Control cuántico en lenguajes de programación

Alejandro Díaz-Caro

Universidad Nacional de Quilmes & CONICET

IV Jornada de Lógica, Computación e Información Cuántica

1ro de Marzo de 2018

Universidad Nacional de Quilmes

Motivación

Nos interesa estudiar la manera más natural de **impedir el clonado** en **lenguajes de programación cuánticos** y **lógicas formales**

Contenido de la charla

Lambda cálculo simplemente tipado, en cinco slides

Relación con lógica

Motivación, mejor explicada

Trabajo con Gilles Dowek: Un lambda cálculo cuántico

Trabajo con Octavio Malherbe: Interpretación categórica

Trabajo con Juan Pablo Rinaldi: Normalización fuerte

Lambda cálculo simplemente tipado, en cinco slides

(I) Historia, definiciones e intuiciones

Introducido en 1936 por Alonzo Church

Motivación: Investigar los *fundamentos de la matemática*
(en particular, el concepto de recursión)

Porqué aún lo seguimos investigando

- Las funciones recursivas son fundamentales en computación
- Sistema simple para estudiar propiedades de lenguajes de prog.

Lambda cálculo simplemente tipado, en cinco slides

(I) Historia, definiciones e intuiciones

Introducido en 1936 por Alonzo Church

Motivación: Investigar los *fundamentos de la matemática* (en particular, el concepto de recursión)

Porqué aún lo seguimos investigando

- Las funciones recursivas son fundamentales en computación
- Sistema simple para estudiar propiedades de lenguajes de prog.

Dos simplificaciones fundamentales al concepto de función

- Anonimicidad de funciones:
  Ejemplo : $sqsum(x, y) = x^2 + y^2$
  se escribe anónimamente como $(x, y) \mapsto x^2 + y^2$

  Los nombres no son necesarios

- Todas las funciones son a una sóla variable:
  Ejemplo: $(x, y) \mapsto x^2 + y^2$
  se escribe anónimamente como $x \mapsto (y \mapsto x^2 + y^2)$

  Una función a dos variables es una función a una variable, que devuelve una función a una variable, la cual hace el cálculo

Lambda cálculo simplemente tipado, en cinco slides

(II) Formalisación

Lenguaje de términos (una gramática)

$$t \quad ::= \quad x \quad | \quad \lambda x.t \quad | \quad tt$$

- Una variable $x \in \mathit{Vars}$ es un término
- Si t es un término y x una variable, $\lambda x.t$ es un término $\qquad (x \mapsto t)$
- Si t y r son dos términos, tr es un término $\qquad$ (aplicación)

Esos son los únicos términos posibles

Lambda cálculo simplemente tipado, en cinco slides

(II) Formalisación

Lenguaje de términos (una gramática)

$$t \quad ::= \quad x \quad | \quad \lambda x.t \quad | \quad tt$$

- Una variable $x \in \mathit{Vars}$ es un término
- Si t es un término y x una variable, $\lambda x.t$ es un término $(x \mapsto t)$
- Si t y r son dos términos, tr es un término (aplicación)

Esos son los únicos términos posibles

Una regla de reescritura (β-reducción)

$$(\lambda x.t)r \longrightarrow (r/x)t$$

Lenguaje de términos (una gramática)

$$t \quad ::= \quad x \quad | \quad \lambda x.t \quad | \quad tt$$

- Una variable $x \in \mathit{Vars}$ es un término
- Si t es un término y x una variable, $\lambda x.t$ es un término $(x \mapsto t)$
- Si t y r son dos términos, tr es un término (aplicación)

Esos son los únicos términos posibles

Una regla de reescritura (β-reducción)

$$(\lambda x.t)r \longrightarrow (r/x)t$$

Ejemplo:

$$f(g, x) = g(x) \qquad \text{se escribe} \qquad \lambda g.\lambda x.gx$$

Lambda cálculo simplemente tipado, en cinco slides

(II) Formalisación

Lenguaje de términos (una gramática)

$$t \quad ::= \quad x \quad | \quad \lambda x.t \quad | \quad tt$$

- Una variable $x \in \mathit{Vars}$ es un término
- Si t es un término y x una variable, $\lambda x.t$ es un término $(x \mapsto t)$
- Si t y r son dos términos, tr es un término (aplicación)

Esos son los únicos términos posibles

Una regla de reescritura (β-reducción)

$$(\lambda x.t)r \longrightarrow (r/x)t$$

Ejemplo:

$$f(g,x) = g(x) \qquad \text{se escribe} \qquad \lambda g.\lambda x.gx$$

$f(g_0, x_0)$ se escribe $(\lambda g.\lambda x.gx)g_0x_0$ y β-reduce así

$$(\underbrace{\lambda g.}_{(\lambda x.}\underbrace{\lambda x.gx}_{t)})\underbrace{g_0}_{r}x_0 \longrightarrow (\underbrace{\lambda x.g_0x}_{(r/x)t})x_0 \longrightarrow g_0x_0$$

Lambda cálculo simplemente tipado, en cinco slides

(III) Formas normales

No todo cómputo termina bien...

Sea $\lambda x.xx$

(la función que toma como argumento una función y la aplica a sí misma)

Lambda cálculo simplemente tipado, en cinco slides

(III) Formas normales

No todo cómputo termina bien...

Sea $\lambda x.xx$

(la función que toma como argumento una función y la aplica a sí misma)

$$\Omega = (\lambda x.xx)(\lambda x.xx)$$

Lambda cálculo simplemente tipado, en cinco slides

(III) Formas normales

No todo cómputo termina bien...

Sea $\lambda x.xx$

(la función que toma como argumento una función y la aplica a sí misma)

$$\Omega = (\lambda x.xx)(\lambda x.xx) \longrightarrow (\lambda x.xx/x)xx$$

Lambda cálculo simplemente tipado, en cinco slides

(III) Formas normales

No todo cómputo termina bien...

Sea $\lambda x.xx$
(la función que toma como argumento una función y la aplica a sí misma)

$$\Omega = (\lambda x.xx)(\lambda x.xx) \;\longrightarrow\; (\lambda x.xx/x)xx \;=\; (\lambda x.xx)(\lambda x.xx) = \Omega$$

$$\Omega \longrightarrow \Omega \to \Omega \to \cdots$$

Lambda cálculo simplemente tipado, en cinco slides

(III) Formas normales

No todo cómputo termina bien...

Sea $\lambda x.xx$
(la función que toma como argumento una función y la aplica a sí misma)

$$\Omega = (\lambda x.xx)(\lambda x.xx) \ \longrightarrow \ (\lambda x.xx/x)xx \ = \ (\lambda x.xx)(\lambda x.xx) = \Omega$$

$$\Omega \longrightarrow \Omega \to \Omega \to \cdots$$

Normalización

t está en forma normal, si no reescribe ej. $\lambda x.x$

Lambda cálculo simplemente tipado, en cinco slides

(III) Formas normales

No todo cómputo termina bien...

Sea $\lambda x.xx$
(la función que toma como argumento una función y la aplica a sí misma)

$$\Omega = (\lambda x.xx)(\lambda x.xx) \;\longrightarrow\; (\lambda x.xx/x)xx \;=\; (\lambda x.xx)(\lambda x.xx) = \Omega$$

$$\Omega \longrightarrow \Omega \to \Omega \to \cdots$$

Normalización

t está en forma normal, si no reescribe — ej. $\lambda x.x$

t es normalizante si *puede* terminar — ej. $(\lambda x.\lambda y.y)\Omega$

Lambda cálculo simplemente tipado, en cinco slides

(III) Formas normales

No todo cómputo termina bien...

Sea $\lambda x.xx$
(la función que toma como argumento una función y la aplica a sí misma)

$$\Omega = (\lambda x.xx)(\lambda x.xx) \ \longrightarrow\ (\lambda x.xx/x)xx \ =\ (\lambda x.xx)(\lambda x.xx) = \Omega$$

$$\Omega \longrightarrow \Omega \to \Omega \to \cdots$$

Normalización

t está en forma normal, si no reescribe	ej.	$\lambda x.x$
t es normalizante si *puede* terminar	ej.	$(\lambda x.\lambda y.y)\Omega$
t es fuertemente normalizante si siempre termina	ej.	$(\lambda x.x)(\lambda x.x)$

Lambda cálculo simplemente tipado, en cinco slides

(III) Formas normales

No todo cómputo termina bien...

Sea $\lambda x.xx$
(la función que toma como argumento una función y la aplica a sí misma)

$$\Omega = (\lambda x.xx)(\lambda x.xx) \longrightarrow (\lambda x.xx/x)xx = (\lambda x.xx)(\lambda x.xx) = \Omega$$

$$\Omega \longrightarrow \Omega \to \Omega \to \cdots$$

Normalización

t está en forma normal, si no reescribe	ej.	$\lambda x.x$
t es normalizante si *puede* terminar	ej.	$(\lambda x.\lambda y.y)\Omega$
t es fuertemente normalizante si siempre termina	ej.	$(\lambda x.x)(\lambda x.x)$

¿Cómo saber si un término es (fuertemente) normalizante?

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente
(i.e. sin reducirlos)

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

Términos	t	$::=$	x	$\mid$	$\lambda x^A.t$	$\mid$	tt
Tipos	A	$::=$	τ	$\mid$	$A \Rightarrow A$		

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

Términos	t	$::=$	$x \mid \lambda x^A.t \mid tt$
Tipos	A	$::=$	$\tau \mid A \Rightarrow A$

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\quad \Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A \qquad$ "t tiene tipo A en el contexto Γ"

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente
(i.e. sin reducirlos)

$$\begin{array}{llllllll} \textbf{Términos} & t & ::= & x & \mid & \lambda x^A.t & \mid & tt \\ \textbf{Tipos} & A & ::= & \tau & \mid & A \Rightarrow A & & \end{array}$$

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\quad \Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A \qquad$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

$$\begin{array}{lcclclcl} \textbf{Términos} & t & ::= & x & \mid & \lambda x^A.t & \mid & tt \\ \textbf{Tipos} & A & ::= & \tau & \mid & A \Rightarrow A & & \end{array}$$

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

$$\frac{}{\Gamma, x^A \vdash x : A}\ ax$$

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente
(i.e. sin reducirlos)

$$\begin{array}{llcl}
\textbf{Términos} & t & ::= & x \mid \lambda x^A.t \mid tt \\
\textbf{Tipos} & A & ::= & \tau \mid A \Rightarrow A
\end{array}$$

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\quad \Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A \qquad$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

$$\frac{}{\Gamma, x^A \vdash x : A}\ ax \qquad \frac{\Gamma, x^A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \Rightarrow_I$$

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

$$
\begin{array}{lrcl}
\textbf{Términos} & t & ::= & x \mid \lambda x^A.t \mid tt \\
\textbf{Tipos} & A & ::= & \tau \mid A \Rightarrow A
\end{array}
$$

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

$$
\frac{}{\Gamma, x^A \vdash x : A}\ ax \qquad \frac{\Gamma, x^A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash r : A}{\Gamma \vdash tr : B} \Rightarrow_E
$$

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

$$\begin{array}{llcl} \textbf{Términos} & t & ::= & x \mid \lambda x^A.t \mid tt \\ \textbf{Tipos} & A & ::= & \tau \mid A \Rightarrow A \end{array}$$

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

$$\frac{}{\Gamma, x^A \vdash x : A}\ ax \qquad \frac{\Gamma, x^A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash r : A}{\Gamma \vdash tr : B} \Rightarrow_E$$

Ejemplo de derivación de tipo

$$\frac{}{x^\tau \vdash x : \tau}\ ax$$

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

Términos	t	$::=$	$x \mid \lambda x^A.t \mid tt$
Tipos	A	$::=$	$\tau \mid A \Rightarrow A$

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\quad \Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A \qquad$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

$$\frac{}{\Gamma, x^A \vdash x : A}\ ax \qquad \frac{\Gamma, x^A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash r : A}{\Gamma \vdash tr : B} \Rightarrow_E$$

Ejemplo de derivación de tipo

$$\frac{\dfrac{}{x^\tau \vdash x : \tau}\ ax}{\vdash \lambda x^\tau.x : \tau \Rightarrow \tau} \Rightarrow_I$$

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

Términos	t	$::=$	x	$\mid$	$\lambda x^A.t$	$\mid$	tt
Tipos	A	$::=$	τ	$\mid$	$A \Rightarrow A$		

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\qquad \Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A \qquad$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

$$\frac{}{\Gamma, x^A \vdash x : A}\ ax \qquad \frac{\Gamma, x^A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash r : A}{\Gamma \vdash tr : B} \Rightarrow_E$$

Ejemplo de derivación de tipo

$$\frac{}{x^{\tau \Rightarrow \tau} \vdash x : \tau \Rightarrow \tau}\ ax \qquad\qquad \frac{\dfrac{}{x^\tau \vdash x : \tau}\ ax}{\vdash \lambda x^\tau.x : \tau \Rightarrow \tau} \Rightarrow_I$$

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

Términos	t	$::=$	x	$\mid$	$\lambda x^A.t$	$\mid$	tt
Tipos	A	$::=$	τ	$\mid$	$A \Rightarrow A$		

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

$$\frac{}{\Gamma, x^A \vdash x : A}\ ax \qquad \frac{\Gamma, x^A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash r : A}{\Gamma \vdash tr : B} \Rightarrow_E$$

Ejemplo de derivación de tipo

$$\frac{\overline{x^{\tau \Rightarrow \tau} \vdash x : \tau \Rightarrow \tau}\ ax}{\vdash \lambda x^{\tau \Rightarrow \tau}.x : (\tau \Rightarrow \tau) \Rightarrow (\tau \Rightarrow \tau)} \Rightarrow_I \qquad \frac{\overline{x^{\tau} \vdash x : \tau}\ ax}{\vdash \lambda x^{\tau}.x : \tau \Rightarrow \tau} \Rightarrow_I$$

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

Términos	t	$::=$	x	$\mid$	$\lambda x^A.t$	$\mid$	tt
Tipos	A	$::=$	τ	$\mid$	$A \Rightarrow A$		

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\qquad \Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A \qquad$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

$$\frac{}{\Gamma, x^A \vdash x : A}\ ax \qquad \frac{\Gamma, x^A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash r : A}{\Gamma \vdash tr : B} \Rightarrow_E$$

Ejemplo de derivación de tipo

$$\frac{\dfrac{\dfrac{}{x^{\tau \Rightarrow \tau} \vdash x : \tau \Rightarrow \tau}\ ax}{\vdash \lambda x^{\tau \Rightarrow \tau}.x : (\tau \Rightarrow \tau) \Rightarrow (\tau \Rightarrow \tau)} \Rightarrow_I \qquad \dfrac{\dfrac{}{x^{\tau} \vdash x : \tau}\ ax}{\vdash \lambda x^{\tau}.x : \tau \Rightarrow \tau} \Rightarrow_I}{\vdash (\lambda x^{\tau \Rightarrow \tau}.x)(\lambda x^{\tau}.x) : \tau \Rightarrow \tau} \Rightarrow_E$$

Lambda cálculo simplemente tipado, en cinco slides

(IV) Tipos simples

Una forma de clasificar términos estáticamente (i.e. sin reducirlos)

Términos	t	$::=$	x	$\mid$	$\lambda x^A.t$	$\mid$	tt
Tipos	A	$::=$	τ	$\mid$	$A \Rightarrow A$		

- τ es un *tipo básico*
- $A \Rightarrow A$ es el tipo funcional

Contexto: conjunto de variables tipadas $\quad \Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

$\Gamma \vdash t : A \quad$ "t tiene tipo A en el contexto Γ"

Reglas de tipado

$$\frac{}{\Gamma, x^A \vdash x : A}\ ax \qquad \frac{\Gamma, x^A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash r : A}{\Gamma \vdash tr : B} \Rightarrow_E$$

Ejemplo de derivación de tipo

$$\frac{\dfrac{\dfrac{}{x^{\tau\Rightarrow\tau} \vdash x : \tau \Rightarrow \tau}\ ax}{\vdash \lambda x^{\tau\Rightarrow\tau}.x : (\tau \Rightarrow \tau) \Rightarrow (\tau \Rightarrow \tau)} \Rightarrow_I \quad \dfrac{\dfrac{}{x^{\tau} \vdash x : \tau}\ ax}{\vdash \lambda x^{\tau}.x : \tau \Rightarrow \tau} \Rightarrow_I}{\vdash (\lambda x^{\tau\Rightarrow\tau}.x)(\lambda x^{\tau}.x) : \tau \Rightarrow \tau} \Rightarrow_E$$

Verificación: $(\lambda x^{\tau\Rightarrow\tau}.x)(\lambda x^{\tau}.x)$ reescribe a $\lambda x^{\tau}.x$ (de tipo $\tau \Rightarrow \tau$)

Lambda cálculo simplemente tipado, en cinco slides

(V) Normalización

Ω no tiene tipo en esta teoría

Más aún...

Teorema (Normalización fuerte)

Si t tiene tipo simple, t es fuertemente normalizante

Slogan *"Well-typed programs cannot go wrong"* — `[R. Milner'78]`

Otras razones para necesitar tipos:

$$(\lambda x.x + 1)$$

Lambda cálculo simplemente tipado, en cinco slides

(V) Normalización

Ω no tiene tipo en esta teoría

Más aún...

Teorema (Normalización fuerte)

Si t tiene tipo simple, t es fuertemente normalizante

Slogan *"Well-typed programs cannot go wrong"* — `[R. Milner'78]`

Otras razones para necesitar tipos:

$$(\lambda x.x + 1)(\lambda y.y) \to (\lambda y.y) + 1 \qquad \leftarrow ?$$

$\lambda x.x + 1$ debería tener tipo $\mathbb{N} \Rightarrow \mathbb{N}$

¿Cómo se relaciona esto con lógica intuicionista?

Unas palabras sobre la correspondencia de Curry-Howard

Lógica clásica: una fórmula bien formada se asume verdadera o falsa

Lógica intuicionista: una fórmula es verdadera (falsa) si existe una prueba constructiva de que es verdadera (falsa)

¡La ley del tercero excluido no es un axioma! (y tampoco puede ser probada) en lógica intuicionista

¿Cómo se relaciona esto con lógica intuicionista?

Unas palabras sobre la correspondencia de Curry-Howard

Lógica clásica: una fórmula bien formada se asume verdadera o falsa

Lógica intuicionista: una fórmula es verdadera (falsa) si existe una prueba constructiva de que es verdadera (falsa)

¡La ley del tercero excluido no es un axioma!
(y tampoco puede ser probada) en lógica intuicionista

Lógica intuicionista mínima (incluyendo sólo la implicación)

$$\frac{}{\Gamma, A \vdash A}\ ax \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \Rightarrow_E$$

Reglas de tipado

$$\frac{}{\Gamma, x : A \vdash x : A}\ ax \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash r : A}{\Gamma \vdash tr : B} \Rightarrow_E$$

El término es la prueba de la fórmula

Las pruebas... son programas!

Haskell Curry y William Howard, entre 1934 y 1969

Lógicas más complejas corresponden a sistemas de tipos más complejos

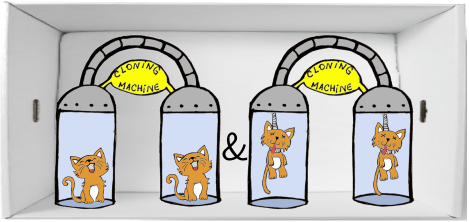
Motivación

Dos enfoques en la literatura para lidiar con el no-clonado

Enfoque de la lógica lineal

e.g. $\lambda x.(x \otimes x)$ no es válido

Enfoque del álgebra lineal



e.g. $f(\alpha\,|0\rangle + \beta\,|1\rangle) \to \alpha f(|0\rangle) + \beta f(|1\rangle)$

Motivación

Medición

El enfoque del álgebra lineal no tiene sentido aquí...

...pero el de la lógica lineal, sí

---

e.g.

$$(\lambda x.\pi x)\ (\alpha.\,|0\rangle + \beta.\,|1\rangle) \longrightarrow \alpha.(\lambda x.\pi x)\,|0\rangle + \beta.(\lambda x.\pi x)\,|1\rangle$$ **¡Incorrecto!**

(Operador de medición)

Clave

Necesitamos distinguir estados en superposición de estados de base usando <u>tipos</u>

Los estados de base pueden ser clonados
Los estados superpuestos, no

Una función que admite recibir un estado superpuesto, no puede clonar su argumento

Sintaxis

Primera versión, sin tensor

Tipos

$$\Psi := \mathbb{B} \mid S(\Psi) \qquad \text{Tipos “Qubit”}$$

$$A := \Psi \mid \Psi \Rightarrow A \mid S(A) \qquad \text{Tipos generales}$$

Términos

$$t := \underbrace{x \mid \lambda x^{\Psi}.t \mid |0\rangle \mid |1\rangle}_{\text{términos de base}} \mid tt \mid \pi t \mid ?t{\cdot}t \mid \underbrace{t + t \mid \alpha.t \mid \vec{0}_{S(A)}}_{\text{combinaciones lineales}}$$

donde $\alpha \in \mathbb{C}$

Dos clases de linealidad

$$(\lambda x^{\mathbb{B}}.t)\underbrace{b}_{\mathbb{B}} \quad\to\quad (b/x)t \qquad \text{call-by-base}$$

$$\underbrace{(\lambda x^{S(\Psi)}.t)}_{\text{abstracción lineal}}\ \underbrace{u}_{S(\Psi)} \quad\to\quad (u/x)t \qquad \text{call-by-name}$$

$$(\lambda x^{\mathbb{B}}.t)\underbrace{(b_1+b_2)}_{S(\mathbb{B})} \quad\to\quad (\lambda x^{\mathbb{B}}.t)\underbrace{b_1}_{\mathbb{B}}+(\lambda x^{\mathbb{B}}.t)\underbrace{b_2}_{\mathbb{B}} \qquad \text{distribución lineal}$$

Medición

$$\pi(\alpha_1.b_1 + \alpha_2.b_2) \longrightarrow_{\left(\frac{|\alpha_k|^2}{|\alpha_1|^2+|\alpha_2|^2}\right)} b_k$$

- Para $i = 1, 2$, $b_i = |0\rangle$ o $b_i = |1\rangle$.
- $k = 1, 2$

Ejemplo

$$\begin{tikzcd} & {|0\rangle} \\ {\pi(i.\,|0\rangle + 2.\,|1\rangle)} \arrow[ur, "\left(\frac{1}{5}\right)"'] \arrow[dr, "\left(\frac{4}{5}\right)"'] & \\ & {|1\rangle} \end{tikzcd}$$

Agregando producto tensorial

Interpretación de tipos

$$
\begin{aligned}
[\![\mathbb{B}]\!] &= \{|0\rangle, |1\rangle\} \subseteq \mathbb{C}^2 \\
[\![A \times B]\!] &= [\![A]\!] \times [\![B]\!] \\
[\![S(A)]\!] &= \mathcal{G}\,[\![A]\!] \\
\mathcal{G}(B_1 \times B_2) &\simeq \mathcal{G}(B_1) \otimes \mathcal{G}(B_2)
\end{aligned}
$$

Agregando producto tensorial

Interpretación de tipos

$$\llbracket \mathbb{B} \rrbracket = \{\left|0\right\rangle, \left|1\right\rangle\} \subseteq \mathbb{C}^2$$

$$\llbracket A \times B \rrbracket = \llbracket A \rrbracket \times \llbracket B \rrbracket$$

$$\llbracket S(A) \rrbracket = \mathcal{G} \llbracket A \rrbracket$$

$$\mathcal{G}(B_1 \times B_2) \simeq \mathcal{G}(B_1) \otimes \mathcal{G}(B_2)$$

Ejemplos:

$\mathcal{G}(\{\left|0\right\rangle, \left|1\right\rangle\} \times \{\left|0\right\rangle, \left|1\right\rangle\})$

Agregando producto tensorial

Interpretación de tipos

$$\llbracket \mathbb{B} \rrbracket = \{|0\rangle, |1\rangle\} \subseteq \mathbb{C}^2$$
$$\llbracket A \times B \rrbracket = \llbracket A \rrbracket \times \llbracket B \rrbracket$$
$$\llbracket S(A) \rrbracket = \mathcal{G} \llbracket A \rrbracket$$
$$\mathcal{G}(B_1 \times B_2) \simeq \mathcal{G}(B_1) \otimes \mathcal{G}(B_2)$$

Ejemplos:

$$\mathcal{G}(\{|0\rangle, |1\rangle\} \times \{|0\rangle, |1\rangle\}) = \mathcal{G}\{(|0\rangle, |0\rangle), (|0\rangle, |1\rangle), (|1\rangle, |0\rangle), (|1\rangle, |1\rangle)\}$$

Agregando producto tensorial

Interpretación de tipos

$$
\begin{aligned}
[\![\mathbb{B}]\!] &= \{|0\rangle\,, |1\rangle\} \subseteq \mathbb{C}^2 \\
[\![A \times B]\!] &= [\![A]\!] \times [\![B]\!] \\
[\![S(A)]\!] &= \mathcal{G}\,[\![A]\!] \\
\mathcal{G}(B_1 \times B_2) &\simeq \mathcal{G}(B_1) \otimes \mathcal{G}(B_2)
\end{aligned}
$$

Ejemplos:

$$
\begin{aligned}
\mathcal{G}(\{|0\rangle\,, |1\rangle\} \times \{|0\rangle\,, |1\rangle\}) &= \mathcal{G}\{(|0\rangle\,, |0\rangle), (|0\rangle\,, |1\rangle), (|1\rangle\,, |0\rangle), (|1\rangle\,, |1\rangle)\} \\
&\simeq \mathcal{G}\{|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle\}
\end{aligned}
$$

Agregando producto tensorial

Interpretación de tipos

$$
\begin{aligned}
[\![\mathbb{B}]\!] &= \{|0\rangle, |1\rangle\} \subseteq \mathbb{C}^2\\
[\![A \times B]\!] &= [\![A]\!] \times [\![B]\!]\\
[\![S(A)]\!] &= \mathcal{G}\,[\![A]\!]\\
\mathcal{G}(B_1 \times B_2) &\simeq \mathcal{G}(B_1) \otimes \mathcal{G}(B_2)
\end{aligned}
$$

Ejemplos:

$$
\begin{aligned}
\mathcal{G}(\{|0\rangle, |1\rangle\} \times \{|0\rangle, |1\rangle\}) &= \mathcal{G}\{(|0\rangle, |0\rangle), (|0\rangle, |1\rangle), (|1\rangle, |0\rangle), (|1\rangle, |1\rangle)\}\\
&\simeq \mathcal{G}\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}\\
&= \mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2
\end{aligned}
$$

Agregando producto tensorial

Interpretación de tipos

$$\llbracket \mathbb{B} \rrbracket = \{\left|0\right\rangle, \left|1\right\rangle\} \subseteq \mathbb{C}^2$$
$$\llbracket A \times B \rrbracket = \llbracket A \rrbracket \times \llbracket B \rrbracket$$
$$\llbracket S(A) \rrbracket = \mathcal{G}\,\llbracket A \rrbracket$$
$$\mathcal{G}(B_1 \times B_2) \simeq \mathcal{G}(B_1) \otimes \mathcal{G}(B_2)$$

Ejemplos:

$$\begin{aligned}
\mathcal{G}(\{\left|0\right\rangle, \left|1\right\rangle\} \times \{\left|0\right\rangle, \left|1\right\rangle\}) &= \mathcal{G}\{(\left|0\right\rangle, \left|0\right\rangle), (\left|0\right\rangle, \left|1\right\rangle), (\left|1\right\rangle, \left|0\right\rangle), (\left|1\right\rangle, \left|1\right\rangle)\} \\
&\simeq \mathcal{G}\{\left|00\right\rangle, \left|01\right\rangle, \left|10\right\rangle, \left|11\right\rangle\} \\
&= \mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2 \\
&= \mathcal{G}\{\left|0\right\rangle, \left|1\right\rangle\} \otimes \mathcal{G}\{\left|0\right\rangle, \left|1\right\rangle\}
\end{aligned}$$

Agregando producto tensorial

Interpretación de tipos

$$
\begin{aligned}
[\![\mathbb{B}]\!] &= \{|0\rangle, |1\rangle\} \subseteq \mathbb{C}^2 \\
[\![A \times B]\!] &= [\![A]\!] \times [\![B]\!] \\
[\![S(A)]\!] &= \mathcal{G}\,[\![A]\!] \\
\mathcal{G}(B_1 \times B_2) &\simeq \mathcal{G}(B_1) \otimes \mathcal{G}(B_2)
\end{aligned}
$$

Ejemplos:

$$
\begin{aligned}
\mathcal{G}(\{|0\rangle, |1\rangle\} \times \{|0\rangle, |1\rangle\}) &= \mathcal{G}\{(|0\rangle, |0\rangle), (|0\rangle, |1\rangle), (|1\rangle, |0\rangle), (|1\rangle, |1\rangle)\} \\
&\simeq \mathcal{G}\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \\
&= \mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2 \\
&= \mathcal{G}\{|0\rangle, |1\rangle\} \otimes \mathcal{G}\{|0\rangle, |1\rangle\}
\end{aligned}
$$

$$
(\underbrace{|0\rangle}_{\mathbb{B}}, \underbrace{(1/\sqrt{2}.\,|0\rangle + 1/\sqrt{2}.\,|1\rangle)}_{S(\mathbb{B})}) \in \{|0\rangle, |1\rangle\} \times \mathbb{C}^2
$$

$$
\underbrace{1/\sqrt{2}.(|0\rangle, |0\rangle) \;+\; 1/\sqrt{2}.(|0\rangle, |1\rangle)}_{S(\mathbb{B}\times\mathbb{B})} \in \mathbb{C}^2 \otimes \mathbb{C}^2
$$

Algo de información se pierde con la reducción

Subtipado

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \qquad \text{entonces} \qquad \mathbb{B} \leq S(\mathbb{B})$$

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \qquad \text{entonces} \qquad S(S(\mathbb{B})) \leq S(\mathbb{B})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \times \mathbb{C}^2 \qquad \text{entonces} \qquad \mathbb{B} \times S(\mathbb{B}) \leq S(\mathbb{B} \times \mathbb{B})$$

Algo de información se pierde con la reducción

Subtipado

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{entonces} \quad \mathbb{B} \leq S(\mathbb{B})$$
$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{entonces} \quad S(S(\mathbb{B})) \leq S(\mathbb{B})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \times \mathbb{C}^2 \quad \text{entonces} \quad \mathbb{B} \times S(\mathbb{B}) \leq S(\mathbb{B} \times \mathbb{B})$$

$$(|0\rangle, \ |0\rangle + |1\rangle) \quad : \quad \mathbb{B} \times S(\mathbb{B})$$

$$(|0\rangle, |0\rangle) + (|0\rangle, |1\rangle) \quad : \quad S(\mathbb{B} \times \mathbb{B})$$

Algo de información se pierde con la reducción

Subtipado

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{entonces} \quad \mathbb{B} \leq S(\mathbb{B})$$

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{entonces} \quad S(S(\mathbb{B})) \leq S(\mathbb{B})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \times \mathbb{C}^2 \quad \text{entonces} \quad \mathbb{B} \times S(\mathbb{B}) \leq S(\mathbb{B} \times \mathbb{B})$$

$$(|0\rangle, |0\rangle + |1\rangle) \quad : \quad \mathbb{B} \times S(\mathbb{B})$$

$$(|0\rangle, |0\rangle) + (|0\rangle, |1\rangle) \quad : \quad S(\mathbb{B} \times \mathbb{B})$$

Algo de información se pierde con la reducción

Subtipado

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{entonces} \quad \mathbb{B} \leq S(\mathbb{B})$$

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{entonces} \quad S(S(\mathbb{B})) \leq S(\mathbb{B})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \times \mathbb{C}^2 \quad \text{entonces} \quad \mathbb{B} \times S(\mathbb{B}) \leq S(\mathbb{B} \times \mathbb{B})$$

$$(|0\rangle,\ |0\rangle + |1\rangle) \quad : \quad \mathbb{B} \times S(\mathbb{B})$$

$$(|0\rangle, |0\rangle) + (|0\rangle, |1\rangle) \quad : \quad S(\mathbb{B} \times \mathbb{B})$$

¡Lo mismo pasa en otros ámbitos de la matemática!

$$(X-1)(X-2) \longrightarrow X^2 - 3X + 2$$

perdimos la información de que era un producto

Algo de información se pierde con la reducción

Subtipado

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{entonces} \quad \mathbb{B} \leq S(\mathbb{B})$$
$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{entonces} \quad S(S(\mathbb{B})) \leq S(\mathbb{B})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \times \mathbb{C}^2 \quad \text{entonces} \quad \mathbb{B} \times S(\mathbb{B}) \leq S(\mathbb{B} \times \mathbb{B})$$

$$(|0\rangle, \ |0\rangle + |1\rangle) \quad : \quad \mathbb{B} \times S(\mathbb{B})$$
$$(|0\rangle, |0\rangle) + (|0\rangle, |1\rangle) \quad : \quad S(\mathbb{B} \times \mathbb{B})$$

¡Lo mismo pasa en otros ámbitos de la matemática!

$$(X-1)(X-2) \longrightarrow X^2 - 3X + 2$$

perdimos la información de que era un producto

Solución: casting

$$(|0\rangle, |0\rangle + |1\rangle) \not\to (|0\rangle, |0\rangle) + (|0\rangle, |1\rangle)$$
$$\Uparrow(|0\rangle, |0\rangle + |1\rangle) \to (|0\rangle, |0\rangle) + (|0\rangle, |1\rangle)$$

Sintaxis completa

Types

$$Q := \mathbb{B} \mid Q \times Q \qquad \text{Basis qubit types}$$

$$\Psi := Q \mid S(\Psi) \mid \Psi \times \Psi \qquad \text{Qubit types}$$

$$A := \Psi \mid \Psi \Rightarrow A \mid S(A) \mid A \times A \qquad \text{Types}$$

Terms

$$t := x \mid \lambda x^{\Psi}.t \mid \ |0\rangle \ \mid \ |1\rangle \ \mid tt \mid \pi_j t \mid ?t{\cdot}t \mid t + t \mid \alpha.t \mid \vec{0}_{S(A)}$$
$$\mid t \times t \mid \mathit{head}\ t \mid \mathit{tail}\ t \mid \ \Uparrow t$$

con $\alpha \in \mathbb{C}$

Medición de los primeros j qubits

Ejemplo

$$
\begin{tikzcd}
 & \pi_2(\ 2\,|\mathbf{01}1\rangle\ +\ |\mathbf{01}0\rangle\ +\ 3\,|\mathbf{11}1\rangle\ ) \arrow[dl, "(\frac{5}{14})"'] \arrow[dr, "(\frac{9}{14})"] & \\
|\mathbf{01}\rangle \times (\frac{2}{\sqrt{5}}\,|1\rangle + \frac{1}{\sqrt{5}}\,|0\rangle) & & |\mathbf{11}\rangle \times (1\,|1\rangle)
\end{tikzcd}
$$

Sistema de tipos

$Q := \mathbb{B} \mid Q \times Q$	Tipos qubit de base
$\Psi := Q \mid S(\Psi) \mid \Psi \times \Psi$	Tipos qubits
$A := \Psi \mid \Psi \Rightarrow A \mid S(A) \mid A \times A$	Tipos generales

$$\frac{}{x : \Psi \vdash x : \Psi}\ \mathsf{ax} \qquad \frac{}{\vdash \vec{0}_{S(A)} : S(A)}\ \mathsf{ax}_{\vec{0}} \qquad \frac{}{\vdash |0\rangle : \mathbb{B}}\ \mathsf{ax}_{|0\rangle} \qquad \frac{}{\vdash |1\rangle : \mathbb{B}}\ \mathsf{ax}_{|1\rangle}$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \alpha.t : S(A)}\ S_I^{\alpha} \qquad \frac{\Gamma \vdash t : A \quad \Delta \vdash u : A}{\Gamma, \Delta \vdash t + u : S(A)}\ S_I^{+} \qquad \frac{\Gamma \vdash t : S(\prod_{i=1}^{n} \mathbb{B})}{\Gamma \vdash \pi_j t : \prod_{i=1}^{j} \mathbb{B} \times S(\prod_{i=j+1}^{n} \mathbb{B})}\ S_E$$

$$\frac{\Gamma \vdash t : A \ {\scriptstyle (A \preceq B)}}{\Gamma \vdash t : B}\ \preceq \qquad \frac{\Gamma \vdash t : A \quad \Gamma \vdash u : A}{\Gamma \vdash ?t{\cdot}u : \mathbb{B} \Rightarrow A}\ \mathsf{if} \qquad \frac{\Gamma, x : \Psi \vdash t : A}{\Gamma \vdash \lambda x : \Psi\ t : \Psi \Rightarrow A}\ \Rightarrow_I$$

$$\frac{\Gamma \vdash t : \Psi \Rightarrow A \quad \Delta \vdash u : \Psi}{\Gamma, \Delta \vdash tu : A}\ \Rightarrow_E \qquad \frac{\Gamma \vdash t : S(\Psi \Rightarrow A) \quad \Delta \vdash u : S(\Psi)}{\Gamma, \Delta \vdash tu : S(A)}\ \Rightarrow_{ES}$$

$$\frac{\Gamma \vdash t : A}{\Gamma, x : Q \vdash t : A}\ W \qquad \frac{\Gamma, x : Q, y : Q \vdash t : A}{\Gamma, x : Q \vdash (x/y)t : A}\ C$$

$$\frac{\Gamma \vdash t : A \quad \Delta \vdash u : B}{\Gamma, \Delta \vdash t \times u : A \times B}\ \times_I \qquad \frac{\Gamma \vdash t : \mathbb{B} \times Q}{\Gamma \vdash \mathit{head}\ t : \mathbb{B}}\ \times_{Er} \qquad \frac{\Gamma \vdash t : \mathbb{B} \times Q}{\Gamma \vdash \mathit{tail}\ t : Q}\ \times_{El}$$

$$\frac{\Gamma \vdash t : S(S(A) \times B)}{\Gamma \vdash \Uparrow t : S(A \times B)}\ \Uparrow_r \qquad \frac{\Gamma \vdash t : S(A \times S(B))}{\Gamma \vdash \Uparrow t : S(A \times B)}\ \Uparrow_l$$

Interpretación categórica

Trabajo en progreso con Octavio Malherbe

En general:

$$[\![\Gamma \vdash t : A]\!] = [\![\Gamma]\!] \xrightarrow{t} [\![A]\!]$$

Ejemplos:

$$\left[\!\!\left[\frac{}{x : \Psi \vdash x : \Psi}\right]\!\!\right] = \Psi \xrightarrow{\mathsf{Id}} \Psi$$

$$\left[\!\!\left[\frac{\Gamma \vdash t : A \quad \Delta \vdash r : A}{\Gamma, \Delta \vdash t + r : S(A)}\right]\!\!\right] = \Gamma \times \Delta \xrightarrow{t \times r} A \times A \xrightarrow{+} S(A)$$

Interpretación categórica

Trabajo en progreso con Octavio Malherbe

En general:

$$[\![\Gamma \vdash t : A]\!] = [\![\Gamma]\!] \xrightarrow{t} [\![A]\!]$$

Ejemplos:

$$\left[\!\!\left[\frac{}{x : \Psi \vdash x : \Psi}\right]\!\!\right] = \Psi \xrightarrow{\mathsf{Id}} \Psi$$

$$\left[\!\!\left[\frac{\Gamma \vdash t : A \quad \Delta \vdash r : A}{\Gamma, \Delta \vdash t + r : S(A)}\right]\!\!\right] = \Gamma \times \Delta \xrightarrow{t \times r} A \times A \xrightarrow{+} S(A)$$

$$\left[\!\!\left[\frac{\Delta \vdash r : \Psi \quad \Gamma \vdash t : \Psi \Rightarrow A}{\Delta, \Gamma \vdash tr : A}\right]\!\!\right] = \Delta \times \Gamma \xrightarrow{r \times t} \Psi \times [\Psi, A] \xrightarrow{\varepsilon} A$$

Interpretación categórica

Trabajo en progreso con Octavio Malherbe

En general:

$$[\![\Gamma \vdash t : A]\!] = [\![\Gamma]\!] \xrightarrow{t} [\![A]\!]$$

Ejemplos:

$$\left[\!\!\left[\frac{}{x : \Psi \vdash x : \Psi}\right]\!\!\right] = \Psi \xrightarrow{\mathrm{Id}} \Psi$$

$$\left[\!\!\left[\frac{\Gamma \vdash t : A \quad \Delta \vdash r : A}{\Gamma, \Delta \vdash t + r : S(A)}\right]\!\!\right] = \Gamma \times \Delta \xrightarrow{t \times r} A \times A \xrightarrow{+} S(A)$$

$$\left[\!\!\left[\frac{\Delta \vdash r : \Psi \quad \Gamma \vdash t : \Psi \Rightarrow A}{\Delta, \Gamma \vdash tr : A}\right]\!\!\right] = \Delta \times \Gamma \xrightarrow{r \times t} \Psi \times [\Psi, A] \xrightarrow{\varepsilon} A$$

$$\left[\!\!\left[\frac{\Delta \vdash r : S(\Psi) \quad \Gamma \vdash t : S(\Psi \Rightarrow A)}{\Delta, \Gamma \vdash tr : S(A)}\right]\!\!\right] = \Delta \times \Gamma \xrightarrow{r \times t} S(\Psi) \times S([\Psi, A])$$

Interpretación categórica

Trabajo en progreso con Octavio Malherbe

En general:

$$[\![\Gamma \vdash t : A]\!] = [\![\Gamma]\!] \xrightarrow{t} [\![A]\!]$$

Ejemplos:

$$\left[\!\!\left[\frac{}{x : \Psi \vdash x : \Psi}\right]\!\!\right] = \Psi \xrightarrow{\mathsf{Id}} \Psi$$

$$\left[\!\!\left[\frac{\Gamma \vdash t : A \quad \Delta \vdash r : A}{\Gamma, \Delta \vdash t + r : S(A)}\right]\!\!\right] = \Gamma \times \Delta \xrightarrow{t \times r} A \times A \xrightarrow{+} S(A)$$

$$\left[\!\!\left[\frac{\Delta \vdash r : \Psi \quad \Gamma \vdash t : \Psi \Rightarrow A}{\Delta, \Gamma \vdash tr : A}\right]\!\!\right] = \Delta \times \Gamma \xrightarrow{r \times t} \Psi \times [\Psi, A] \xrightarrow{\varepsilon} A$$

$$\left[\!\!\left[\frac{\Delta \vdash r : S(\Psi) \quad \Gamma \vdash t : S(\Psi \Rightarrow A)}{\Delta, \Gamma \vdash tr : S(A)}\right]\!\!\right] = \Delta \times \Gamma \xrightarrow{r \times t} S(\Psi) \times S([\Psi, A])$$

$$\xrightarrow{\otimes} S(\Psi) \otimes S([\Psi, A]) \approx S(\Psi \times [\Psi, A])$$

Interpretación categórica

Trabajo en progreso con Octavio Malherbe

En general:

$$[\![\Gamma \vdash t : A]\!] = [\![\Gamma]\!] \xrightarrow{t} [\![A]\!]$$

Ejemplos:

$$\left[\!\!\left[\frac{}{x : \Psi \vdash x : \Psi}\right]\!\!\right] = \Psi \xrightarrow{\mathsf{Id}} \Psi$$

$$\left[\!\!\left[\frac{\Gamma \vdash t : A \quad \Delta \vdash r : A}{\Gamma, \Delta \vdash t + r : S(A)}\right]\!\!\right] = \Gamma \times \Delta \xrightarrow{t \times r} A \times A \xrightarrow{+} S(A)$$

$$\left[\!\!\left[\frac{\Delta \vdash r : \Psi \quad \Gamma \vdash t : \Psi \Rightarrow A}{\Delta, \Gamma \vdash tr : A}\right]\!\!\right] = \Delta \times \Gamma \xrightarrow{r \times t} \Psi \times [\Psi, A] \xrightarrow{\varepsilon} A$$

$$\left[\!\!\left[\frac{\Delta \vdash r : S(\Psi) \quad \Gamma \vdash t : S(\Psi \Rightarrow A)}{\Delta, \Gamma \vdash tr : S(A)}\right]\!\!\right] = \Delta \times \Gamma \xrightarrow{r \times t} S(\Psi) \times S([\Psi, A])$$

$$\xrightarrow{\otimes} S(\Psi) \otimes S([\Psi, A]) \approx S(\Psi \times [\Psi, A])$$

$$\xrightarrow{S(\varepsilon)} S(A)$$

Interpretación categórica

Ejemplo

$$
\dfrac{\dfrac{\vdash t : \mathbb{B} \Rightarrow A}{\vdash t : S(\mathbb{B} \Rightarrow A)} \quad \dfrac{\vdash r : \mathbb{B} \quad \vdash s : \mathbb{B}}{\vdash r + s : S(\mathbb{B})}}{\vdash t(r+s) : S(A)}
\qquad
\dfrac{\dfrac{\vdash t : \mathbb{B} \Rightarrow A \quad \vdash r : \mathbb{B}}{\vdash tr : A} \quad \dfrac{\vdash t : \mathbb{B} \Rightarrow A \quad \vdash s : \mathbb{B}}{\vdash ts : A}}{\vdash tr + ts : S(A)}
$$

$$
\begin{tikzcd}
\mathbf{1} \arrow[r, dashed, "\approx"] \arrow[d, dashed, "\approx"] & \mathbf{1} \times \mathbf{1} \times \mathbf{1} \arrow[r, "r \times s \times t"] & \mathbb{B} \times \mathbb{B} \times [\mathbb{B}, A] \arrow[d, "+ \times \eta"] \\
\mathbf{1} \times \mathbf{1} \times \mathbf{1} \times \mathbf{1} \arrow[d, "r \times t \times s \times t"] & & S(\mathbb{B}) \times S([\mathbb{B}, A]) \arrow[d, "\otimes"] \\
\mathbb{B} \times [\mathbb{B}, A] \times \mathbb{B} \times [\mathbb{B}, A] \arrow[d, "\varepsilon \times \varepsilon"] & & S(\mathbb{B}) \otimes S([\mathbb{B}, A]) \arrow[d, dashed, "\approx"] \\
A \times A \arrow[dr, "+"] & & S(\mathbb{B} \times [\mathbb{B}, A]) \arrow[dl, "S(\varepsilon)"] \\
& S(A) &
\end{tikzcd}
$$

Normalización fuerte

Trabajo en progreso con Juan Pablo Rinaldi

Definimos una interpretación $(\!|A|\!)$ alternativa para cada tipo con las siguientes propiedades:

$$\text{Si } t \in (\!|A|\!) \text{ entonces } t \in \mathsf{FN} \tag{1}$$

$$\text{Si } \Gamma \vdash t : A \text{ entonces } t \in (\!|A|\!) \tag{2}$$

Luego

Teorema (Normalización fuerte)

Si $\Gamma \vdash t : A$ entonces $t \in \mathsf{FN}$

Prueba: Si $\Gamma \vdash t : A$, por propiedad (2), $t \in (\!|A|\!)$, y por (1), $t \in \mathsf{FN}$

¡La dificultad es encontrar la definición correcta de $(\!|A|\!)$!
(y demostrar que esas propiedades se cumplen)

Resumen final

- Extensión del cálculo lambda para computación cuántica
- Linealidad algebraica y lógica combinadas para evitar el clonado
- Semántica categórica cartesiana, con productos tensoriales internos

Trabajos en progreso

- Terminar la prueba de normalización fuerte (con J. P. Rinaldi)
- Modelo categórico abstracto (con O. Malherbe)
- Implementación en Haskell (con I. Grimma y P. E. Martínez López)

Backup slides

Why first order

$$\mathsf{CM} = \lambda y^{S(\mathbb{B})}.((\lambda x^{\mathbb{B}\Rightarrow S(\mathbb{B})}.(x\,|0\rangle) \otimes (x\,|0\rangle))\ (\lambda z^{\mathbb{B}}.y))$$

$$\begin{aligned}
&\mathsf{CM}\ (\alpha.\,|0\rangle + \beta.\,|1\rangle)\\
&\to (\lambda x^{\mathbb{B}\Rightarrow S(\mathbb{B})}.(x\,|0\rangle) \otimes (x\,|0\rangle))\ (\lambda z^{\mathbb{B}}.(\alpha.\,|0\rangle + \beta.\,|1\rangle))\\
&\to ((\lambda z^{\mathbb{B}}.(\alpha.\,|0\rangle + \beta.\,|1\rangle))\,|0\rangle) \otimes ((\lambda z^{\mathbb{B}}.(\alpha.\,|0\rangle + \beta.\,|1\rangle))\,|0\rangle)\\
&\to^2 (\alpha.\,|0\rangle + \beta.\,|1\rangle) \otimes (\alpha.\,|0\rangle + \beta.\,|1\rangle)
\end{aligned}$$

Deutsch algorithm

Preliminaries

Hadamard

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Deutsch algorithm

Preliminaries

Hadamard

$$H\,|0\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \qquad H\,|1\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$$

$$H = \lambda x^{\mathbb{B}}.{}^{1}/_{\sqrt{2}}.(|0\rangle + x?{-|1\rangle}\cdot|1\rangle)$$

Deutsch algorithm

Preliminaries

Hadamard

$$H\,|0\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \qquad H\,|1\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$$

$$H = \lambda x^{\mathbb{B}}.{}^{1}/{\scriptstyle\sqrt{2}}.(|0\rangle + x ? {-|1\rangle} \cdot |1\rangle)$$

Oracle

A "black box" implementing a function $f : \{0,1\} \to \{0,1\}$

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$$

Deutsch algorithm

Preliminaries

Hadamard

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$H = \lambda x^{\mathbb{B}}.{}^{1}/_{\sqrt{2}}.(|0\rangle + x?{-}|1\rangle \cdot |1\rangle)$$

Oracle

A "black box" implementing a function $f : \{0,1\} \to \{0,1\}$

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$$

$$not = \lambda x^{\mathbb{B}}.x?|0\rangle \cdot |1\rangle$$

Deutsch algorithm

Preliminaries

Hadamard

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$H = \lambda x^{\mathbb{B}}.{}^{1}/_{\sqrt{2}}.(|0\rangle + x?{-|1\rangle}\cdot|1\rangle)$$

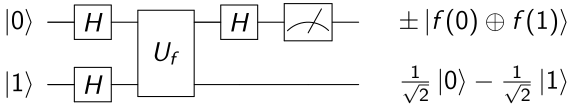
Oracle

A "black box" implementing a function $f : \{0,1\} \to \{0,1\}$

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$$

$$\begin{aligned} not &= \lambda x^{\mathbb{B}}.x?|0\rangle\cdot|1\rangle \\ U_f &= \lambda x^{\mathbb{B}\otimes\mathbb{B}}.(head\ x) \otimes ((tail\ x)?not(f(head\ x))\cdot f(head\ x)) \end{aligned}$$

Deutsch in λ



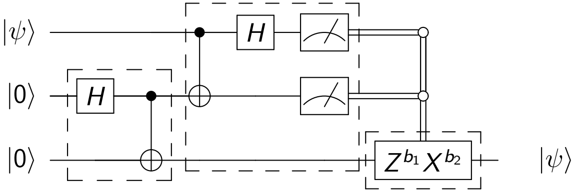
$$
\begin{aligned}
not &= \lambda x^{\mathbb{B}}.x?|0\rangle{\cdot}|1\rangle \\
H &= \lambda x^{\mathbb{B}}.{}^{1}\!/\!_{\sqrt{2}}.(|0\rangle + x?{-}|1\rangle{\cdot}|1\rangle) \\
H^{\otimes 2} &= \lambda x^{\mathbb{B}\otimes\mathbb{B}}.(H(head\ x)) \otimes (H(tail\ x)) \\
U_f &= \lambda x^{\mathbb{B}\otimes\mathbb{B}}.(head\ x) \otimes ((tail\ x)?not(f(head\ x)){\cdot}f(head\ x)) \\
H_1 &= \lambda x^{\mathbb{B}\otimes\mathbb{B}}.(H(head\ x)) \otimes (tail\ x)
\end{aligned}
$$

$$
Deutsch_f = \pi_1(\Uparrow^{S(\mathbb{B}\otimes\mathbb{B})}_{S(S(\mathbb{B})\otimes\mathbb{B})} H_1(U_f \Uparrow^{S(\mathbb{B}\otimes\mathbb{B})}_{S(\mathbb{B}\otimes S(\mathbb{B}))} \Uparrow^{S(\mathbb{B}\otimes S(\mathbb{B}))}_{S(S(\mathbb{B})\otimes S(\mathbb{B}))} H^{\otimes 2}(|0\rangle \otimes |1\rangle))
$$

$$
\vdash Deutsch_f : \mathbb{B} \otimes S(\mathbb{B})
$$

$$
\begin{aligned}
Deutsch_{id} &\longrightarrow^{*}_{(1)} \pi_1({}^{1}\!/\!_{\sqrt{2}}.\,|1\rangle \otimes |0\rangle - {}^{1}\!/\!_{\sqrt{2}}.\,|1\rangle \otimes |1\rangle) \\
&\longrightarrow_{(1)} |1\rangle \otimes ({}^{1}\!/\!_{\sqrt{2}}.\,|0\rangle - {}^{1}\!/\!_{\sqrt{2}}.\,|1\rangle)
\end{aligned}
$$

Teleportation in λ



$$\text{epr} = \lambda x^{\mathbb{B}\otimes\mathbb{B}}.\text{cnot}(H_1\ x)$$
$$\text{alice} =$$
$$\lambda x^{S(\mathbb{B})\otimes S(\mathbb{B}\otimes\mathbb{B})}.\pi_2(\Uparrow^{S(\mathbb{B}\otimes\mathbb{B}\otimes\mathbb{B})}_{S(S(\mathbb{B})\otimes\mathbb{B}\otimes\mathbb{B})} H_1^3(cnot_{12}^3 \Uparrow^{S(\mathbb{B}\otimes\mathbb{B}\otimes\mathbb{B})}_{S(\mathbb{B}\otimes S(\mathbb{B}\otimes\mathbb{B}))}\Uparrow^{S(\mathbb{B}\otimes S(\mathbb{B}\otimes\mathbb{B}))}_{S(S(\mathbb{B})\otimes S(\mathbb{B}\otimes\mathbb{B}))} x))$$

$$U^b = (\lambda b^{\mathbb{B}}.\lambda x^{\mathbb{B}}.b?Ux{\cdot}x)\ b$$
$$\text{bob} = \lambda x^{\mathbb{B}\otimes\mathbb{B}\otimes\mathbb{B}}.Z^{head\ x} not^{head\ (tail\ x)}.(tail\ (tail\ x))$$
$$Teleportation = \lambda q^{S(\mathbb{B})}.\text{bob}\ (\Uparrow^{S(\mathbb{B}\otimes\mathbb{B}\otimes\mathbb{B})}_{S(\mathbb{B}\otimes\mathbb{B}\otimes S(\mathbb{B}))} \text{alice}\ (q\otimes(\text{epr}\ \ |0\rangle\otimes|0\rangle)))$$

$$\vdash Teleportation : S(\mathbb{B}) \Rightarrow S(\mathbb{B})$$
$$Teleportation\ q \longrightarrow_{(1)} q$$