Gamma \vdash \quad \sigma} \land_{e_{2}}$$

Producto

$$\frac{\Gamma \vdash M : \tau \qquad \Gamma \vdash N : \sigma}{\tau \vdash \langle M, N \rangle : \tau \times \sigma}$$

$$\frac{\Gamma \vdash M : \tau \times \sigma}{\Gamma \vdash \mathsf{fst}(M) : \tau} \qquad \frac{\Gamma \vdash M : \tau \times \sigma}{\Gamma \vdash \mathsf{snd}(M) : \sigma}$$

Conjunción: corte

$$\frac{\vdots}{\Gamma \vdash \tau} \quad \frac{\vdots}{\Gamma \vdash \sigma} \\
\frac{\Gamma \vdash \tau}{\Gamma \vdash \tau} \quad \frac{\tau \land \sigma}{\tau} \land_{e_{1}}$$

$$\frac{\vdots}{\Gamma \vdash \tau} \quad \frac{\vdots}{\Gamma \vdash \sigma} \\
\frac{\Gamma \vdash \tau}{\Gamma \vdash \sigma} \quad \frac{\tau \land \sigma}{\tau} \land_{e_{2}}$$

Conjunción: eliminación de corte

$$\frac{\vdots}{\Gamma \vdash \tau} \frac{\vdots}{\Gamma \vdash \sigma} \xrightarrow{\Gamma \vdash \sigma} \wedge_{i} \rightarrow \frac{\vdots}{\Gamma \vdash \tau} \xrightarrow{\Gamma \vdash \sigma} \wedge_{e_{1}} \qquad \frac{\vdots}{\Gamma \vdash \tau} \xrightarrow{\Gamma \vdash \sigma} \wedge_{i} \rightarrow \frac{\vdots}{\Gamma \vdash \sigma} \xrightarrow{\Gamma \vdash \sigma} \wedge_{e_{2}} \rightarrow \frac{\vdots}{\Gamma \vdash \sigma}$$

Producto: reducción

$$\begin{array}{c|c} \vdots & \vdots \\ \hline {\Gamma \vdash M : \tau} & \hline {\Gamma \vdash N : \sigma} \\ \hline {\Gamma \vdash \langle M, N \rangle : \tau \times \sigma} \\ \hline {\Gamma \vdash \mathsf{fst}(\langle), M \rangle N : \tau} \\ \hline \vdots & \vdots \\ \hline {\Gamma \vdash M : \tau} & \hline {\Gamma \vdash N : \sigma} \\ \hline {\Gamma \vdash \langle M, N \rangle : \tau \times \sigma} \\ \hline {\Gamma \vdash \mathsf{snd}(\langle), M \rangle N : \sigma} \\ \hline \end{array} \rightarrow \begin{array}{c} \vdots \\ \hline {\Gamma \vdash N : \sigma} \\ \hline \hline {\Gamma \vdash \mathsf{N} : \sigma} \\ \hline \end{array}$$

Cálculo- λ^{\times} — resumen

Tipos y términos

$$au, \sigma, \dots ::= \dots \mid \tau \times \sigma$$

 $M, N, \dots ::= \dots \mid \langle M, N \rangle \mid \mathsf{fst}(M) \mid \mathsf{snd}(M)$

Reglas de tipado

$$\frac{\Gamma \vdash M : \tau \quad \Gamma \vdash N : \sigma}{\Gamma \vdash \langle M, N \rangle : \tau \times \sigma} \times_{i}$$

$$\frac{\Gamma \vdash M : \tau \times \sigma}{\Gamma \vdash \mathsf{fst}(M) : \tau} \times_{e_{1}} \frac{\Gamma \vdash M : \tau \times \sigma}{\Gamma \vdash \mathsf{snd}(M) : \tau} \times_{e_{2}}$$

Cálculo- λ^{\times} — resumen

Cálculo- λ^{\times} — resumen

Valores

$$V, W, \ldots ::= \ldots \mid \langle V, W \rangle$$

Reglas de cómputo

$$\overline{\mathsf{fst}(\langle V,W\rangle) \to V}^{\text{E-FSTPAIR}} \quad \overline{\mathsf{snd}(\langle V,W\rangle) \to W}^{\text{E-SNDPAIR}}$$

Reglas de congruencia

$$\frac{M \to M'}{\langle M, N \rangle \to \langle M', N \rangle} \text{E-PAIR1} \qquad \frac{N \to N'}{\langle V, N \rangle \to \langle V, N' \rangle} \text{E-PAIR2}$$

$$\frac{M \to M'}{\text{fst}(M) \to \text{fst}(M')} \text{E-FST} \qquad \frac{M \to M'}{\text{snd}(M) \to \text{snd}(M')} \text{E-SND}$$

Disyunción

Suma

$$\frac{\Gamma \vdash M : \tau}{\Gamma \vdash \mathsf{left}^{\sigma}(M) : \tau + \sigma} \qquad \frac{\Gamma \vdash M : \sigma}{\Gamma \vdash \mathsf{right}^{\tau}(M) : \tau + \sigma}$$

$$\frac{\Gamma \vdash M : \tau + \sigma \qquad \Gamma, x : \tau \vdash M : \rho \qquad \Gamma, x : \tau \vdash N : \rho}{\Gamma \vdash \mathsf{case} \ M \left\{ \mathsf{left}(x) \mapsto N \ \| \ \mathsf{right}(x) \mapsto P \right\} : \rho}$$

Disyunción: corte

$$\begin{array}{c|c} \vdots \\ \hline {\Gamma \vdash M : \tau} \\ \hline \\ \hline {\Gamma \vdash \mathsf{left}^{\sigma}(M) : \tau + \sigma}^{\bigvee_{i_2}} & \overline{\Gamma, x : \tau \vdash N : \rho} & \overline{\Gamma, x : \sigma \vdash P : \rho} \\ \hline \\ {\Gamma \vdash \mathsf{case} \; \mathsf{left}^{\sigma}(M) \, \{\mathsf{left}(x) \mapsto N \; \| \; \mathsf{right}(x) \mapsto P\} : \rho} \\ \hline \end{array} \\ \vee_e \\$$

Suma: reducción (1)

```
 \frac{ \overline{\Gamma \vdash M : \tau} }{ \frac{\Gamma \vdash \mathsf{left}^\sigma(M) : \tau + \sigma}{\Gamma \vdash \mathsf{case} \; \mathsf{left}^\sigma(M) \, \{ \mathsf{left}(x) \mapsto N \; \| \; \mathsf{right}(x) \mapsto P \} : \rho} }{ \Gamma \vdash \mathsf{case} \; \mathsf{left}^\sigma(M) \, \{ \mathsf{left}(x) \mapsto N \; \| \; \mathsf{right}(x) \mapsto P \} : \rho } \vee_e 
                                                                                                                                                                                                                                                                                 \Gamma \vdash N\{x := M\} : \rho
```

Suma: reducción (2)

```
\frac{\overline{\Gamma \vdash M : \sigma}}{\frac{\Gamma \vdash \mathsf{right}^\tau(M) : \tau + \sigma}{\Gamma \vdash \mathsf{case} \ \mathsf{right}^\sigma(M) \, \{\mathsf{left}(x) \mapsto N \parallel \mathsf{right}(x) \mapsto P\} : \rho}}{\Gamma \vdash \mathsf{case} \ \mathsf{right}^\sigma(M) \, \{\mathsf{left}(x) \mapsto N \parallel \mathsf{right}(x) \mapsto P\} : \rho} \vee_e
                                                                                                                                                                                                                                                                              \Gamma \vdash M : \tau
                                                                                                                                                                                                                                                         \Gamma \vdash P\{x := M\} : \rho
```

Cálculo- λ^+ : resumen

Tipos y términos

Reglas de tipado

$$\frac{\Gamma \vdash M : \tau}{\Gamma \vdash \mathsf{left}^{\sigma}(M) : \tau + \sigma} +_{i_1} \frac{\Gamma \vdash M : \sigma}{\Gamma \vdash \mathsf{right}^{\tau}(M) : \tau + \sigma} +_{i_2}$$

$$\frac{\Gamma \vdash M : \tau + \sigma \quad \Gamma, x : \tau \vdash N : \rho \quad \Gamma, y : \sigma \vdash P : \rho}{\Gamma \vdash \mathsf{case} \ M \left\{ \mathsf{left}(x) \mapsto N \ \| \ \mathsf{right}(y) \mapsto P \right\} : \rho} +_{e}$$

Cálculo- λ^+ : resumen

Valores

$$V,W,\ldots:=\ldots\mid \mathsf{left}^{ au}(V)\mid \mathsf{right}^{ au}(V)$$

Reglas de cómputo

$$\mathsf{case}\;\mathsf{left}^{\scriptscriptstyle T}(V)\,\{\mathsf{left}(\mathsf{x})\mapsto \mathit{M}\;\|\;\mathsf{right}(y)\mapsto \mathit{N}\}\to \mathit{M}\{\mathsf{x}:=V\}$$

$$\overline{\mathsf{case}\;\mathsf{right}^{\scriptscriptstyle\mathsf{T}}(V)\,\{\mathsf{left}(\mathsf{x})\mapsto \mathit{M}\;\|\;\mathsf{right}(y)\mapsto \mathit{N}\}\to \mathit{N}\{y:=V\}}^{\,\mathrm{E-CASER}}$$

Reglas de congruencia

$$\frac{M \to M'}{\mathsf{left}^{\tau}(M) \to \mathsf{left}^{\tau}(M')} \to \mathsf{E-INL} \qquad \frac{M \to M'}{\mathsf{right}^{\tau}(M) \to \mathsf{right}^{\tau}(M')} \to \mathsf{E-INR}$$

$$\frac{M \to M'}{\text{case } M \left\{ \text{left}(x) \mapsto N \parallel \text{right}(y) \mapsto P \right\}} \text{E-CASE}$$
$$\to \text{case } M' \left\{ \text{left}(x) \mapsto N \parallel \text{right}(y) \mapsto P \right\}$$

Absurdo

$$\frac{\Gamma \vdash \qquad \perp}{\Gamma \vdash \qquad \qquad \tau} \perp_e$$

Absurdo

```
\frac{\Gamma \vdash M : \bot}{\Gamma \vdash \mathsf{case}^{\tau} \ M\{\} : \tau} \bot_{e}
```

- Notar que no hay constructores para el tipo ⊥.
- ► El tipo ⊥ es el tipo vacío (sin habitantes).
- Se puede definir como un tipo de datos algebraico sin constructores.
- ▶ El eliminador es un case con 0 ramas.
- Las ocurrencias de case^{τ} $M\{\}$ siempre corresponden a situaciones imposibles (código inalcanzable).

Cálculo- λ^{\perp} : resumen

Tipos y términos

$$au, \sigma, \dots ::= \dots \mid \perp$$

 $M, N, \dots ::= \dots \mid \mathsf{case}^{\tau} M\{\}$

Reglas de tipado

$$\frac{\Gamma \vdash M : \bot}{\Gamma \vdash \mathsf{case}^{\tau} \ M\{\} : \tau} \bot_{\mathsf{e}}$$

No se extienden los valores ni las reglas de reducción.

Tipo Unit

Se puede considerar una extensión de \mathbf{NJ} con la fórmula \top ("verdadero"):

$$\overline{\Gamma \vdash \top}^{\top_i}$$

ightharpoonup El cálculo- $\lambda^{ op}$ resulta de la siguiente extensión:

$$\sigma, \tau, \dots$$
 ::= ... | \top M, N, P, \dots ::= ... | \star

► Con una única regla de tipado:

$$\overline{\Gamma \vdash \star : \top}^{\top_i}$$

► El tipo ⊤ es un tipo algebraico con un único constructor ⋆.

Propiedades

El cálculo- $\lambda^{\times,+,\perp,\top}$ tiene buenas propiedades:

- 1. Unicidad de tipos. Si $\Gamma \vdash M : \tau$ y $\Gamma \vdash M : \sigma$ son derivables, entonces $\tau = \sigma$.
- 2. Weakening + Strengthening. Si $\Gamma \vdash M : \tau$ es derivable y $fv(M) \subseteq dom(\Gamma \cap \Gamma')$ entonces $\Gamma' \vdash M : \tau$ es derivable.
- 3. Determinismo. Si $M \rightarrow N_1$ y $M \rightarrow N_2$ entonces $N_1 = N_2$.
- 4. Preservación de tipos. Si $\vdash M : \tau \ y \ M \to N$ entonces $\vdash N : \tau$.
- 5. Progreso. Si \vdash M : τ entonces:
 - 5.1 O bien M es un valor.
 - 5.2 O bien existe N tal que $M \rightarrow N$.
- 6. Terminación. Si $\vdash M : \tau$, entonces no hay una cadena infinita de pasos:

$$M \rightarrow M_1 \rightarrow M_2 \rightarrow \dots$$

Correspondencia de Curry-Howard

Teorema (Correspondencia de Curry-Howard)

Son equivalentes:

- 1. $\tau_1, \ldots, \tau_n \vdash \sigma$ es derivable en **NJ**
- 2. Existe un término M tal que $x_1 : \tau_1, \dots, x_n : \tau_n \vdash M : \sigma$.

Nota

En el teorema de arriba identificamos tácitamente los símbolos:



Consistencia de la lógica

La relación entre reducción y pruebas permite concluir que la lógica es consistente.

Corolario

El juicio $\vdash \bot$ **no** es derivable en NJ.

Se obtiene a partir del siguiente razonamiento:

- ▶ Debe existir M, tal que $\vdash M : \bot$.
- Por terminación y preservación de tipos, debería existir un valor V, tal que ⊢ V : ⊥. Por analisis de casos en los posibles valores, se puede concluir que no existe.

Sobre la negación

La negación se puede codificar como:

$$\neg \sigma \equiv (\sigma \to \bot)$$

- Notar que la regla:
 - ightharpoonup \neg_i corresponde $a \Rightarrow_i$
 - ightharpoonup \neg_e corresponde $a \Rightarrow_e$
- No hay necesidad de extender el cálculo- λ con negación.

Sobre los booleanos

Los ignoramos porque se pueden codificar.

Booleanos como sumas

```
\begin{aligned} \mathsf{Bool} &\equiv \top + \top \\ \mathsf{true} &\equiv \mathsf{left}^\top(\star) \\ \mathsf{false} &\equiv \mathsf{right}^\top(\star) \\ \mathsf{if} \ \mathit{M} \ \mathsf{then} \ \mathit{N} \ \mathsf{else} \ \mathit{P} &\equiv \mathsf{case} \ \mathit{M} \ \{\mathsf{left}(\_) \mapsto \mathit{N} \ \| \ \mathsf{right}(\_) \mapsto \mathit{P} \} \end{aligned}
```

Recursión

Extendemos la sintaxis con un nuevo operador:

$$M ::= \dots \mid \text{fix } M$$

▶ No se precisan nuevos tipos pero sí una regla de tipado.

$$\frac{\Gamma \vdash M : \tau \to \tau}{\Gamma \vdash \text{fix } M : \tau} \text{T-FIX}$$

Semántica operacional small-step

No hay valores nuevos pero sí reglas de evaluación nuevas.

$$\frac{M \to M'}{\text{fix } M \to \text{fix } M'} \text{E-FIX}$$

$$\overline{\text{fix } (\lambda x : \tau. M)} \rightarrow M\{x := \text{fix } (\lambda x : \tau. M)\}$$
 E-FIXBETA

Ejemplos

```
Sea M el término
```

```
\lambda f: \mathsf{nat} \to \mathsf{nat}.

\lambda x: \mathsf{nat}.

if \mathsf{iszero}(x) then \underline{1} else x * f(\mathsf{pred}(x))
```

en

fix $M \underline{3}$

Ejemplos

Ahora podemos definir funciones parciales:

fix
$$(\lambda x : \sigma.x)$$

- ▶ Notar que \vdash fix $(\lambda x : \sigma.x) : \sigma$ para cualquier σ .
- ▶ En particular, vale para $\sigma = \bot$.
- ▶ En consecuencia, si se extiende NJ con un operador fix , la lógica resulta inconsistente ($\vdash \bot$ sería derivable)

Lectura recomendada

Capítulos 3 y 4 del libro de Sørensen y Urzyczyn.

Morten Sørensen y Paweł Urzyczyn. Lectures on the Curry–Howard Isomorphism

Elsevier, 2006.