Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales
Departamento de Computación

Una extensión polimórfica para los λ-cálculos cuánticos λ_ρ y λ_ρ°

Tesis de Licenciatura en Ciencias de la Computación

Lucas Rafael Romero

Director: Alejandro Díaz-Caro

Buenos Aires, 2020

UNA EXTENSIÓN POLIMÓRFICA PARA LOS λ-CÁLCULOS CUÁNTICOS λ_ρ Y λ_ρ°

En 2017 Díaz-Caro presentó dos extensiones al cálculo lambda simplemente tipado que modelaban el cómputo cuántico, llamadas λ_ρ y λ_ρ°. La novedad de estos cálculos radica en que representan los sistemas cuánticos mediante sus matrices de densidad asociadas haciendo que el cálculo esté más cercano a su semántica. El paper original contiene las demostraciones de las propiedades de subject reduction y progreso. En 2019 Borgna demostró en su tesis de licenciatura la normalización fuerte de los cálculos mediante una traducción al cálculo cuántico λ_q de Selinger y Valiron.

Este trabajo apunta a extender ambos cálculos con un sistema de tipado polimórfico *a la Curry*, extensión de System F, y contextos de tipado un poco más permisivos. Sobre estas extensiones demostramos que se mantienen subject reduction y presentamos una demostración de normalización fuerte mediante candidatos de reducibilidad. También probamos que λ_ρ° es confluente, y utilizando la noción de confluencia probabilística definida por Martínez en 2018, presentamos las dificultades y posibles enfoques para lograr la confluencia de λ_ρ.

Palabras claves: Lambda cálculo, Computación cuántica, Polimorfísmo, Reducción probabilística, Subject reduction, Normalización fuerte, Confluencia.

A POLIMORPHIC EXTENSION FOR THE QUANTUM λ-CALCULI λ_ρ AND λ_ρ°

In 2017 Díaz-Caro presented two extensions for the simply typed lambda calculus called λ_ρ and λ_ρ° modelling quantum computing. The novelty in these calculi stems from the fact that they represent quantum system using density matrices. The original paper proved both subject reduction and progress. In 2019 Borgna showed a translation between these calculi and the quantum λ-calculus λ_q. In this way, he proved strong normalization for both calculi.

This work focuses on extending both calculi with a polimorphic typing system *a la Curry*, as an extension to System F and with slightly more permissive typing contexts. From these extensions we prove that subject reduction still holds and we give a proof for strong normalization using reducibility candidates. We also prove that λ_ρ° is confluent, and using the notion of probabilistic confluence defined by Martínez in 2018, we explore the dificulties and posible approaches for achieving confluence for λ_ρ.

Keywords: Lambda calculus, Quantum computing, Polimorphism, Probabilistic reductions, Subject reduction, Strong normalization, Confluence.

AGRADECIMIENTOS

A mi familia que me bancó todo este trayecto desde el principio.
A mis amigues que evitan que me vuelva completamente loco, o completamente cuerdo.
A Jano, por darme la oportunidad de trabajar en el tema y continuar hacia adelante.
Al lector de esta tesis, por su tiempo.

A mis personas favoritas.

Índice general

1. INTRODUCCIÓN

Hay varios λ-cálculos capaces de modelar computación cuántica, por ejemplo: [1, 2, 7, 16, 19, 21, 24]. Sin embargo, estos modelos se basan en vectores en espacios vectoriales para interpretar los estados cuánticos. Hay otra interpretación posible, las matrices de densidad. La ventaja de este enfoque, radica en la capacidad de representar estados mixtos, los cuales representan distribuciones probabilísticas de estados cuánticos.

Bajo esta idea está definido λ_ρ. Las matrices están representadas como términos del cálculo junto con las mediciones y las operaciones unitarias. La forma de representar una medición que puede tener distintos resultados es a través de reducciones probabilísticas. Estas toman un estado cuántico y reducen a uno de los posibles estados después de medirlo.

Los estados mixtos nos permiten modelar mediciones sobre las cuales no se conoce el resultado. Esta idea es el fundamento de λ_ρ°, una variación de λ_ρ donde las estructuras de control junto a las mediciones reducen a distribución probabilística representada por una combinación lineal de los posibles términos resultantes, lo que se puede considerar una generalización de los estados mixtos.

Además de como tratan los datos, vectores en un espacio vectorial o matrices de densidad, otra forma de separar los cálculos cuánticos es por como definen sus estructuras de control. La idea de datos cuánticos / control clásico definida por Selinger en [18] postula que las computadoras cuánticas van a correr en un dispositivo especializado junto a una computadora clásica [19,24]. Está computadora clásica será la que le de las instrucciones al dispositivo cuántico sobre que operaciones aplicar en determinados qubits. Por otro lado, se encuentra el paradigma de datos y control cuántico. La idea radica en dar nociones computacionales de los conceptos de espacios de vectores y funciones bilineales [8–10].

El cálculo λ_ρ cae bajo el paradigma de datos cuánticos y control clásico, donde los datos cuánticos están dados por las matrices de densidad. Similar a la interpretación de los diagramas de flujos cuánticos presentados en [18]. El cálculo λ_ρ° no cae completamente bajo el paradigma de control y datos cuánticos ya que no es posible realizar una superposición de programas. Sin embargo, consideramos las matrices de densidad de un estado mixto a partir de una medición. Entonces podemos catalogar el control como control probabilístico o una forma más débil de control cuántico.

Hasta la fecha, se demostraron subject reduction, progreso y strong normalization tanto para λ_ρ como λ_ρ°. El objetivo de este trabajo es expandir el tipado original de los cálculos con una extensión polimórfica como la de System F. Además tomamos contextos de tipado más permisivos en un caso particular. Esto nos permitirá expandir el poder expresivo de los cálculos y darnos una base para razonar sobre sus propiedades.

A lo largo de esta tesis apuntamos a probar que tanto subject reduction como normalización fuerte se mantienen para las extensiones propuestas. Además, si bien se conjeturaba que λ_ρ y λ_ρ° son cálculos confluentes, hasta el momento no había una demostración concreta. Nos proponemos demostrar confluencia para las extensiones y, por consiguiente a los cálculos originales.

Para el caso de λ_ρ° la demostración es bastante directa. Sin embargo, λ_ρ requiere un estudio más complejo. Primero hay que definir qué significa que un cálculo sea confluente cuando sus reducciones son probabilísticas. Para esto nos apoyamos en la tesis de licenciatura de Guido Martínez [14] y definimos estructuras que van a modelar los espacios de posibilidades a los cuales puede reducir un término. Una particularidad que encontramos es que si bien el cálculo original λ_ρ es confluente, la extensión definida no lo es. Esto se debe a que se pierde la propiedad de afinidad del tipado. Más adelante damos posibles soluciones comunes en la literatura para enfrentar el problema.

El outline de la tesis es el siguiente:

- En el capítulo 2 presentamos conceptos preliminares de tipado polimórfico, confluencia probabilística y computación cuántica.
- En el capítulo 3 damos cuenta de los cálculos originales λ_ρ y λ_ρ° junto a las propiedades ya probadas sobre ellos.
- En el capítulo 4 definimos las extensiones pertinentes a este trabajo y analizamos los cálculos resultantes.
- En el capítulo 5 exponemos nuestras conclusiones y posibles líneas de trabajo futuro.

2. PRELIMINARES

2.1. System F

System F es una extensión al sistema de tipos del λ-cálculo simplemente tipado introducido independientemente por Girard [11] y Reynolds [17]. La motivación de Girard estaba en la de teoría de pruebas, relacionando demostrabilidad en lógica de segundo orden con la expresibilidad en System F. La motivación de Reynolds venía por el lado de la programación, donde intentaba capturar la noción de polimorfismo. Los papers originales tomaban un tipado *a la Church*. En este trabajo tomamos como base la versión del tipado *a la Curry*, ver por ejemplo [4]. Otro de los nombres que toma este sistema es $\lambda 2$, vamos a utilizar indistintamente los dos nombres.

2.1.1. El cálculo

Los términos del cálculo son los mismos que los del λ-cálculo simplemente tipado. Cuenta con variables, abstracciones y aplicaciones:

$$t := x \mid \lambda x.t \mid tt$$

Las reglas de reducción también se mantienen:

$$(\lambda x.t)r \to t[r/x]$$

$$\frac{t \to r}{\lambda x.t \to \lambda x.r} \qquad \frac{t \to r}{ts \to rs} \qquad \frac{t \to r}{st \to sr}$$

Los tipos están definidos inductivamente de la siguiente manera:

1. Las variables de tipo son tipos.
2. Si σ y τ son tipos, entonces $\sigma \to \tau$ es un tipo.
3. Si σ es un tipo y X una variable de tipo, entonces $\forall X.\sigma$ es un tipo.

Para entender la idea de polimorfismo en el λ-cálculo, consideremos la función identidad:

$$\vdash \lambda x.x : \sigma \to \sigma$$

Para algún σ arbitrario. En $\lambda 2$ podemos definirla de la siguiente manera:

$$\vdash \lambda x.x : \forall X.X \to X$$

Donde X es una variable de tipo, para indicar que $\lambda x.x$ tiene todos los tipos posibles $\sigma \to \sigma$. La intuición del $\forall$ podría decir que $\forall X.\sigma$ define una función que para cada tipo τ, asocia a un tipo $\sigma[\tau/X]$. Formalmente lo definimos como sigue.

Definición 2.1.1 (Sistema de tipado de $\lambda 2$)**.** El sistema de tipos de $\lambda 2$ queda definido de la siguiente manera:

$$\sigma = X \mid \sigma \to \sigma \mid \forall X.\sigma$$

Donde X representa un elemento en el conjunto de variables de tipo V.

Para una variable de tipo X y tipo σ vamos a notar $X \in \mathrm{FV}(\sigma)$ si X no está ligada por un cuantificador $\forall$ dentro de σ. A su vez notamos para un contexto Γ, $X \in \mathrm{FV}(\Gamma)$ si X aparece libre en algún tipo del contexto.

$$\frac{}{\Gamma, x:\sigma \vdash x:\sigma}\ \mathsf{ax} \qquad \frac{\Gamma, x:\sigma \vdash t:\tau}{\Gamma \vdash \lambda x.t : \sigma \to \tau}\ \to_i \qquad \frac{\Gamma \vdash t:\sigma \to \tau \quad \Gamma \vdash r:\sigma}{\Gamma \vdash tr:\tau}\ \to_e$$

$$\frac{X \notin \mathrm{FV}(\Gamma) \quad \Gamma \vdash t:\sigma}{\Gamma \vdash t : \forall X.\sigma}\ \forall_i \qquad \frac{\Gamma \vdash t : \forall X.\sigma}{\Gamma \vdash t : \sigma[X/\tau]}\ \forall_e$$

Vamos a tomar las reglas de introducción y eliminación del cuantificador universal para introducir la noción de polimorfismo en los cálculos con los que vamos a trabajar.

2.2. Propiedades de System F

A lo largo de este trabajo nos centraremos en demostrar tres propiedades de System F para la extensión polimórfica de λ_ρ. Estas son: Subject Reduction, Normalización Fuerte y Confluencia. Pasamos a enunciar y demostrar cada una de ellas.

2.2.1. Subject Reduction

Esta propiedad asegura que la reducción preserva el tipo. Más formalmente:

Teorema (Subject Reduction para System F)**.** $\Gamma \vdash t:\sigma$ *y* $t \to s$*, entonces* $\Gamma \vdash s:\sigma$*.*

Seguimos la demostración de [4] con las modificaciones de [1]. Primero definimos la relación $\sigma \prec \tau$ entre dos tipos.

Definición 2.2.1 (definición de $\prec$)**.** Para todo par de tipos σ y τ, contexto Γ y todo término t tales que $\Gamma \vdash t:\tau$ como consecuencia de $\Gamma \vdash t:\sigma$:

1. Si $X \notin FV(\Gamma)$, se nota $\sigma \prec^t_{X,\Gamma} \tau$ si pasa alguno de los siguientes casos:
   - $\tau = \forall X.\sigma$.
   - $\sigma = \forall X.\sigma'$ y $\tau = \sigma'[\gamma/X]$ para algún γ y X.
2. Si V es un conjunto de variables de tipo tal que $V \cap FV(\Gamma) = \varnothing$, definimos $\preceq^t_{V,\Gamma}$ inductivamente como:
   - Si $X \in V$ y $\sigma \prec^t_{X,\Gamma} \tau$, entonces $\sigma \preceq^t_{\{X\},\Gamma} \tau$.
   - Si $V_1, V_2 \subseteq V$, $\sigma \preceq^t_{V_1,\Gamma} \tau$ y $\sigma \preceq^t_{V_2,\Gamma} \tau$ entonces, $\sigma \preceq^t_{V_1 \cup V_2,\Gamma} \tau$.

- Si $\sigma = \tau$, entonces $\sigma \preceq^t_{V,\Gamma} \tau$.

Notar que hay solo 2 reglas en las cuales el sujeto no cambia, la eliminación e introducción del $\forall$. Se pueden aplicar estas reglas de manera consecutiva varias veces, obteniendo así:

$$\dfrac{\dfrac{\Gamma \vdash t : \sigma}{\vdots}}{\Gamma \vdash t : \tau}$$

La definición de $\preceq$ es tal que $\sigma \preceq^t_{V,\Gamma} \tau$, donde V contiene a las variables de tipo ligadas por los cuantificadores universales.

Lo siguiente a demostrar es la estabilidad de la relación con respecto a la $\to$

Lema 2.2.2 (Estabilidad de $\preceq$)**.** Para todo par de tipos σ, τ, conjunto de variables de tipo V, términos t y r y contexto Γ, si $\sigma \preceq^t_{V,\Gamma} \tau$, $t \to r$ y $\Gamma \vdash r : \sigma$, entonces $\sigma \preceq^r_{V,\Gamma} \tau$.

Demostración. Basta mostrar que el lema vale para $\prec^t_{X,\Gamma}$ con $X \in V$. Como $\sigma \prec^t_{X,\Gamma} \tau$, sabemos que $X \notin \mathrm{FV}(\Gamma)$. Solo tenemos que probar que $\Gamma \vdash r : \tau$ a partir de $\Gamma \vdash r : \sigma$. Analizamos los casos:

- $\tau = \forall X.\sigma$, entonces usando la regla $\forall_i$ podemos deducir $\Gamma \vdash r : \tau$.
- $\sigma = \forall X.\sigma'$ y $\tau = \sigma'[\gamma/X]$ para algún γ y X. En este caso usando la regla $\forall_e$ llegamos a $\Gamma \vdash r : \tau$. □

Lemas auxiliares

Vamos a notar un vector de variables o tipos con $\vec{(\cdot)}$. Entonces podemos escribir una sucesión de sustituciones de la siguiente manera:

$$t[\sigma_1/X_1][\sigma_2/X_2]\cdots[\sigma_n/X_n] = t[\vec{\sigma}/\vec{X}]$$

El siguiente lema que queremos demostrar postula que si un par de tipos flecha están ordenadas por la relación $\preceq$, estas son equivalentes bajo ciertas sustituciones. Para llegar a eso primero definimos un mapeo $\overline{(\cdot)}$ inductivamente de la siguiente manera:

$$\begin{aligned}\overline{(X)} &= X\\ \overline{(\sigma \to \tau)} &= \sigma \to \tau\\ \overline{(\forall X.\sigma)} &= \overline{(\sigma)}\end{aligned}$$

Luego hay que demostrar dos lemas intermedios:

Lema 2.2.3.

1. Para todo par de tipos σ y τ, existe un tipo γ tal que: $\overline{(\sigma[\tau/X])} = \overline{(\sigma)}[\gamma/X]$.
2. Para todo par de tipos σ y τ, un conjunto de variables V, contexto Γ y término t, si $\sigma \preceq^t_{V,\Gamma} \tau$, entonces existen $\vec{\gamma}$ y $\vec{X} \in V$ tales que $\overline{(\tau)} = \overline{(\sigma)}[\vec{\gamma}/\vec{X}]$.

Demostración. Demostración de (1) por inducción sobre σ:

$\sigma = \sigma_1 \to \sigma_2$:
$\overline{((\sigma_1 \to \sigma_2)[\tau/X])} = \overline{(\sigma_1[\tau/X] \to \sigma_2[\tau/X])} =$
$\sigma_1[\tau/X] \to \sigma_2[\tau/X] = (\sigma_1 \to \sigma_2)[\tau/X] = \overline{(\sigma_1 \to \sigma_2)}[\tau/X]$.

$\sigma = X$:
$\overline{(X[\tau/X])} = \overline{(\tau)} = X[\overline{(\tau)}/X] = \overline{(X)}[\overline{(\tau)}/X]$.

$\sigma = Y$: Con $Y \neq X$
$\overline{(Y[\tau/X])} = Y = \overline{(Y)}[\tau/X]$.

$\sigma = \forall Y.\sigma_1$: Con $Y \neq X$ y $Y \notin \mathrm{FV}(\tau)$
$\overline{((\forall Y.\sigma_1)[\tau/X])} = \overline{((\forall Y.\sigma_1[\tau/X]))} = \overline{(\sigma_1[\tau/X])}$ Por hipótesis inductiva tenemos que $\overline{(\sigma_1[\tau/X])} = \overline{(\sigma_1)}[\gamma/X] = \overline{(\forall Y.\sigma_1)}[\gamma/X]$.

Para demostrar (2) es suficiente con mostrarlo para $\sigma \prec^t_{X,\Gamma} \tau$:

Caso 1: $\tau = \forall X.\sigma$, entonces $\overline{(\tau)} = \overline{(\sigma)}$.

Caso 2: $\sigma = \forall X.\sigma'$ y $\tau = \sigma'[\gamma/X]$. Por el resultado anterior se tiene que $\overline{(\tau)} = \overline{(\sigma'[\gamma/X])} = \overline{(\sigma')}[\gamma'/X] = \overline{(\sigma)}[\gamma'/X]$ para algún γ'. □

Con estos 2 resultados intermedios, podemos demostrar el lema de comparación de flechas:

Lema 2.2.4 (Comparación de flechas)**.** Para tipos $\sigma, \tau, \sigma'\tau'$, contexto Γ, conjunto de variables de tipo V y término t tales que $\sigma \to \tau \preceq^t_{V,\Gamma} \sigma' \to \tau'$, existen tipos $\vec{\gamma}$ y variables $\vec{X} \subseteq V$ tal que:

$$\sigma' \to \tau' = (\sigma \to \tau)[\vec{\gamma}/\vec{X}].$$

Demostración. $\sigma' \multimap \tau' = \overline{(\sigma' \multimap \tau')}$. Por el lema 2.2.3 (2), existen tipos $\vec{\gamma}$ y variables de tipo $\vec{X}$ tales que:

$$\overline{(\sigma' \multimap \tau')} = \overline{(()\sigma \multimap \tau)}[\vec{\gamma}/\vec{X}] = \sigma \multimap \tau[\vec{\gamma}/\vec{X}]$$

□

Demostrar subject reduction significa demostrar que cada regla de reducción preserva el tipo. Vamos a analizar cada componente del término junto con sus tipos y tratar de llegar al reducto. Para ello utilizamos los lemas de generación, pasamos a enunciarlos para sus respectivas reglas. La demostración se consigue aplicando inducción sobre los juicios de tipado.

Lema 2.2.5 (Lemas de generación)**.**

variable Si $\Gamma \vdash x : \sigma$, entonces existen tipo τ, conjunto de variables de tipo V con $\tau \preceq^x_{V,\Gamma} \sigma$ tales que $x : \tau \in \Gamma$.

app Si $\Gamma \vdash tr : \sigma$, entonces, existen tipos τ, σ', conjunto de variables de tipo V con $\sigma' \preceq^{tr}_{V,\Gamma} \sigma$ tales que $\Gamma \vdash t : \tau \to \sigma'$ y $\Gamma \vdash r : \tau$.

abs Si $\Gamma \vdash \lambda x.t : \sigma$, entonces, existen tipos τ, σ', conjunto de variables de tipo V con $\tau \to \sigma' \preceq^{\lambda x.t}_{V,\Gamma} \sigma$ tales que $\Gamma, x : \tau \vdash t : \sigma'$. □

A continuación, presentamos los lemas de strengthening y weakening. Utilizaremos estos lemas para demostrar el lema de sustitución, la última pieza necesaria para probar subject reduction. Ambos lemas se pueden demostrar mediante inducción sobre la derivación del tipo de t.

Lema 2.2.6 (weakening)**.** Si $\Gamma \vdash t : \sigma$ y $x \notin \mathrm{FV}(t)$ entonces, $\Gamma, x : \tau \vdash t : \sigma$. □

Lema 2.2.7 (stregthening)**.** Si $\Gamma, x : \tau \vdash t : \sigma$ y $x \notin \mathrm{FV}(t)$ entonces, $\Gamma \vdash t : \sigma$. □

Finalmente, enunciamos el último lema necesario para llevar a cabo la demostración de subject reduction.

Lema 2.2.8 (Lema de sustitución)**.** Si $\Gamma, x : \tau \vdash t : \sigma$ y $\Delta \vdash r : \tau$, entonces $\Gamma, \Delta \vdash t[r/x] : \sigma$.

Demostración. Por inducción en t:

$t = x$: Por lema 2.2.5 (variable), existen tipo τ, conjunto de variables de tipo V con $\tau <^t_{V,\Gamma} \sigma$ tales que $x : \tau \in \Gamma$. Por lema 2.2.6, $\Gamma, \Delta \vdash r : \tau$. Por definición 2.2.1 $\Gamma, \Delta \vdash r : \sigma$. Notar que $t[r/x] = r$.

$t = y$ con $y \neq x$: Entonces por lemas 2.2.6 y 2.2.7, $\Gamma, \Delta \vdash y : \sigma$. Notar que $t[r/x] = t$.

$t = \lambda y.s$ con $y \neq x$ y $y \notin FV(r)$: Entonces $\Gamma, x : \tau \vdash \lambda y.s : \sigma$. Por lema 2.2.5 (abs) existen tipos γ_1, γ_2 y variables de tipo V con $\gamma_1 \to \gamma_2 \leq^t_{V,\Gamma} \sigma$ tales que $\Gamma, x : \tau, y : \gamma_1 \vdash s : \gamma_2$.

Por hipótesis inductiva, $\Gamma, \Delta, y : \gamma_1 \vdash s[r/x] : \gamma_2$. Aplicando la regla $\to_i$ nuevamente tenemos $\Gamma, \Delta \vdash \lambda y.s[r/x] : \gamma_1 \to \gamma_2$. Por definición de la relación 2.2.1 llegamos a $\Gamma, \Delta \vdash \lambda y.s[r/x] : \sigma$.

$t = t_1 t_2$: Entonces $\Gamma, x : \tau \vdash t_1 t_2 : \sigma$. Por lema 2.2.5 (app), existen tipos γ, σ' y variables de tipo V con $\sigma' \leq^t_{V,(\Gamma, x:\tau)} \sigma$ tales que $\Gamma, x : \tau \vdash t_1 : \gamma \to \sigma'$ y $\Gamma \vdash t_2 : \sigma$.

Por hipótesis inductiva, $\Gamma, \Delta \vdash t_1[r/x] : \gamma \to \sigma'$ y $\Gamma, \Delta \vdash t_2[r/x] : \gamma$, entonces por regla $\to_e$, $\Gamma, \Delta \vdash (t_1 t_2)[r/x] : \sigma'$. Finalmente, por definición de la relación 2.2.1 $\Gamma, \Delta \vdash (t_1 t_2)[r/x] : \sigma$. □

Con estos lemas definidos, tenemos las piezas para demostrar la propiedad de *Subject Reduction* para $\lambda 2$.

Demostración de *Subject Reduction*

Teorema 2.2.9 (Subject reduction para $\lambda 2$)**.** *Para todo par de términos t y t', contexto Γ y tipo σ. Si $t \to t'$ y $\Gamma \vdash t : \sigma$, entonces $\Gamma \vdash t' : \sigma$.*

Demostración. Demostración por inducción sobre $\to$.

- $t = (\lambda x.s)r$ y $t' = t[r/x]$.

  $\Gamma \vdash (\lambda x.s)r : \sigma$. Por lema de 2.2.5 (app) tenemos que $\exists\ \gamma, \tau$ con $\gamma \leq^t_{V_1,\Gamma} \sigma$ tales que $\Gamma \vdash \lambda x.s : \tau \to \gamma$ y $\Gamma \vdash r : \tau$.

  Aplicamos el lema 2.2.5 (abs) para $\Gamma \vdash \lambda x.s : \tau \to \gamma$ y obtenemos γ', τ'con $\tau' \to \gamma' \leq^{\lambda x.s}_{V_2,\Gamma} \tau \to \gamma$ tales que $\Gamma, x : \tau' \vdash s : \gamma'$.

Por lema 2.2.4 existen tipos $\vec{\chi}$ y variables de tipo $\vec{X} \in V$ tales que $\gamma = \gamma'[\vec{\chi}/\vec{X}]$ y $\tau = \tau'[\vec{\chi}/\vec{X}]$.

Además, como $\vec{X} \notin FV(\Gamma)$, ya que son las variables de tipo ligadas por los $\forall$, $\Gamma[\vec{\chi}/\vec{X}] = \Gamma$, entonces por definición 2.2.1, $\Gamma, x : \tau \vdash s : \gamma$ y por lema 2.2.8, $\Gamma, \Delta \vdash s[r/x] : \gamma$. Por lema 2.2.2, tenemos que $\Gamma, \Delta \vdash s[r/x] : \sigma$.

Continuamos con los casos contextuales. Sea $s \to s'$:

- $t = \lambda x.s$ y $t' = \lambda x.s'$.

  $\Gamma \vdash \lambda x.s : \sigma$. Por lema 2.2.5 (abs), existen tipos τ, γ y variables de tipo V tales que $\tau \to \gamma \leq^t_{V,\Gamma} \sigma$ y $\Gamma, x : \tau \vdash s : \gamma$. Por HI, $\Gamma, x : \tau \vdash s' : \gamma$. Aplicando la introducción de la abstracción llegamos a $\Gamma \vdash \lambda x.s' : \tau \to \gamma$. Por definición 2.2.1 y lema 2.2.2 obtenemos $\Gamma \vdash \lambda x.s' : \sigma$.

- $t = sr$ y $t' = s'r$.

  $\Gamma \vdash rs : \sigma$. Por el lema 2.2.5 (app), existen tipos τ, γ y variables de tipo V tales que $\gamma \leq^t_{V,\Gamma} \sigma$ y $\Gamma \vdash s : \tau \to \gamma$ y $\Gamma \vdash r : \gamma$. Por HI, $\Gamma \vdash s' : \tau \to \gamma$. Por regla $\to_e$, $\Gamma \vdash s'r : \gamma$. Luego, por definición 2.2.1 y lema 2.2.2 llegamos a $\Gamma \vdash rs' : \sigma$.

- $t = rs$ y $t' = rs'$.

  $\Gamma \vdash rs : \sigma$. Por el lema 2.2.5 (app), existen tipos τ, γ y variables de tipo V tales que $\gamma \leq^t_{V,\Gamma} \sigma$ y $\Gamma \vdash r : \tau \to \gamma$ y $\Gamma \vdash s : \tau$. Por hipótesis inductiva, $\Gamma \vdash s' : \tau$. Por regla $\to_e$, $\Gamma \vdash rs' : \gamma$. Finalmente por definición 2.2.1 y lema 2.2.2 llegamos a $\Gamma \vdash rs' : \sigma$. □

2.2.2. Normalización Fuerte

La propiedad de *Strong normalization* asegura que todo término t perteneciente al sistema, tiene una cantidad finita de reducciones y siempre llega a una forma normal. Una forma normal es aquella que no se puede reducir. Es decir, términos como $\Omega = (\lambda x.xx)(\lambda x.xx)$ que tienen una cantidad infinitas de β-reducciones, no son tipables dentro de $\lambda 2$.

Damos una idea de la demostración que vamos a construir en la siguiente sección. Esta se basa en la demostración mediante candidatos de reducibilidad. Vamos a definir un candidato de reducibilidad como un subconjunto de términos cerrado bajo ciertas reglas contenido en el conjunto de términos fuertemente normalizantes. A continuación definiremos una interpretación para cada tipo que deriva en un candidato de reducibilidad. Finalmente, mostramos que cada término está contenido en la interpretación de su tipo.

Vamos a enunciar lemas y definiciones que van a facilitar la demostración de la propiedad. Primero definimos la noción de neutralidad. Llamamos términos neutrales a las variables y a las aplicaciones. Adicionalmente definimos $\mathrm{Red}(t) = \{t' \mid t \to t'\}$, el conjunto de reductos de t en un paso. Un conjunto de términos U es un candidato de reducibilidad (notado $U \in \mathrm{CR}$) si cumple las siguientes condiciones:

CR1: $R \subseteq \mathrm{SN}$.

CR2: Si $t \in R$ y $t \to t'$, entonces $t' \in R$.

CR3: Si t neutral y $\mathrm{Red}(t) \subseteq R$, entonces $t \in R$.

Definimos inductivamente la siguiente interpretación de tipos:

$$\begin{aligned}
[\![X]\!]_\alpha &= \alpha(X) && \text{Donde } \alpha \text{ es una valuación tal que } \alpha : V \to \mathrm{CR}.\\
[\![\sigma \to \tau]\!]_\alpha &= [\![\sigma]\!]_\alpha \to [\![\tau]\!]_\alpha && \text{Donde } R_1 \to R_2 = \{t \mid \forall v \in R_1, tv \in R_2\}.\\
[\![\forall X.\sigma]\!]_\alpha &= \bigcap_{R \in CR} [\![\sigma]\!]_{\alpha, X=R}
\end{aligned}$$

Tomamos α como una función total en $V \to CR$ y notamos $\alpha, X = R$ como la función α redefinida para $X = R$. De aquí en adelante definimos $|t|$ como la máxima cantidad de reducciones de t hasta llegar a una forma normal. Vamos a utilizar esta notación en el siguiente lema y en las demostraciones de normalización fuerte en las siguientes secciones.

Lema 2.2.10. Para todo tipo σ, $[\![\sigma]\!]_\alpha \in \mathrm{CR}$.

Demostración. Probamos por inducción en σ:

- $[\![\sigma \to \tau]\!]_\alpha = \{t \mid \forall v \in [\![\sigma]\!]_\alpha,\ tv \in [\![\tau]\!]_\alpha\}$.

  CR1: $tv \in [\![\tau]\!]_\alpha$. Por HI $[\![\tau]\!]_\alpha \in \mathrm{CR}$. Entonces $tv \in \mathrm{SN}$ luego, $t \in \mathrm{SN}$.

  CR2: $t \in [\![\sigma \to \tau]\!]_\alpha$. Entonces $\forall v \in [\![\sigma]\!]_\alpha,\ tv \in [\![\tau]\!]_\alpha$. Por HI $\forall v \in [\![\sigma]\!]_\alpha,\ t'v \in [\![\tau]\!]_\alpha$. Luego $t' \in [\![\sigma \to \tau]\!]_\alpha$.

  CR3: $\mathrm{Red}(t) \subseteq [\![\sigma \to \tau]\!]_\alpha$ y t neutral. Entonces $\forall t' \in \mathrm{Red}(t)$ y $v \in [\![\sigma]\!]_\alpha, t'v \in [\![\tau]\!]_\alpha$. Por HI, $[\![\sigma]\!]_\alpha \in \mathrm{CR}$. Por lo tanto, $v \in \mathrm{SN}$.

  Razonando por inducción en $|v|$, $\forall v \in [\![\sigma]\!]_\alpha$ tv reduce a:

  1. $t'v$ con t' a un paso de t, pero $t' \in [\![\sigma \to \tau]\!]_\alpha$. Entonces, $t'v \in [\![\tau]\!]_\alpha$.
  2. tv' con $|v'| < |v|$. Por la segunda HI $tv' \in [\![\tau]\!]_\alpha$.

  Dado que t es neutral, las anteriores son las únicas reducciones posibles. Entonces $\mathrm{Red}(tv) \subseteq [\![\tau]\!]_\alpha$ y como es una aplicación tv es neutral. Entonces por la HI original (CR3) $\forall v \in [\![\sigma]\!]_\alpha,\ tv \in [\![\tau]\!]_\alpha$. Entonces, $t \in [\![\sigma \to \tau]\!]_\alpha$.

- $[\![X]\!]_\alpha = \alpha(X)$ y por definición $\alpha(X) \in \mathrm{CR}$.

- $[\![\forall X.\sigma]\!]_\alpha = \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha, X=R}$.

  CR1: Por HI $\forall R \in \mathrm{CR}$, $[\![\sigma]\!]_{\alpha,X=R} \subseteq \mathrm{SN}$. Entonces $\bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha,X=R} \subseteq \mathrm{SN}$.

  CR2: Sea $R \in \mathrm{CR}$ y $t \in [\![\sigma]\!]_{\alpha,X=R}$. Por HI, $t' \in [\![\sigma]\!]_{\alpha,X=R}$. Entonces $\forall R \in \mathrm{CR}, t' \in \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha,X=R}$. Luego, $t' \in [\![\forall X.\sigma]\!]_\alpha$.

  CR3: Sea $R \in \mathrm{CR}$, y $\mathrm{Red}(t) \subseteq [\![\sigma]\!]_{\alpha,X=R}$. Por HI, $t \in [\![\sigma]\!]_{\alpha,X=R}$. Entonces, $t \in \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha,X=R}$. Luego, $\forall R \in \mathrm{CR},\ t \in [\![\forall X.\sigma]\!]_\alpha$. □

El lema precedente establece que las interpretaciones de los tipos definen candidatos de reducibilidad. Lo siguiente es demostrar que las variables pertenecen a las interpretaciones de todos los tipos. Un corolario de esto es que los candidatos de reducibilidad nunca son vacios.

Lema 2.2.11. Para toda variable x, tipo σ, y valuación α, $x \in [\![\sigma]\!]_\alpha$.

Demostración. La variable x es neutral y $\mathrm{Red}(x) = \varnothing \subseteq [\![\sigma]\!]_\alpha$. Por CR3, $x \in [\![\sigma]\!]_\alpha$. □

Dado un contexto Γ, decimos que una sustitución χ satisface Γ con la valuación α (Notado $\chi, \alpha \vDash \Gamma$) cuando $x : \sigma \in \Gamma \Rightarrow \chi(x) \in [\![\sigma]\!]_\alpha$. Un juicio de tipado $\Gamma \vdash t : \sigma$ se dice válido (notado $\Gamma \vDash t : \sigma$) si para cada valuación α y sustitución χ que satisfacen Γ tenemos que $\chi(t) \in [\![\sigma]\!]_\alpha$.

Antes de demostrar adecuación, vamos a necesitar un lema auxiliar para el caso de $\forall_e$.

Lema 2.2.12. Para todo tipo σ y τ y toda valuación α definida en $(\mathrm{FV}(\sigma) \setminus \{X\}) \cup \mathrm{FV}(\tau)$,

$$[\![\sigma[\tau/X]]\!]_\alpha = [\![\sigma]\!]_{\alpha, X = [\![\tau]\!]_\alpha}$$

Demostración. Demostramos mediante inducción en la forma de σ.

$\sigma = \sigma_1 \to \sigma_2$
$[\![(\sigma_1 \to \sigma_2)[\tau/X]]\!]_\alpha = [\![\sigma_1[\tau/X] \to \sigma_2[\tau/X]]\!]_\alpha = [\![\sigma_1[\tau/X]]\!]_\alpha \to [\![\sigma_2[\tau/X]]\!]_\alpha$. Por hipótesis inductiva, es igual a $[\![\sigma_1]\!]_{\alpha, X=[\tau/X]} \to [\![\sigma_2]\!]_{\alpha, X=[\![\tau]\!]_\alpha} = [\![\sigma_1 \to \sigma_2]\!]_{\alpha, X=[\![\tau]\!]_\alpha}$.

$\sigma = X$
$[\![X[\tau/X]]\!]_\alpha = [\![\tau]\!]_\alpha$. Podemos redefinir α de manera tal que $X = [\![\tau]\!]_\alpha$. Entonces, $[\![\tau]\!]_\alpha = [\![X]\!]_{\alpha, X=[\![\tau]\!]_\alpha}$.

$\sigma = Y$ Con $Y \neq X$
$[\![Y[\tau/X]]\!]_\alpha = [\![Y]\!]_\alpha$. Podemos redefinir α de manera tal que $X = [\![\tau]\!]_\alpha$. Entonces, $[\![Y]\!]_\alpha = [\![Y]\!]_{\alpha, X=[\![\tau]\!]_\alpha}$.

$\sigma = \forall Y.\sigma'$ Con $Y \neq X$ y $Y \notin \mathrm{FV}(\tau)$
$[\![(\forall Y.\sigma')[\tau/X]]\!]_\alpha = [\![\forall Y.\sigma'[\tau/X]]\!]_\alpha = \bigcap_{R \in CR} [\![\sigma'[\tau/X]]\!]_{\alpha, Y=R}$. Aplicando la hipótesis inductiva, llegamos a $\bigcap_{R \in CR} [\![\sigma']\!]_{\alpha, Y=R, X=[\![\tau]\!]_\alpha} = [\![\forall Y.\sigma']\!]_{\alpha, X=[\![\tau]\!]_\alpha}$. □

Ya tenemos las herramientas para demostrar el lema de adecuación.

Lema 2.2.13 (Adecuación)**.** Todo juicio de tipado es válido. Es decir, para todo contexto Γ, término t y tipo σ, tales que $\Gamma \vdash t : \sigma$ se tiene $\Gamma \vDash t : \sigma$.

Demostración. Probamos por inducción en el juicio de tipado.

$\Gamma, x : \sigma \vdash x : \sigma$
Si $\chi, \alpha \vDash \Gamma, x : \sigma$. Entonces $\chi(x) \in [\![\sigma]\!]_\alpha$. Cumple por definición.

$\Gamma \vdash \lambda x.t : \sigma \to \tau$
Sean $\chi, \alpha \vDash \Gamma$. Para probar que $\chi(\lambda x.t) \in [\![\sigma \to \tau]\!]_\alpha$, hay que ver que $\forall r \in [\![\sigma]\!]_\alpha$, $\chi(\lambda x.t) r \in [\![\tau]\!]_\alpha$.

Si $\mathrm{Red}(\chi(\lambda x.t) r) \subseteq [\![\tau]\!]_\alpha$, dado que el término es neutral podemos concluir por CR3 que $\chi(\lambda x.t) r \in [\![\tau]\!]_\alpha$. Las siguientes son las reducciones posibles razonando por inducción en $|r| + |t|$.

- $\chi(\lambda x.t) r = (\lambda x.\chi(t)) r \to [r/x], \chi(t)$. Como $\chi, \alpha \vDash \Gamma$ entonces, $[r/x], \chi, \alpha \vDash \Gamma, x : \sigma$. Por hipótesis inductiva $\Gamma, x : \sigma \vDash t : \tau$, luego $[r/x], \chi(t) \in [\![\tau]\!]_\alpha$.

- Reducción interna dentro de la abstracción, $\chi(\lambda x.t)r \to \chi(\lambda x.t')r$ con t' a un paso de t. Entonces $|t| > |t'|$ y por segunda hipótesis inductiva $\chi(\lambda x.t')r \in [\![\tau]\!]_\alpha$.
- Reducción interna en r, $\chi(\lambda x.t)r \to \chi(\lambda x.t)r'$ con r' a un paso de r. Entonces $|r| > |r'|$ y por segunda hipótesis inductiva $\chi(\lambda x.t)r' \in [\![\tau]\!]_\alpha$.

Todas las reducciones pertenecen a $[\![\tau]\!]_\alpha$, entonces por CR3 $\chi(\lambda x.t) \in [\![\sigma \to \tau]\!]_\alpha$.

$\Gamma \vdash tr : \tau$

Sean $\chi, \alpha \vDash \Gamma$. Luego por hipótesis inductiva, $\chi(t) \in [\![\sigma \to \tau]\!]_\alpha$ y $\chi(r) \in [\![\sigma]\!]_\alpha$. Además $\chi(tr) = \chi(t)\chi(r)$, con lo cual $\chi(tr) \in [\![\tau]\!]_\alpha$.

$\Gamma \vdash t : \forall X.\sigma$

Sean $\chi, \alpha \vDash \Gamma$, Si $X \notin \mathrm{FV}(\Gamma)$, entonces $\forall R \in \mathrm{CR}$, $\chi, \alpha, X = [\![R]\!]_\alpha \vDash \Gamma$. Por lo tanto $\forall R \in \mathrm{CR}$, $\chi(t) \in [\![\sigma]\!]_{\alpha, X=[\![R]\!]_\alpha}$. Finalmente, $t \in \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha, X=[\![R]\!]_\alpha} = [\![\forall X.\sigma]\!]_\alpha$.

$\Gamma \vdash t : \sigma[\tau/X]$

Sean $\chi, \alpha \vDash \Gamma$, por HI $\chi(t) \in [\![\forall X.\sigma]\!]_\alpha = \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha, X=[\![R]\!]_\alpha}$. En particular, $t \in [\![\sigma]\!]_{\alpha, X[\![\tau]\!]_\alpha}$. Por el lema 2.2.12, $t \in [\![\sigma[\tau/X]]\!]_\alpha$. □

Normalización fuerte para $\lambda 2$ es un corolario directo del lema anterior:

Teorema 2.2.14. *Todo término tipable en $\lambda 2$ es fuertemente normalizante.*

Demostración. Si un término t es tipable para un tipo σ en un contexto Γ, dado que la sustitución identidad y cualquier valuación α satisfacen trivialmente Γ, $t \in [\![\sigma]\!]_\alpha$. Por CR1, $[\![\sigma]\!]_\alpha \subseteq \mathrm{SN}$. Entonces $t \in \mathrm{SN}$. □

2.2.3. Confluencia

Primero vamos a dar las definiciones de confluencia global y local.

Definición 2.2.15. Un término t es globalmente confluente, o *Church-Rosser*(CR), si para todo s_1, s_2 con $t \to^* s_1$ y $t \to^* s_2$ existe r tal que $s_1 \to^* r$ y $s_2 \to^* r$. Si todo término cumple con esa propiedad, se dice que el sistema es globalmente confluente.

Definición 2.2.16. Un término t es localmente confluente, o *Weak Church-Rosser*(WCR), si para todo s_1, s_2 con $t \to s_1$ y $t \to s_2$ existe r tal que $s_1 \to^* r$ y $s_2 \to^* r$. Si todo término cumple con esa propiedad, se dice que el sistema es localmente confluente. La diferencia con la confluencia global es que s_1 y s_2 están separados de t por exactamente un solo paso de reducción.

Vamos a utilizar el lema de Newman [20, Teorema 1.2.1] para probar confluencia global mediante la confluencia local del sistema.

Lema 2.2.17 (Lema de Newman)**.** *Todo sistema de rescritura abstracto que satisface normalización fuerte y confluencia local, satisface confluencia global.* □

Primero vamos a definir la noción de par crítico. Encontramos un par crítico cuando un término tiene un par de redexes superpuestos. Es decir, la reducción de uno de los redex destruye el otro. Por ejemplo el término $t = (\lambda x.t)r$. En este caso, se puede reducir r, llegando a $(\lambda x.t)r'$ o aplicar la β-reducción $t[r/x]$.

En el caso anterior, luego de elegir una de las reducciones, no es posible aplicar la otra inmediatamente. El redex es destruido. A esta clase de reducciones se les llaman reducciones destructivas. Un par crítico se considera *convergente*, si existe un reducto común entre las posibles reducciones del término.

Para probar confluencia local de $\lambda 2$, vamos a usar el lema de pares críticos [20, Teorema 2.7.15].

Lema 2.2.18 (Lema de pares críticos)**.** *Un sistema de rescritura de términos es WCR sii todos sus pares críticos son convergentes.* □

Para probar que los pares críticos de $\lambda 2$ convergen, primero tenemos que demostrar algunos lemas auxiliares. Para la siguiente demostración y en adelante, vamos a definir la convención de variables a utilizar. Una variable ligada en un término t puede ser renombrada a una variable no utilizada por α-conversión. Consideramos los términos bajo α-equivalencia y adoptamos la convención de Barendregt [3, Página 11], la cual estipula que el conjunto de variables libres es disjunto del conjunto de variables ligadas, y que cada subtérmino $\lambda x.t$ liga a una variable diferente.

Lema 2.2.19 (Sustitución)**.** Si $y \notin \mathrm{FV}(r)$, entonces $t[q/y][r/x] = t[r/x][q[r/x]/y]$.

Demostración. Por inducción en t:

***t* = *x*:** Se tiene que:

$$x[q/y][r/x] = x[r/x] = r.$$

Por otro lado:

$$x[r/x][q[r/x]/y] = r[q[r/x]/y] = r \text{ porque } y \notin \mathrm{FV}(r).$$

***t* = *y*:** Por un lado:

$$y[q/y][r/x] = q[r/x].$$

Además,

$$y[r/x][q[r/x]/y] = y[q[r/x]/y] = q[r/x].$$

***t* = *z*:** Con $z \neq x$ y $z \neq y$. Primero, se tiene que:

$$z[q/y][r/x] = z.$$

Por otro lado,

$$z[r/x][q[r/x]/y] = z.$$

***t* = *λz.s*:** $z \neq x$ y $z \neq y$.

$$\begin{aligned}(\lambda z.s)[q/y][r/x] &= \lambda z.s[q/y][r/x] \text{ Por convención de variables } z \notin \mathrm{FV}(r) \cup \mathrm{FV}(q)\\ &=^{\mathrm{HI}} \lambda z.s[r/x][q[r/x]/y]\\ &= (\lambda z.s)[r/x][q[r/x]/y] \text{ Porque } z \notin \mathrm{FV}(r) \cup \mathrm{FV}(q).\end{aligned}$$

***t* = *s*₁*s*₂:** Se tiene que:

$$(s_1 s_2)[q/y][r/x] = s_1[q/y][r/x]s_2[q/y][r/x].$$

Por hipótesis inductiva, el término es igual a:

$$s_1[r/x][q[r/x]/y]s_2[r/x][q[r/x]/y] = (s_1 s_2)[r/x][q[r/x]/y].$$

□

El objetivo es probar que la sustitución se comporta de la manera esperada con respecto a la reducción. Con ese fin, definimos un par de lemas.

Lema 2.2.20. Si $t \to t'$, entonces $t[r/x] \to t'[r/x]$.

Demostración. Inducción sobre t

***t* = λ*y*.*s*:**
$\lambda y.s \to \lambda y.s'$. Entonces quiero probar que $(\lambda y.s)[r/x] \to (\lambda y.s')[r/x]$. $(\lambda y.s)[r/x] = \lambda y.s[r/x] \to^{\text{HI}} \lambda y.s'[r/x] = (\lambda y.s')[r/x]$ ya que $y \notin \text{FV}(r)$.

***t* = *s*₁*s*₂:** Hay dos casos: Reducción en la raíz y reducción interna.

- Reducción a la raíz con $s_1 = \lambda y.q$, $y \notin \text{FV}(r)$. $t = (\lambda y.q)s_2$ y $t' = q[s_2/y]$:

  $((\lambda y.q)s_2)[r/x] = (\lambda y.q[r/x])s_2[r/x]$ por convención de variables
  $\to q[r/x][s_2[r/x]/y]$
  $= q[s_2/y][r/x]$ por lema 2.2.19 ($y \notin \text{FV}(r)$ por convención de variables).

- Reducción interna: $s_1 s_2 \to s_1' s_2$ con $s_1 \to s_1'$

  $(s_1 s_2)[r/x] = s_1[r/x]s_2[r/x] \to^{\text{HI}} s_1'[r/x]s_2[r/x] = (s_1' s_2)[r/x]$.

  Similar para el caso simétrico. □

Lema 2.2.21. Si $r \to r'$, entonces $t[r/x] \to^* t[r'/x]$.

Demostración. Demostramos mediante induccion en t:

***t* = *y*:** Hay 2 casos posibles:

- $y = x$ en cuyo caso: $x[r/x] = r \to r' = x[r'/x]$.
- $y \neq x$, entonces $y[r/x] = y = y[r'/x]$.

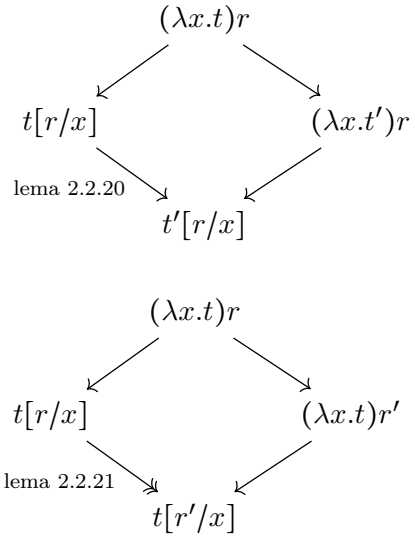
***t* = λ*y*.*s*:** con $y \notin \text{FV}(r)$
$(\lambda y.s)[r/x] = \lambda y.s[r/x]$
$\to^{\text{HI}} \lambda y.s[r'/x]$
$= (\lambda y.s)[r'/x]$ $y \notin \text{FV}(r')$ ya que la reducción no introduce variables libres.

***t* = *s*₁*s*₂:**
$(s_1 s_2)[r/x] = s_1[r/x]s_2[r/x]$
$\to^{\text{HI}^*} s_1[r'/x]s_2[r/x]$
$= (s_1 s_2)[r'/x]$. □

Teniendo estos lemas, se puede mostrar que los dos pares críticos confluyen. Dado que todos los pares críticos confluyen, podemos afirmar que $\lambda 2$ es localmente confluente.

Teorema 2.2.22. $\rightarrow$ *es WCR.*

Demostración. La demostración pasa por analizar los pares críticos de $\lambda 2$ y mostrar que son confluentes. Hay dos casos para analizar.



□

Finalmente sabiendo que el cálculo es también fuertemente normalizante, llegamos a la conclusión de que es globalmente confluente.

2.3. Confluencia probabilística

2.3.1. *Probabilistic Abstract Rewriting Systems*

Uno de los cálculos que tratamos en este trabajo hace uso de reducciones probabilísticas. Es decir, reducciones que pueden derivar en distintos términos con distintas probabilidades. Tratar con ellas es un trabajo más delicado. Primero vamos a querer definir qué significa que un cálculo sea confluente cuando tiene reducciones probabilísticas. Es evidente que la definición de confluencia que dimos en la sección anterior no es suficiente, aplicar la misma reducción a un mismo término puede desembocar en dos resultados distintos.

Con ese fin, vamos a utilizar la definición de confluencia probabilística presentada en [14]. La idea se basa en que, para cada par crítico, en lugar de considerar reducciones puntuales, analizamos el subconjunto de reductos posibles. Para cada término de ese subconjunto hay una probabilidad asociada de reducir a él y buscamos que sea la misma probabilidad tomando cualquiera de los dos caminos. El objetivo final es probar confluencia estándar sobre las distribuciones asociadas a la reducción.

Para ese análisis, primero vamos a definir $\mathcal{L}(X)$ como el conjunto de listas con elementos de tipo X donde $[\,]$, : y + representan la lista vacía, el constructor de listas y la concatenación, respectivamente. Además usamos la notación $[a, b, c]$ para referirnos a $a : b : c : [\,]$.

Luego definimos $\mathcal{D}(A)$ como el conjunto de listas finitas de pares en $\mathbb{R}_{[0,1]} \times A$ que definen una distribución. Es decir, que la suma del primer elemento de los pares da 1. No se ponen más restricciones sobre $\mathcal{D}$, en particular, un elemento de A puede aparecer más de una vez. Por ejemplo, $[(\frac{1}{8}, a), (\frac{1}{2}, b), (\frac{3}{8}, a)]$. Vamos a notar pA donde $p \in \mathbb{R}_{[0,1]}$ y $A \in \mathcal{D}(A)$ como la distribución del producto de p por el primer miembro de cada elemento de A.

En un nodo de una distribución, (p, a), p es el *peso* y a el *elemento*. Buscamos que dos distribuciones sean equivalentes si asignan el mismo peso total a cada elemento, sin tomar en cuenta el orden o elementos duplicados. Utilizamos esta representación en lugar de conjuntos ya que permiten una mayor rigurosidad en las demostraciones y en su uso facilitan el seguimiento de trazas particulares. Si bien este modelo solo contempla distribuciones finitas, es apropiado para el caso que queremos estudiar.

Con el fin de razonar sobre la equivalencia de distribuciones, definimos la relación $\sim$. Partimos de las siguientes reglas:

$$[(p_1, a_1), (p_2, a_2)] \sim [(p_2, a_2), (p_1, a_1)] \quad \text{(FLIP)}$$
$$[(p_1, a), (p_2, a)] \sim [(p_1 + p_2, a)] \quad \text{(JOIN)}$$
$$[(p_1 + p_2, a)] \sim [(p_1, a), (p_2, a)] \quad \text{(SPLIT)}$$

La relación $\sim$ está definida como la clausura congruente de esas reglas. Es decir, la relación más pequeña tal que $D_1 \sim D_2$ implica que $E_1 +\!\!+ D_1 +\!\!+ E_2 \sim E_1 +\!\!+ D_2 +\!\!+ E_2$. Decimos que dos ditribuciones son equivalentes si están relacionadas por la clausura reflexiva-transitiva de $\sim$ y lo notamos $\approx$. Esta relación cumple con las características que buscamos.

Luego, definimos la noción de PARS (*Probabilistic Abstract Rewriting System*).

Definición 2.3.1. Un PARS es un par $(A, \mapsto)$ donde A es un conjunto (llamado *carrier*) y una relación $A \times \mathcal{D}(A)$ (llamada la relación de evolución punto a punto).

Por ejemplo, sea A el PARS definido como:

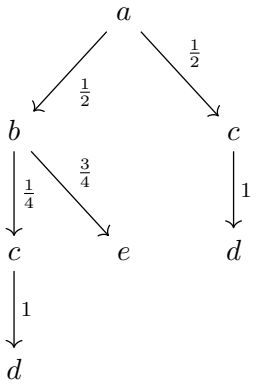
$$a \mapsto [(\frac{1}{2}, b), (\frac{1}{2}, c)] \quad a \mapsto [(\frac{1}{3}, c), (\frac{2}{3}, d)]$$
$$b \mapsto [(\frac{1}{4}, c), (\frac{3}{4}, e)] \quad c \mapsto [(1, d)]$$

En este caso, a es el único elemento no determinístico. Además, d y e son elementos terminales, ya que no reescriben a una distribución.

Definición 2.3.2. Dado un PARS $(A, \mapsto)$, se define el conjunto de sus árboles de computación con raíz a (notado $\mathcal{T}(A)$) inductivamente mediante las siguientes reglas:

$$\frac{}{a \in \mathcal{T}(A)} \qquad \frac{a \mapsto [(p_1, a_1), \cdots, (p_n, a_n)] \quad t_i \in \mathcal{T}(a_i)}{[a; (p_1, t_1) \cdots; (p_n, t_n)] \in \mathcal{T}(A)}$$

Un árbol de computación para el término $a \in A$ podría ser:



Entonces cada árbol $t \in \mathcal{T}(a)$ representa una posible evolución a partir de a. Cuando todas las hojas son elementos terminales, decimos que el árbol es maximal. Se puede calcular la probabilidad de cada hoja tomando el producto de cada p_i en el camino que parte desde el nodo. Listando cada hoja junto a su probabilidad, conseguimos una distribución perteneciente a $\mathcal{D}(A)$. Llamamos a esta distribución el soporte de t, notado $\text{supp}(T)$.

La idea de árboles de computación asocia términos a distribuciones, sin embargo el objetivo final es analizar confluencia sobre distribuciones. Tomando la relación $\mapsto$ como base, definimos la evolución paralela.

Definición 2.3.3. Dado un PARS $\mathcal{A} = (A, \mapsto)$, se define la evolución paralela como una relación de tipo $\mathcal{P}(\mathcal{A} \times \mathcal{A})$ notada $\twoheadrightarrow_P$ por las reglas

$$\frac{}{[] \twoheadrightarrow_P []} \qquad \frac{ds \twoheadrightarrow_P ds'}{(p,a) : ds \twoheadrightarrow_P (p,a) : ds'} \qquad \frac{a \mapsto A \quad ds \twoheadrightarrow_P ds'}{(p,a) : ds \twoheadrightarrow_P (pA) +\!\!+ ds'}$$

En [14], se demuestra que esta relación es suficiente para simular los árboles de computación. Es decir $[(1,a)] \twoheadrightarrow_P^* \text{supp}(a)$.

Con esta noción, nos acercamos a la idea de confluencia probabilística. Sin embargo no es suficiente comparar por igualdad los soportes de los árboles de las ramas de los pares críticos. Podemos tener dos soportes que representen la misma distribución, pero que no sean iguales. Por ejemplo $[(\frac{1}{2}, a), (\frac{1}{2}, a)] \neq [(1,a)]$. Hay que tomar un enfoque que pueda comparar módulo equivalencia.

Con esto en mente, definimos una reescritura sobre distribuciones más flexible que resuelve este problema.

Definición 2.3.4. Dado un PARS $\mathcal{A} = (A, \mapsto)$, definimos un ARS asociado $\text{Det}(\mathcal{A})$ (la determinización de $\mathcal{A}$) sobre sus distribuciones dado por la relación $\twoheadrightarrow_= (\twoheadrightarrow_P \cup \approx)$.

Utilizando esta relación es posible definir un ARS sobre las distribuciones junto a los pasos de equivalencia. Vamos a considerar que un PARS es confluente si esa relación es confluente tradicionalmente.

Definición 2.3.5 (Confluencia de distribuciones)**.** Decimos que un PARS $\mathcal{A}$ es confluente en sus distribuciones (o simplemente confluente) si $\text{Det}(\mathcal{A})$ es confluente.

2.4. Bases de la computación cuántica

La computación cuántica como concepto fue propuesta por Richard Feynman en el año 1981 en la charla "Simulating physics with computers", donde mencionaba la posibilidad de usar efectos cuánticos como base para la computación. En las décadas subsiguientes se exploraron distintos sistemas para modelar este paradigma.

Usualmente el lenguaje elegido para representar el estado cuántico de un sistema son vectores en un espacio vectorial. Sin embargo, existen otras formulaciones para representar dichos estados. Entre ellas, están las matrices de densidad. Este enfoque nos permite describir estados que no son enteramente conocidos, más precisamente nos permiten describir un conjunto de distintos estados probables.

2.4.1. Notación

Vamos a utilizar la notación de Dirac para representar vectores unitarios en el espacio vectorial $\mathbb{C}^2$. Los vectores $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ y $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ que componen la base canónica son denotados con los kets $|0\rangle$ y $|1\rangle$ respectivamente. Otros vectores referenciados son $|+\rangle = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ y $|-\rangle = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right)$ respectivamente.

Un *bra* representa el conjugado traspuesto de un ket, también denotado con un $\dagger$, $|\psi\rangle^\dagger = \langle\psi|$. Notar que $\langle\theta|\psi\rangle$ corresponde al producto interno entre los vectores y $|\theta\rangle\langle\psi|$ representa el producto diádico. Dos vectores $|\theta\rangle$ y $|\psi\rangle$ en los espacios V y W pueden combinarse en un vector $|\theta\psi\rangle$ en un tercer espacio $V \otimes W$ mediante el producto tensorial $|\theta\psi\rangle = |\theta\rangle \otimes |\psi\rangle$.

2.4.2. Estados cuánticos

Un estado cuántico esta compuesto por unidades de bits cuánticos, también llamados *qubits*. Al igual que los bits clásicos que pueden estar en estado 0 o 1, los qubits pueden estar en 2 estados definidos como $|0\rangle$ y $|1\rangle$. Además, pueden estar en una combinación lineal compleja de estos estados, o superposición $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ donde $\alpha, \beta \in \mathbb{C}$. Es decir elegimos la base $\{|0\rangle, |1\rangle\}$ y un qubit es cualquier vector del espacio $\mathbb{C}^2$ generado por dicha base.

Una composición de n qubits puede ser representada por un vector normalizado en $\mathbb{C}^{2^n}$. La base canónica de este espacio puede ser descripta por la combinación de los vectores base de cada qubit. Para $n = 2$ esto corresponde a $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Hay estados compuestos que no pueden ser representados como el producto tensorial de estados de qubits individuales. Por ejemplo el estado de Bell:

$$\beta_{00} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Se dice que los qubits de este estado estan *entrelazados*.

Evolución

La evolución de un sistema cuántico cerrado (un sistema que no interactúa con sistemas físicos externos), puede definirse como una sucesión de pasos discretos como operadores unitarios. Matrices $U \in \mathbb{C}^{2^n \times 2^n}$ tal que $U^\dagger U = I$. Un operador en $\mathbb{C}^{2^n}$ también es llamado

una *compuerta n-aria* ya que opera sobre el estado de n qubits. Por definición, estas operaciones son inversibles.

Ejemplo 2.4.1. La compuerta de Hadamard es un operador unitario que actúa sobre un solo qubit que mapea los estados $|0\rangle$ y $|1\rangle$ a los estados $|+\rangle$ y $|-\rangle$ respectivamente. Está definida de la siguiente manera:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Ejemplo 2.4.2. Otra compuerta usualmente referenciada es el CNot binario, o Not controlado. Ejecuta una negación del segundo qubit cuando el primero está en estado $|1\rangle$, o lo pasa sin modificar en caso contrario.

$$\mathsf{CNot} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Una consecuencia importante de esto es el teorema de no clonado [22]. Suponiendo que tenemos un estado $|s\rangle$ y un operador unitario U capaz de copiar 2 estados θ y ψ:

$$U|\theta s\rangle = |\theta\theta\rangle$$
$$U|\psi s\rangle = |\psi\psi\rangle$$

Entonces $\langle U\theta s|U\psi s\rangle = \langle\theta\theta|\psi\psi\rangle = \langle\theta|\psi\rangle^2$. Pero, por el otro lado $\langle U\theta s|U\psi s\rangle\langle\theta s|U^\dagger U|\psi s\rangle = \langle\theta s|\psi s\rangle = \langle\theta|\psi\rangle$. Entonces tenemos que $\langle\theta|\psi\rangle^2 = \langle\theta|\psi\rangle$. Es decir que $\langle\theta|\psi\rangle = 0$ o $\langle\theta|\psi\rangle = 1$, eso significa que θ y ψ son iguales u ortogonales. Entonces un operador unitario solo puede clonar estados ortogonales, no existe una máquina de clonado universal.

Formalmente, no existe compuerta U y estado $|\theta\rangle \in \mathbb{C}^n$ tal que para cualquier $|\psi\rangle \in \mathbb{C}^n$, $U|\psi\theta\rangle = |\psi\psi\rangle$. Esta es una restricción importante que vamos a querer mantener en los cálculos que modelamos.

Medición

Alternativamente, un estado puede evolucionar mediante una interacción con un sistema físico externo, este proceso se llama medición. El observador externo es capaz de obtener información del estado del sistema, simultáneamente perturbándolo. La medición puede definirse como un conjunto de operadores de medición $\{M_i\}_{i=1}^m$ con la propiedad:

$$\sum_{i=1}^{m} M_i^\dagger M_i = I$$

.

Cuando se aplica la medición sobre un estado $|\psi\rangle$, un solo operador es elegido aleatoriamente con probabilidad:

$$p_i = \langle\psi|M_i^\dagger M_i|\psi\rangle$$

El índice k del operador M_k elegido es el resultado de la medición. Este proceso colapsa el sistema a un nuevo estado $|\psi'\rangle$:

$$|\psi'\rangle = \frac{M_k|\psi\rangle}{\sqrt{\langle\psi|M_i^\dagger M_i|\psi\rangle}}$$

Esta operación es idempotente, siguientes mediciones utilizando el mismo conjunto de operadores devuelven el mismo resultado. Un solo conjunto de operadores de medición es suficiente para realizar cualquier medición al combinar sus elementos con un operador unitario. En este trabajo utilizamos los operadores derivados de la base canónica:

$$\pi = \{|00\cdots0\rangle\langle00\cdots0|, |00\cdots1\rangle\langle00\cdots1|, \cdots, |11\cdots1\rangle\langle11\cdots1|\}$$

Escribimos la medición de un estado $|\psi\rangle$ sobre la base canónica como $\pi|\psi\rangle$

Ejemplo 2.4.3. Consideramos una medición del estados $|+\rangle$ sobre la base canónica, $\pi|+\rangle$. Los operadores de medición asociados son:

$$M_0 = |0\rangle\langle0| \qquad M_1 = |1\rangle\langle1|$$

Las probabilidades para cada operador de medición son:

$$p_0 = \langle+|M_0^\dagger M_0|+\rangle = \frac{1}{2} \qquad p_1 = \langle+|M_1^\dagger M_1|+\rangle = \frac{1}{2}$$

Y los posibles estados finales son:

$$|\psi_0\rangle = \frac{M_0|+\rangle}{\sqrt{\langle+|M_0^\dagger M_0|+\rangle}} = |0\rangle \qquad |\psi_1\rangle = \frac{M_1|+\rangle}{\sqrt{\langle+|M_1^\dagger M_1|+\rangle}} = |1\rangle$$

2.4.3. Matrices de densidad

Supongamos que tenemos un estado cuántico que puede estar en varios estados $|\psi_i\rangle$ cada uno con probabilidad p_i. Un arreglo de qubits es un conjunto $\{p_i, |\psi_i\rangle\}_i$ con $\sum_i p_i = 1$. Una matriz de densidad, también llamada *operador de densidad*, para este estado está definida como:

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$$

Esta matriz es hermítica[1], semidefinida positiva[2] y tiene traza[3] 1. Si una matriz puede ser descompuesta en un solo estado $\rho = |\psi\rangle\langle\psi|$, decimos que el estado es puro. Esto es lo mismo que pedir que el cuadrado de la matriz también tenga traza 1. Si la matriz de densidad no representa un estado puro, decimos que representa un estado mixto.

[1] Una matriz que es igual a su transpuesto conjugado, $M = M^\dagger$.
[2] $\langle z|M|z\rangle \geq 0$ para todo z no nulo.
[3] La suma de los elementos de la diagonal, $\sum_i a_{ii}$

2.4.4. Postulados de la mecánica cuántica

Con los conceptos base definidos, vamos a definir y dar las bases de la computación cuántica. A lo largo de este trabajo vamos a representar los estados cuánticos mediante matrices de densidad. Por ende, presentamos los postulados bajo ese modelo.

Postulado 1: Asociado a cualquier sistema físico aislado, existe un espacio vectorial complejo con producto interno conocido como el espacio de estados del sistema. El sistema está completamente descripto por su operador de densidad, el cual es un operador positivo ρ con traza 1 actuando en el espacio de estados. Si un sistema cuántico está en el estado ρ_i con probabilidad p_i, entonces el operador del sistema es $\sum_i p_i \rho_i$.

Postulado 2: La evolución de un sistema cuántico *cerrado* está dada por una transformación unitaria. Es decir, el estado ρ del sistema en el tiempo t_1 está relacionado al estado del sistema ρ' en el tiempo t_2 por un operador unitario U que depende sólo de los tiempos t_1 y t_2. $\rho' = U\rho U^\dagger$.

Postulado 3: Las mediciones cuánticas pueden describirse mediante una colección $\{M_m\}$ de operadores de medición. Estos operadores actúan en el mismo espacio de estados del sistema que está siendo medido. El índice m se refiere a los posibles resultados que pueden ocurrir en el experimento. Si el estado ρ describe el instante previo a la medición, la probabilidad de que ocurra el resultado m está dada por:

$$p_m = \mathrm{tr}(M_m^\dagger M_m \rho)$$

Y el estado del sistema luego de la medición es:

$$\frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}$$

Los operadores de medición satisfacen la ecuación de completitud:

$$\sum_m M_m^\dagger M_m = I$$

Postulado 4: El espacio de estados de un sistema físico compuesto es el producto tensorial de los espacios de estados de los sistemas físicos componentes. Más aún, si tenemos sistemas numerados del 1 a n y el sistema i está en el estado $|\rho_i\rangle$, entonces el estado conjunto del sistema entero es $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$.

2.5. λ-cálculos orientados a computación cuántica

Ha habido una gran cantidad de trabajos enfocados al tema de cálculos λ que modelen el cómputo cuántico [2, 7, 19, 21, 24]. En todos estos sistemas, el lenguage elegido para representar estados cuánticos es el de vectores en un espacio vectorial. Sin embargo, mostramos que también es posible enunciar los postulados de la mecánica cuántica en términos de matrices de densidad. Por lo tanto debería ser posible describir el cómputo cuántico en este formalismo.

Selinger [18] introdujo un lenguaje para diagramas de flujo cuántico y una interpretación de este en un orden parcial completo de matrices de densidad. Además, el libro "Foundations of Quantum Programming" [23] está escrito en el lenguaje de matrices de densidad. A pesar de eso, no conocemos otro λ-cálculo que trabaje con esta representación más allá de [6].

2.5.1. El cálculo λ_ρ

A lo largo de este trabajo, vamos a tomar como base los cálculos λ_ρ y λ_ρ° para extender y demostrar sobre ellos. Estos cálculos poseen propiedades deseables, codifican los postulados en los términos, respetan el no clonado y describen los estados cuánticos mediante matrices de densidad.

En [19] se introdujo el cálculo λ_q, base de un lenguaje de programación embebido en Haskell llamado Quipper [12]. En [6] quedaron demostradas las propiedades de subject reduction y progreso de λ_ρ y λ_ρ°. En [5], se presentó una traducción entre λ_q y los cálculos λ_ρ y λ_ρ°, probando así la propiedad de normalización fuerte. En este trabajo vamos a extender los cálculos λ_ρ y λ_ρ° y demostrar subject reduction, normalización fuerte y confluencia.

3. LOS CÁLCULOS λ_ρ Y λ_ρ°

3.1. El cálculo λ_ρ

λ_ρ es una extensión al λ-cálculo simplemente tipado. Los términos de la gramática pueden dividirse en tres categorías:

- términos estándar de λ-cálculo: variables, abstracciones y aplicaciones.
- términos para modelar los postulados cuánticos con la medición restringida a la base canónica: ρ^n para representar una matriz de densidad de un sistema, $U^n t$ para describir su evolución, π^n representa la medición del sistema de n-qubits, $t \otimes t$ describe un sistema compuesto.
- términos para el control clásico: un par (b^m, ρ^n) para representar el resultado de una medición, y un condicional $\mathsf{letcase}$ que decide en base al resultado de la medición.

3.1.1. Gramática de términos

$$
\begin{aligned}
t \coloneqq\ & x \mid \lambda x.t \mid tt && \text{(Cálculo lambda standard)} \\
& \mid \rho^n \mid U^n t \mid \pi^n t \mid t \otimes t && \text{(Postulados cuánticos)} \\
& \mid (b^m, \rho^n) \mid \mathsf{letcase}\ x = r\ \mathsf{in}\ \{t, \ldots, t\} && \text{(Control clásico)}
\end{aligned}
$$

donde:

- $n, m \in \mathbb{N}$, $m \leq n$.
- ρ^n es una matriz de densidad de n-qubits, una matriz positiva de dimensión $2^n \times 2^n$ con traza 1.
- $b^m \in \mathbb{N}$, $0 \leq b^m < 2^m$.
- $\{t, \ldots, t\}$ contiene 2^m términos.
- U^n es un operador unitario de dimensión $2^n \times 2^n$, es decir, una matriz de dimensión $2^n \times 2^n$ tal que $(U^n)^\dagger = (U^n)^{-1}$.
- $\pi^n = \{\pi_0, \ldots, \pi_{2^n-1}\}$, es una medición cuántica en la base computacional donde cada π_i es el operador de proyección 2^n proyectando a un vector de la base canónica.

3.1.2. Sistema de reescritura

El sistema de reescritura está dado por una relación probabilística. Si un término t reduce con probabilidad p a s, lo notamos $t \to_p s$. Vamos a usar esta reducción para poder tratar

el caso de la medición cuántica.

$$(\lambda x.t)r \longrightarrow_1 t[r/x]$$

$$U^m\rho^n \longrightarrow_1 \rho'^n \qquad \text{con } \rho'^n = \overline{U^m}\rho^n\overline{U^m}^\dagger$$

$$\pi^m\rho^n \longrightarrow_{p_i} (i, \rho_i^n) \qquad \text{con } \begin{cases} p_i = \mathsf{tr}(\overline{\pi_i}^\dagger\overline{\pi_i}\rho^n) \\ \rho_i^n = \frac{\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger}{p_i} \end{cases}$$

$$\rho \otimes \rho' \rightsquigarrow \rho'' \qquad \text{con } \rho'' = \rho \otimes \rho'$$

$$\mathsf{letcase}\ x = (b^m, \rho^n)\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \longrightarrow_1 t_{b^m}[\rho^n/x]$$

$$\frac{t \longrightarrow_p r}{\lambda x.t \longrightarrow_p \lambda x.r} \qquad \frac{t \longrightarrow_p r}{ts \longrightarrow_p rs} \qquad \frac{t \longrightarrow_p r}{st \longrightarrow_p sr} \qquad \frac{t \longrightarrow_p r}{U^n t \longrightarrow_p U^n r}$$

$$\frac{t \longrightarrow_p r}{\pi^n t \longrightarrow_p \pi^n r} \qquad \frac{t \longrightarrow_p r}{t \otimes s \longrightarrow_p r \otimes s} \qquad \frac{t \longrightarrow_p r}{s \otimes t \longrightarrow_p s \otimes r}$$

$$\frac{t \longrightarrow_p r}{\mathsf{letcase}\ x = t\ \mathsf{in}\ \{s_0, \ldots, s_n\} \longrightarrow_p \mathsf{letcase}\ x = r\ \mathsf{in}\ \{s_0, \ldots, s_n\}}$$

Donde la aplicación de un operador $U^m\rho^n$, con $m \leq n$, lo escribimos $\overline{U^m}$ para denotar $U^m \otimes I^{n-m}$. Del mismo modo, escribimos $\overline{\pi^m}$ para denotar $\{\pi_0 \otimes I^{n-m}, \ldots, \pi_{2^m-1} \otimes I^{n-m}\}$. Unas de las cosas que asumimos en este modelo es que el resultado de una medición es conocido. Sin embargo, podríamos tomar un modelo donde no leemos el resultado de las mediciones y trabajar con estados mixtos. Esta idea es la base del cálculo λ°_ρ que vamos a presentar en la sección 3.2.

3.1.3. Sistema de tipos

Un punto importante a destacar es que el sistema de tipos es afín, es decir que las variables pueden ser utilizadas a lo sumo una sola vez. Esta característica garantiza respetar la propiedad de no clonado del cálculo. Cuando aparece más de un contexto en una regla, estos se consideran disjuntos. La gramática de tipos viene dada por:

$$\sigma := n \mid (m, n) \mid \sigma \multimap \sigma$$

donde $m \leq n \in \mathbb{N}$.

$$\frac{}{x : \sigma \vdash x : \sigma}\ \mathsf{ax} \qquad \frac{\Gamma, x : \sigma \vdash t : \tau}{\Gamma \vdash \lambda x.t : \sigma \multimap \tau}\ \multimap_i \qquad \frac{\Gamma \vdash t : \sigma \multimap \tau \quad \Delta \vdash r : \sigma}{\Gamma, \Delta \vdash tr : \tau}\ \multimap_e$$

$$\frac{}{\Gamma \vdash \rho^n : n}\ \mathsf{ax}_\rho \qquad \frac{\Gamma \vdash t : n}{\Gamma \vdash U^m t : n}\ \mathsf{u} \qquad \frac{\Gamma \vdash t : n}{\Gamma \vdash \pi^m t : (m, n)}\ \mathsf{m} \qquad \frac{\Gamma \vdash t : n \quad \Delta \vdash r : m}{\Gamma, \Delta \vdash t \otimes r : n + m}\ \otimes$$

$$\frac{}{\Gamma \vdash (b^m, \rho^n) : (m, n)}\ \mathsf{ax}_{\mathsf{am}} \qquad \frac{x : n \vdash t_0 : \sigma \quad \ldots \quad x : n \vdash t_{2^m-1} : \sigma \quad \Gamma \vdash r : (m, n)}{\Gamma \vdash \mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} : \sigma}\ \mathsf{lc}$$

Ejemplo 3.1.1. Podemos modelar la tirada de una moneda equilibrada como un término de λ_ρ. Sea H la compuerta de Hadamard (ver ejemplo 2.4.1) y sean r y t dos términos

arbitrarios. Podemos describir la elección entre los dos términos con una tirada de moneda como:

$$\mathsf{letcase}\ x = \pi^1(H|0\rangle\langle 0|)\ \mathsf{in}\ \{t, r\}$$

$H|0\rangle\langle 0|$ reduce $|+\rangle\langle +|$, que al medirlo reduce a $(0, |0\rangle\langle 0|)$ o $(1, |1\rangle\langle 1|)$ con probabilidad $\frac{1}{2}$, y entonces el letcase reduce t o a r con un medio de probabilidad.

Ejemplo 3.1.2. El proceso de teleportación cuántica [15] es un proceso donde información de un estado cuántico $|\psi\rangle$ es transmitida mediante comunicación clásica y un estado cuántico entrelazado compartido entre un emisor (Alice) y un receptor (Bob). El outline del proceso es el siguiente, Alice hace interactuar el qubit $|\psi\rangle$ con su mitad del estado entrelazado y luego mide los qubits en su posesión obtienendo así uno de 4 resultados: 00, 01, 10 y 11. Alice manda esta información a Bob que realiza una de 4 operaciones dependiendo del resultado enviado por Alice para reconstruir el estado $|\psi\rangle$.

Definiendo los operadores unitarios X^1 y Z^1 de la siguiente manera:

$$X^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Z^1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

La forma de codificarlo en λ_ρ es la siguiente:

$$\lambda x.\mathsf{letcase}\ y = \pi^2(H^1(\mathsf{CNot}^2(x \otimes \beta_{00})))\ \mathsf{in}\ \{y, Z_3 y, X_3 y, Z_3 X_3 y\}$$

Donde $Z_3 = I \otimes I \otimes Z^1$ y $X_3 = I \otimes I \otimes X^1$

3.2. El cálculo λ_ρ°

3.2.1. Gramática de términos

La idea detrás de λ_ρ° consiste en tomar el cálculo descrito en la sección anterior y cambiar la forma de interpretar las mediciones. En λ_ρ, una medición toma un estado cuántico y devuelve otro con cierta probabilidad. En λ_ρ°, una medición toma un estado cuántico y devuelve la suma de los términos ponderados por su probabilidad de ocurrencia, en una suerte de generalización a programas de los estados mixtos.

El resto de los términos y reducciones de λ_ρ se mantienen igual.

$$\begin{aligned} t \coloneqq\ & x \mid \lambda x.t \mid tt && (\text{ Cálculo lambda standard }) \\ & \mid \rho^n \mid U^n t \mid \pi^n t \mid t \otimes t && (\text{ Postulados cuánticos }) \\ & \mid \sum_{i=1}^{n} p_i t_i \mid \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t, \ldots, t\} && (\text{ Control probabilístico }) \end{aligned}$$

donde $p_i \in (0, 1]$, $\sum_{i=1}^n p_i = 1$, y $\sum$ es tomada como un constructor de distribuciones: se toma módulo asociatividad y conmutatividad y se considera $p_1 t + p_2 t = (p_1 + p_2)t$.

3.2.2. Sistema de reescritura

El sistema de reescritura está dado por la reducción no probabilística $\rightsquigarrow$. En este caso la medición no reduce por si sola sino que utiliza el letcase como destructor, el cual asigna las probabilidades que se le va a dar a cada término de la sumatoria.

$$
\begin{array}{rl}
(\lambda x.t)r \rightsquigarrow t[r/x] & \\
U^m\rho^n \rightsquigarrow \rho'^n & \text{con } \overline{U^m}\rho^n\overline{U^m}^\dagger = \rho'^n \\
\rho \otimes \rho' \rightsquigarrow \rho'' & \text{con } \rho'' = \rho \otimes \rho' \\
\mathsf{letcase}^\circ\ x = \pi^m\rho^n\ \mathsf{in}\ \{t_0,\ldots,t_{2^m}-1\} \rightsquigarrow \sum_i p_i t_i[\rho_i^n/x] & \text{con } \begin{cases} \rho_i^n = \frac{\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger}{p_i} \\ p_i = \mathsf{tr}(\overline{\pi_i}^\dagger\overline{\pi_i}\rho^n) \end{cases} \\
\sum_i p_i\rho_i \rightsquigarrow \rho' & \text{con } \rho' = \sum_i p_i\rho_i \\
\sum_i p_i t \rightsquigarrow t & \\
(\sum_i p_i t_i)r \rightsquigarrow \sum_i p_i(t_i r) &
\end{array}
$$

$$
\frac{t \rightsquigarrow r}{\lambda x.t \rightsquigarrow \lambda x.r} \qquad \frac{t \rightsquigarrow r}{ts \rightsquigarrow rs} \qquad \frac{t \rightsquigarrow r}{st \rightsquigarrow sr} \qquad \frac{t \rightsquigarrow r}{U^n t \rightsquigarrow U^n r}
$$

$$
\frac{t \rightsquigarrow r}{\pi^n t \rightsquigarrow \pi^n r} \qquad \frac{t \rightsquigarrow r}{t \otimes s \rightsquigarrow r \otimes s} \qquad \frac{t \rightsquigarrow r}{s \otimes t \rightsquigarrow s \otimes r}
$$

$$
\frac{t_j \rightsquigarrow r_j}{\sum_{i=1}^n p_i t_i \rightsquigarrow \sum_{i=1}^n p_i r_i}\ {\scriptstyle (\forall i \neq j, t_i = r_j)}
$$

$$
\frac{t \rightsquigarrow r}{\mathsf{letcase}^\circ\ x = t\ \mathsf{in}\ \{s_0,\ldots,s_{2^m-1}\} \rightsquigarrow \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{s_0,\ldots,s_{2^m-1}\}}
$$

La medición se puede codificar de la siguiente manera:

$$
\mathsf{letcase}^\circ\ x = \pi^m\rho^n\ \mathsf{in}\ \{x,\cdots,x\} \rightsquigarrow \sum_i p_i\rho_i^n \rightsquigarrow \rho'
$$

A pesar de no tener la reducción de medición en este cálculo, no se pierde expresividad con respecto a λ_ρ.

3.2.3. Sistema de tipos

La única diferencia con λ_ρ es que ya no es necesario el axioma de la medición $\mathsf{ax_{am}}$ y en su lugar incorporamos una regla para tipar la suma $(+)$. Usamos $\Vdash$ en lugar de $\vdash$ para diferenciar del tipado de λ_ρ

$$
\sigma := \sigma \mid (m,n) \mid \sigma \multimap \sigma
$$

donde $m \leq n \in \mathbb{N}$.

$$\frac{}{\Gamma, x:\sigma \Vdash x:\sigma}\ \mathsf{ax} \qquad \frac{\Gamma, x:\sigma \Vdash t:\tau}{\Gamma \Vdash \lambda x.t : \sigma \multimap \tau}\ \multimap_i \qquad \frac{\Gamma \Vdash t:\sigma \multimap \tau \quad \Delta \Vdash r:\sigma}{\Gamma, \Delta \Vdash tr:\tau}\ \multimap_e$$

$$\frac{}{\Gamma \Vdash \rho^n : n}\ \mathsf{ax}_\rho \qquad \frac{\Gamma \Vdash t:n}{\Gamma \Vdash U^m t : n}\ \mathsf{u} \qquad \frac{\Gamma \Vdash t:n}{\Gamma \Vdash \pi^m t : (m,n)}\ \mathsf{m} \qquad \frac{\Gamma \Vdash t:n \quad \Delta \Vdash r:m}{\Gamma, \Delta \Vdash t \otimes r : n+m}\ \otimes$$

$$\frac{x:n \Vdash t_0:\sigma \quad \dots \quad x:n \Vdash t_{2^m-1}:\sigma \quad \Gamma \Vdash r:(m,n)}{\Gamma \Vdash \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0,\dots,t_{2^m-1}\}:\sigma}\ \mathsf{lc}$$

$$\frac{\Gamma \Vdash t_1:\sigma \quad \dots \quad \Gamma \Vdash t_n:\sigma \quad \sum_{i=1}^n p_i = 1}{\Gamma \Vdash \sum_{i=1}^n p_i t_i : \sigma}\ +$$

Ejemplo 3.2.1. El término para representar la tirada de una moneda es igual que para λ_ρ.

$$\mathsf{letcase}\ x = \pi^1(H|0\rangle\langle 0|)\ \mathsf{in}\ \{t, r\}$$

Sin embargo la reducción de este termino deriva en la combinación lineal de r y t:

$$\frac{1}{2}r + \frac{1}{2}t$$

3.3. Subject Reduction

Una de las propiedades demostrada sobre ambos cálculos en [6] es *Subject Reduction*. Pasamos a enunciar y mostrar su prueba. Primero vamos a demostrar la propiedad para λ_ρ. Luego, incluimos los casos faltantes para probarla sobre λ°_ρ. Antes de llegar a la demostración de la propiedad, son necesarios algunos lemas auxiliares.

Lema 3.3.1 (Weakening)**.**

1. Si $\Gamma \vdash t:\sigma$ y $x \notin \mathrm{FV}(t)$, entonces $\Gamma, x:\tau \vdash t:\sigma$
2. Si $\Gamma \Vdash t:\sigma$ y $x \notin \mathrm{FV}(t)$, entonces $\Gamma, x:\tau \Vdash t:\sigma$

Demostración. Inducción en las derivaciones de $\Gamma \vdash t:\sigma$ y $\Gamma \Vdash t:\sigma$. □

Lema 3.3.2 (Strenghtening)**.**

1. Si $\Gamma, x:\tau \vdash t:\sigma$ y $x \notin \mathrm{FV}(t)$, entonces $\Gamma \vdash t:\sigma$
2. Si $\Gamma, x:\tau \Vdash t:\sigma$ y $x \notin \mathrm{FV}(t)$, entonces $\Gamma \Vdash t:\sigma$

Demostración. Inducción en las derivaciones de $\Gamma, x:\tau \vdash t:\sigma$ y $\Gamma, x:\tau \Vdash t:\sigma$ □

Lema 3.3.3 (Sustitución)**.**

1. Si $\Gamma, x:\tau \vdash t:\sigma$ y $\Delta \vdash r:\tau$, entonces $\Gamma, \Delta \vdash t[r/x]:\sigma$
2. Si $\Gamma, x:\tau \Vdash t:\sigma$ y $\Delta \Vdash r:\tau$, entonces $\Gamma, \Delta \Vdash t[r/x]:\sigma$

Demostración. Inducción en t. Primero analizamos los casos de λ_ρ.

$\boldsymbol{t = x}$: Entonces $\sigma = \tau$. Por lema 3.3.1, $\Gamma, \Delta \vdash r : \sigma$.

$\boldsymbol{t = y \neq x}$: Entonces por lemas 3.3.1 y 3.3.2, $\Gamma, \Delta \vdash y : \sigma$.

$\boldsymbol{t = \lambda y.s}$ En este caso, $\sigma = \gamma_1 \multimap \gamma_2$. Por inversión en la regla $\multimap_i$, $\Gamma, x : \gamma_1, y : \tau \vdash s : \gamma_2$. Por hipótesis inductiva, $\Gamma, y : \gamma_1, \Delta \vdash s[r/x] : \gamma_2$. Aplicando la regla $\multimap_i$, llegamos a $\Gamma \vdash \lambda y.s[r/x] : \sigma$. Notar que $\lambda y.s[r/x] = (\lambda x.s)[r/x]$.

$\boldsymbol{t = t_1 t_2}$: Entonces $\Gamma, x : \tau = \Gamma_1, \Gamma_2$ con $\Gamma_1 \vdash t_1 : \gamma \multimap \sigma$ y $\Gamma_2 \vdash t_2 : \gamma$. Hay 2 casos posibles:

- $x \in \Gamma_1$, entonces $x \notin \mathrm{FV}(t_2)$:
  Por hipótesis inductiva $\Gamma_1 \setminus \{x : \tau\}, \Delta \vdash t_1 : \gamma \multimap \sigma$. Por regla $\multimap_e$ $\Gamma_1 \setminus \{x : \tau\}, \Gamma_2, \Delta \vdash t_1[r/x]t_2 : \sigma$. Notar que $\Gamma_1 \setminus \{x : \tau\}, \Gamma_2 = \Gamma$ y $t_1[r/x]t_2 = (t_1 t_2)[r/x]$.
- $x \in \Gamma_2$, entonces $x \notin \mathrm{FV}(t_1)$:
  Similar al caso anterior.

$\boldsymbol{t = \rho^n}$: Entonces $\sigma = n$. Por lemas 3.3.1 y 3.3.2, $\Gamma, \Delta \vdash \rho^n : n$.

$\boldsymbol{t = U^m s}$: Entonces $\sigma = n$ y $\Gamma, x : \tau \vdash s : n$. Por hipótesis inductiva, $\Gamma, \Delta \vdash s[r/x] : n$. Además por regla U, $\Gamma \vdash U^m s[r/x] : n$. Notar que $U^m s[r/x] = (U^m s)[r/x]$.

$\boldsymbol{t = \pi^m s}$: Entonces $\sigma = (m, n)$ y $\Gamma, x : \tau \vdash s : n$. Por hipótesis inductiva, $\Gamma, \Delta \vdash s[r/x] : n$. Además por regla π, $\Gamma \vdash \pi^m s[r/x] : n$. Notar que $\pi^m s[r/x] = (\pi^m s)[r/x]$.

$\boldsymbol{t = t_1 \otimes t_2}$: Entonces $\sigma = n_1 + n_2$ y $\Gamma, x : \tau = \Gamma_1, \Gamma_2$. con $\Gamma_i \vdash t_i : n_i$ para $i = 1, 2$. Hay dos casos posibles:

- $x \in \Gamma_1$, entonces $x \notin \mathrm{FV}(t_2)$:
  Por hipótesis inductiva, $\Gamma_1 \setminus \{x : \tau\}\Delta \vdash t_1[r/x] : n_1$. Por regla $\otimes$, $(\Gamma_1 \setminus \{x : \tau\}), \Gamma_2, \Delta \vdash t_1[r/x] \otimes t_2 : n_1 + n_2$. Notar que $(\Gamma_1 \setminus \{x : \tau\}), \Gamma_2 = \Gamma$ y $t_1[r/x] \otimes t_2 = (t_1 \otimes t_2)[r/x]$.
- $x \in \Gamma_2$, entonces $x \notin \mathrm{FV}(t_2)$:
  Similar al caso anterior.

$\boldsymbol{t = (b^m, \rho^n)}$: Entonces $\sigma = (m, n)$. Por lemas 3.3.1 y 3.3.2, $\Gamma, \Delta \vdash (b^m, \rho^n) : (m, n)$.

$\boldsymbol{t = \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}}$: Entonces, $y : n \vdash t_i : \sigma$ para $i = 0, \cdots, 2^m - 1$ y $\Gamma, x : \tau \vdash s : (m, n)$. Por hipótesis inductiva $\Gamma, \Delta \vdash s[r/x] : (m, n)$. Por regla del letcase, $\Gamma, \Delta \vdash \mathsf{letcase}\ y = s[r/x]\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma$. Notar que $\mathsf{letcase}\ y = s[r/x]\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} = (\mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x]$, la sustitución no aplica a los t_i ya que y es la única variable que puede aparecer libre.

Esos son todos los casos para λ_ρ. Para probar el lema en λ°_ρ solo falta considerar el caso de la sumatoria:

$\boldsymbol{t = \sum_i p_i t_i}$: Entonces $\Gamma, x : \tau \Vdash t_i : \sigma$ y, por hipótesis inductiva, $\Gamma, \Delta \Vdash t_i[r/x] : \sigma$. Aplicando la regla $+$ llegamos a $\Gamma, \Delta \Vdash \sum_i p_i t_i[r/x] : \sigma$ Notar que $\sum_i p_i t_i[r/x] = (\sum_i p_i t_i)[r/x]$. □

Con estos lemas, es posible demostrar subject reduction.

Teorema 3.3.4 (Subject reduction para λ_ρ y λ°_ρ)**.**

1. *Si* $\Gamma \vdash t : \sigma$ *y* $t \to_p t'$, *entonces* $\Gamma \vdash t' : \sigma$.
2. *Si* $\Gamma \Vdash t : \sigma$ *y* $t \rightsquigarrow t'$, *entonces* $\Gamma \vdash t' : \sigma$.

Demostración. Inducción sobre $\to_p$ y $\rightsquigarrow$:

- $t = (\lambda x.s)r$ y $t' = s[r/x]$. Entonces $\Gamma = \Gamma_1, \Gamma_2$ con $\Gamma_1 \vdash \lambda x.s : \tau \multimap \sigma$ y $\Gamma_2 \vdash r : \tau$. Podemos ver que $\Gamma_1, x : \tau \vdash s : \sigma$ y por lema 3.3.3 $\Gamma \vdash s[r/x] : \sigma$.
- $t = U^m \rho^n$ y $t' = \rho'^n$ con $\rho'^n = \overline{U^m} \rho^n \overline{U^m}^\dagger$. Entonces $\sigma = n$. Por regla ax_ρ, $\Gamma \vdash \rho'^n : n$.
- $t = \pi^m \rho^n$ y $t' = (i^m, \rho_i^n)$ con $\rho_i^n = \frac{\overline{\pi_i} \rho^n \overline{\pi_i}^\dagger}{p_i}$. Entonces $\sigma = (m, n)$ y, por regla m, $\Gamma \vdash (i^m, \rho_i^n) : (m, n)$.
- $t = \rho_1^n \otimes \rho_2^m$ y $t' = \rho'$ con $\rho' = \rho_1^n \otimes \rho_2^m$. Entonces $\sigma = n + m$ con $\vdash \rho_1^n : n$ y $\vdash \rho_2^m : m$. Dado que ρ' es una matriz de $n + m$ qubits, se tiene por ax_ρ que $\vdash \rho' : n + m$.
- $t = \mathsf{letcase}\ x = (b^m, \rho^n)\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ y $t' = t_{b^m}[\rho^n/x]$. Por inversión, $x : n \vdash t_i : \sigma$ para $i = 0, \cdots, 2^m - 1$ y $\Gamma \vdash (b^m, \rho^n) : (m, n)$. Por regla ax_ρ, $\Gamma \vdash \rho^n : n$. Por lema 3.3.3, $\Gamma \vdash t_{b^m}[\rho/x] : \sigma$.

Casos contextuales, sea $s \to_p s'$:

- $t = \lambda x.s$ y $t' = \lambda x.s'$. Entonces $\sigma = \gamma_1 \multimap \gamma_2$ y $\Gamma, x : \gamma_1 \vdash s : \gamma_2$. Entonces, por la hipótesis inductiva $\Gamma, x : \gamma_1 \vdash s' : \gamma_2$ y por la regla $\multimap_i$ tenemos que $\Gamma \vdash \lambda x.s' : \sigma$.
- $t = sr$ y $t' = s'r$. Entonces $\Gamma = \Gamma_1, \Gamma_2$ con $\Gamma_1 \vdash s : \tau \multimap \sigma$ y $\Gamma_2 \vdash r : \tau$. Por hipótesis inductiva, $\Gamma_1 \vdash s' : \tau \multimap \sigma$. Por regla $\multimap_e$ tenemos que $\Gamma \vdash s'r : \sigma$.
- $t = rs$ y $t' = rs'$. Similar al caso anterior.
- $t = U^m s$ y $t' = U^m s'$. Entonces $\sigma = n$ y $\Gamma \vdash s : n$. Por hipótesis inductiva, $\Gamma \vdash s' : n$ y por regla u, $\Gamma \vdash U^m s' : n$.
- $t = \pi^m s$ y $t' = \pi^m s'$. Entonces $\sigma = (m, n)$ y $\Gamma \vdash s : n$. Por hipótesis inductiva, $\Gamma \vdash s' : n$ y por regla m, $\Gamma \vdash \pi^m s' : (m, n)$.
- $t = s \otimes r$ y $t' = s' \otimes r$. Entonces $\sigma = n + m$ y $\Gamma = \Gamma_1, \Gamma_2$ con $\Gamma_1 \vdash s : n$ y $\Gamma_2 \vdash r : m$. Por hipótesis inductiva, $\Gamma_1 \vdash s' : n$ y por regla $\otimes$, $\Gamma \vdash s' \otimes r : \sigma$.
- $t = r \otimes s$ y $t' = r \otimes s'$. Similar al caso anterior.
- $t = \mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ y $t = \mathsf{letcase}\ x = s'\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$. Entonces $x : n \vdash t_i : \sigma$ y $\Gamma \vdash s : (m, n)$. Por hipótesis inductiva, $\Gamma \vdash s' : (m, n)$ y finalmente por regla lc, $\Gamma \vdash \mathsf{letcase}\ x = s'\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma$.

Estos son los casos comprendidos por λ_ρ. A continuación consideramos los casos introducidos por λ°_ρ para cerrar la inducción en $\rightsquigarrow$.

- $\mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ y $t' = \sum_i p_i t_i[\rho_i^n/x]$ con $\rho_i^n = \frac{\overline{\pi_i} \rho^n \overline{\pi_i}^\dagger}{p_i}$. Entonces $\Gamma \Vdash \pi^m \rho^n : (m, n)$ y $x : n \Vdash t_i : \sigma$. Por lema 3.3.3, $\Gamma \Vdash t_i[\rho_i^n/x]$. Además, tenemos que $\sum_i \mathsf{tr}(\overline{\pi_i}^\dagger \overline{\pi_i} \rho^n) = 1$, vamos a tomar esas probabilidades como p_i. Finalmente por regla $+$, $\Gamma \Vdash \sum_i p_i t_i[\rho_i^n/x] : \sigma$.

- $t = \sum_i p_i\rho_i$ y $t' = \rho'$ con $\rho' = \sum_i p_i\rho_i$. Entonces $\sigma = n$ y por regla ,ax_ρ, $\Gamma \Vdash \rho' : n$.
- $t = \sum_i p_i r$ y $t' = r$. Hipótesis de la regla $+$.
- $t = (\sum_i p_i t_i)r$ y $t' = \sum_i p_i t_i r$. Entonces $\Gamma = \Gamma_1, \Gamma_2$ con $\Gamma_1 \Vdash t_i : \tau \multimap \sigma$ y $\Gamma_2 \Vdash r : \tau$. Por regla $\multimap_e$, $\Gamma \Vdash t_i r : \sigma$, además por regla $+$, $\Gamma \Vdash \sum_i t_i r : \sigma$.

Hay un solo caso contextual que no está considerado en λ_ρ: la reducción interna en la sumatoria. Sea $t = \sum_i p_i s_i$ y $t' = \sum_i p_i r_i$ con $t_j \rightsquigarrow r_j$ y $\forall i \neq j\, t_i = r_i$. Por inversión en la regla $+$, $\Gamma \Vdash t_i : \sigma$, además por hipótesis inductiva, $\Gamma \Vdash r_i : \sigma$. Finalmente, por regla $+$, $\Gamma \Vdash \sum_i p_i r_i : \sigma$. □

4. EXTENSIONES $\lambda_\rho 2$ Y $\lambda_\rho^\circ 2$

4.1. Extensiones de tipado

Los cálculos que vamos a tratar en este trabajo son extensiones sobre el sistema de tipos de λ_ρ y λ_ρ°. Hay dos cambios que vamos a aplicar sobre el tipado de ambos cálculos: Extenderlos polimórficamente y permitir términos abiertos dentro de las ramas de los letcase.

Extensión polimórfica

Tomamos las reglas introducidas por System F (ver sección 2.1) y las incorporamos tanto a λ_ρ como a λ_ρ°. Llamaremos a estos calculos polimórficos $\lambda_\rho 2$ y $\lambda_\rho^\circ 2$ respectivamente. Las reglas a agregar son las siguientes:

$$\frac{X \notin \mathrm{FV}(\Gamma) \quad \Gamma \vdash t : \sigma}{\Gamma \vdash t : \forall X.\sigma}\ \forall_i \qquad \frac{\Gamma \vdash t : \forall X.\sigma}{\Gamma \vdash t : \sigma[X/\tau]}\ \forall_e$$

Extensión del letcase

La siguiente es una modificación introducida por Ivnisky en [13]. Abrimos la posibilidad de incorporar términos con variables libres más allá de la ligada en la medición del letcase. Introducimos un contexto Δ que va a tipar a los términos t internos.

$$\frac{\Gamma \vdash s : (m,n) \quad \Delta, x : n \vdash t_0 : \sigma, \cdots, \Delta, x : n \vdash t_{2^m-1} : \sigma}{\Gamma, \Delta \vdash \mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma}\ \mathsf{lc}$$

En este momento, hay que destacar un punto importante. El sistema de tipado deja de ser afín, sin embargo notamos que se sigue respetando el principio de no clonado. Destacamos que la única regla que reutiliza los contextos es la del letcase y que estos no interactúan entre sí.

Para el caso de $\lambda_\rho 2$, si bien se repiten las variables, cuando se reduce un letcase las ramas no elegidas se descartan. Es decir, un estado que reduce todas sus estructuras de control es afín. Por el otro lado, para $\lambda_\rho^\circ 2$, al reducir todas las estructuras de control, cada término de la sumatoria tiene a lo sumo una sola copia de cada variable. Como cada término representa un estado que compone el estado mixto, los estados son afines.

Si bien a primera vista este cambio parece menor, genera complicaciones a la hora de demostrar confluencia en el cálculo con reducciones probabilísticas. En la sección 4.4.2, analizamos distintas formas de mitigarlas.

El tipado de $\lambda_\rho 2$ queda de la siguiente manera:

$$\sigma ::= n \mid (m,n) \mid \sigma \multimap \sigma \mid X \mid \forall X.\sigma$$

donde $m \leq n \in \mathbb{N}$ y X pertenece al conjunto de variables de tipo V.

$$\frac{}{\Gamma, x:\sigma \vdash x:\sigma}\ \mathsf{ax} \qquad \frac{\Gamma, x:\sigma \vdash t:\tau}{\Gamma \vdash \lambda x.t : \sigma \multimap \tau}\ \multimap_i \qquad \frac{\Gamma \vdash t:\sigma \multimap \tau \quad \Delta \vdash r:\sigma}{\Gamma, \Delta \vdash tr:\tau}\ \multimap_e$$

$$\frac{}{\Gamma \vdash \rho^n : n}\ \mathsf{ax}_\rho \qquad \frac{\Gamma \vdash t:n}{\Gamma \vdash U^m t : n}\ \mathsf{u} \qquad \frac{\Gamma \vdash t:n}{\Gamma \vdash \pi^m t : (m,n)}\ \mathsf{m} \qquad \frac{\Gamma \vdash t:n \quad \Delta \vdash r:m}{\Gamma, \Delta \vdash t \otimes r : n+m}\ \otimes$$

$$\frac{}{\Gamma \vdash (b^m, \rho^n) : (m,n)}\ \mathsf{ax_{am}} \qquad \frac{\Gamma \vdash s:(m,n) \quad \Delta, x:n \vdash t_0:\sigma \quad \cdots \quad \Delta, x:n \vdash t_{2^m-1}:\sigma}{\Gamma, \Delta \vdash \mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma}\ \mathsf{lc}$$

$$\frac{X \notin \mathrm{FV}(\Gamma) \quad \Gamma \vdash t:\sigma}{\Gamma \vdash t : \forall X.\sigma}\ \forall_i \qquad \frac{\Gamma \vdash t : \forall X.\sigma}{\Gamma \vdash t : \sigma[X/\tau]}\ \forall_e$$

Para el caso de $\lambda^\circ_\rho 2$, el tipado es el siguiente:

$$\frac{}{\Gamma, x:\sigma \Vdash x:\sigma}\ \mathsf{ax} \qquad \frac{\Gamma, x:\sigma \Vdash t:\tau}{\Gamma \Vdash \lambda x.t : \sigma \multimap \tau}\ \multimap_i \qquad \frac{\Gamma \Vdash t:\sigma \multimap \tau \quad \Delta \Vdash r:\sigma}{\Gamma, \Delta \Vdash tr:\tau}\ \multimap_e$$

$$\frac{}{\Gamma \Vdash \rho^n : n}\ \mathsf{ax}_\rho \qquad \frac{\Gamma \Vdash t:n}{\Gamma \Vdash U^m t : n}\ \mathsf{u} \qquad \frac{\Gamma \Vdash t:n}{\Gamma \Vdash \pi^m t : (m,n)}\ \mathsf{m} \qquad \frac{\Gamma \Vdash t:n \quad \Delta \Vdash r:m}{\Gamma, \Delta \Vdash t \otimes r : n+m}\ \otimes$$

$$\frac{\Gamma \Vdash s:(m,n) \quad \Delta, x:n \Vdash t_0:\sigma \quad \cdots \quad \Delta, x:n \Vdash t_{2^m-1}:\sigma}{\Gamma, \Delta \Vdash \mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma}\ \mathsf{lc}$$

$$\frac{\Gamma \Vdash t_1:\sigma \quad \ldots \quad \Gamma \Vdash t_n:\sigma \quad \sum_{i=1}^n p_i = 1}{\Gamma \Vdash \sum_{i=1}^n p_i t_i : \sigma}\ + \qquad \frac{X \notin \mathrm{FV}(\Gamma) \quad \Gamma \Vdash t:\sigma}{\Gamma \Vdash t : \forall X.\sigma}\ \forall_i \qquad \frac{\Gamma \Vdash t : \forall X.\sigma}{\Gamma \Vdash t : \sigma[X/\tau]}\ \forall_e$$

Estos son los únicos cambios que introducimos. El conjunto de términos y las rescrituras quedan iguales que en los cálculos originales.

4.2. Subject Reduction

4.2.1. $\lambda_\rho 2$

El objetivo de esta sección es demostrar la propiedad de *Subject Reduction* para el cálculo. Es decir, queremos ver que:

Teorema (Subject reduction para $\lambda_\rho 2$)**.** *Sea $t \to_p t'$, entonces se tiene que:*

$$\Gamma \vdash t:\sigma \ \textit{implica}\ \Gamma \vdash t' : \sigma$$

Definición de $\prec$

Vamos a utilizar la misma relación $\prec$ definida anteriormente para System F (ver definición 2.2.1). La propiedad de estabilidad bajo la reducción se mantiene.

Definición 4.2.1 (definición de $\prec$)**.** Para todo par de tipos σ y τ, contexto Γ y todo término t tal que $\Gamma \vdash t:\tau$ como consecuencia de $\Gamma \vdash t:\sigma$:

1. Si $X \notin FV(\Gamma)$, se nota $\sigma \prec^t_{X,\Gamma} \tau$ si pasa alguno de los siguientes casos:
   - $\tau = \forall X.\sigma$.
   - $\sigma = \forall X.\sigma'$ y $\tau = \sigma'[\gamma/X]$ para algún γ y X.
2. Si V es un conjunto de variables de tipo tal que $V \cap FV(\Gamma) = \varnothing$, definimos $\preceq^t_{V,\Gamma}$ inductivamente como:
   - Si $X \in V$ y $\sigma \prec^t_{X,\Gamma} \tau$, entonces $\sigma \preceq^t_{\{X\},\Gamma} \tau$.
   - Si $V_1, V_2 \subseteq V$, $\sigma \preceq^t_{V_1,\Gamma} \tau$ y $\sigma \preceq^t_{V_2,\Gamma} \tau$, entonces $\sigma \preceq^t_{V_1 \cup V_2,\Gamma} \tau$.
   - Si $\sigma = \tau$, entonces $\sigma \preceq^t_{V,\Gamma} \tau$.

Lema 4.2.2 (Estabilidad de $\preceq$)**.** Para todo par de tipos σ, τ, conjunto de variables de tipo V, términos t y r y contexto Γ, si $\sigma \preceq^t_{V,\Gamma} \tau$, $t \to r$ y $\Gamma \vdash r : \sigma$. Entonces $\sigma \preceq^r_{V,\Gamma} \tau$. □

Lemas auxiliares

El objetivo es demostrar un lema de comparación de flechas similar al de $\lambda 2$. Vamos a expandir el mapeo $\overline{(\cdot)}$ utilizado en la demostración del lema 2.2.4 con los tipos de $\lambda_\rho 2$:

$$\begin{aligned}
\overline{(X)} &= X \\
\overline{(n)} &= n \\
\overline{((n,m))} &= (n,m) \\
\overline{(\sigma \multimap \tau)} &= \sigma \multimap \tau \\
\overline{(\forall X.\sigma)} &= \overline{(\sigma)}
\end{aligned}$$

Luego demostramos dos lemas intermedios:

Lema 4.2.3.

1. Para cualquier par de tipos σ y τ, existe un tipo γ tal que: $\overline{(\sigma[\tau/X])} = \overline{(\sigma)}[\gamma/X]$.
2. Para cualquier par de tipos σ y τ, conjunto de variables V, contexto Γ y término t, si $\sigma \preceq^t_{V,\Gamma} \tau$, existen $\vec{\gamma}$ y $\vec{X} \in V$ tales que $\overline{(\tau)} = \overline{(\sigma)}[\vec{\gamma}/\vec{X}]$.

Demostración. Demostración de (1) por inducción sobre σ:

$\sigma = n$: $\overline{(n[\tau/X])} = n = \overline{(n)}[\tau/X]$.

$\sigma = (m,n)$: $\overline{((m,n)[\tau/X])} = (m,n) = \overline{((m,n))}[\tau/X]$.

$\sigma = \sigma_1 \multimap \sigma_2$: $\overline{(\sigma_1 \multimap \sigma_2[\tau/X])} = \overline{(\sigma_1[\tau/X] \multimap \sigma_2[\tau/X])} = \sigma_1[\tau/X] \multimap [\tau/X] = (\sigma_1 \multimap \sigma_2)[\tau/X] = \overline{(\sigma_1 \multimap \sigma_2)}[\tau/X]$.

$\sigma = X$: $\overline{(X[\tau/X])} = \overline{(\tau)} = X[\overline{(\tau)}/X] = \overline{(X)}[\overline{(\tau)}/X]$.

$\sigma = Y$: Con $Y \neq X$, $\overline{(Y[\tau/X])} = Y = \overline{(Y)}[\tau/X]$.

$\sigma = \forall Y.\sigma_1$: Con $Y \neq X$ y $Y \notin \mathrm{FV}(\tau)$. $\overline{((\forall Y.\sigma_1)[\tau/X])} = \overline{((\forall Y.\sigma_1[\tau/X]))} = \overline{(\sigma_1[\tau/X])}$ Por hipótesis inductiva tenemos que $\overline{(\sigma_1[\tau/X])} = \overline{(\sigma_1)}[\gamma/X] = \overline{(\forall Y.\sigma_1)}[\gamma/X]$.

Para demostrar (2) es suficiente con mostrarlo para $\sigma \prec^t_{X,\Gamma} \tau$.

Caso 1: $\tau = \forall X.\sigma$, entonces $\overline{(\tau)} = \overline{(\sigma)}$.

Caso 2: $\sigma = \forall X.\sigma'$ y $\tau = \sigma'[\gamma/X]$. Por el resultado anterior se tiene que $\overline{(\tau)} = \overline{(\sigma'[\gamma/X])} = \overline{(\sigma')}[\gamma'/X] = \overline{(\sigma)}[\gamma'/X]$ para algún γ'. □

Con estos 2 resultados intermedios, podemos demostrar el lema de comparación de flechas:

Lema 4.2.4 (Comparación de flechas)**.** Para tipos $\sigma, \tau, \sigma', \tau'$, contexto Γ, conjunto de variables de tipo V y término t tales que $\sigma \multimap \tau \leq^t_{V,\Gamma} \sigma' \multimap \tau'$, existen tipos $\vec{\gamma}$ y variables $\vec{X} \subseteq V$ tales que:

$$(\sigma \multimap \tau)[\vec{\gamma}/\vec{X}] = \sigma' \multimap \tau'$$

Demostración. $\sigma' \multimap \tau' = \overline{(\sigma' \multimap \tau')}$. Por el lema 4.2.3 (2), existen tipos $\vec{\gamma}$ y variables de tipo $\vec{X}$ tales que $\overline{(\sigma' \multimap \tau')} = \overline{(()\sigma \multimap \tau)}[\vec{\gamma}/\vec{X}] = \sigma \multimap \tau[\vec{\gamma}/\vec{X}]$

□

Vamos a demostrar subject reduction de la misma forma que para System F. Analizando los componentes de un términos junto con sus tipos y llegando a sus respectivos reductos a través de lemas de generación. Pasamos a enunciar los lemas de generación que utilizaremos

Lema 4.2.5 (Lemas de generación)**.**

variable Si $\Gamma \vdash x : \sigma$, entonces existen tipo τ, conjunto de variables de tipo V con $\tau \leq^x_{V,\Gamma} \sigma$ tales que $x : \tau \in \Gamma$.

app Si $\Gamma \vdash tr : \sigma$, entonces existen tipos τ, σ', conjunto de variables V con $\sigma' \leq^{tr}_{V,\Gamma} \sigma$, tales que $\Gamma_1 \vdash t : \tau \multimap \sigma'$ y $\Gamma_2 \vdash r : \tau$. Con $\Gamma_1, \Gamma_2 = \Gamma$.

abs Si $\Gamma \vdash \lambda x.t : \sigma$, entonces existen tipos τ, σ', conjunto de variables V con $\tau \multimap \sigma' \leq^{\lambda x.t}_{V,\Gamma} \sigma$, tales que $\Gamma, x : \tau \vdash t : \sigma'$.

rho Si $\Gamma \vdash \rho^n : \sigma$, entonces existen tipo n, conjunto de variables de tipo V con $n \leq^{\rho^n}_{V,\Gamma} \sigma$ tales que $\Gamma \vdash \rho^n : n$.

result Si $\Gamma \vdash (b^m, \rho^n) : \sigma$, entonces existe tipo (m, n), conjunto de variables de tipo V con $(n, m) \leq^{(b^m,\rho^n)}_{V,\Gamma} \sigma$ y $n \geq m$ tales que $\Gamma \vdash \rho^n : n$.

unitary Si $\Gamma \vdash U^m t : \sigma$, entonces existe tipo n, conjunto de variables de tipo V con $n \leq^{U^m t}_{V,\Gamma} \sigma$, tales que $\Gamma \vdash t : n$.

measurement Si $\Gamma \vdash \pi^m t : \sigma$, entonces existe tipo n, conjunto de variables de tipo V con $(m, n) \leq^{U^m t}_{V,\Gamma} \sigma$ y $n \geq m$, tales que $\Gamma \vdash t : n$.

tensor Si $\Gamma \vdash t \otimes r : \sigma$, entonces existen tipos n, m, conjunto de variables V con $n+m \leq^{t\otimes r}_{V,\Gamma} \sigma$, tales que $\Gamma_1 \vdash t : n$ y $\Gamma_2 \vdash r : m$. Con $\Gamma_1, \Gamma_2 = \Gamma$

letcase Si $\Gamma \vdash \mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma$, entonces existen tipos $\sigma', (m, n)$, conjunto de variables de tipo V con $\sigma' \leq^{\text{letcase}\cdots}_{V,\Gamma,\Delta} \sigma$, tales que $\Delta, x : n \vdash t_0 : \sigma', \cdots, \Delta, x : n \vdash t_{2^m-1} : \sigma'$ y $\Gamma' \vdash r : (m, n)$. Con $\Gamma', \Delta = \Gamma$.

La demostración se consigue aplicando indución sobre los juicios de tipado.

A continuación, presentamos los lemas de strengthening y weakening. Utilizaremos estos lemas para demostrar el lema de de sustitución, la última pieza necesaria para probar subject reduction.

Lema 4.2.6 (weakening)**.** Si $\Gamma \vdash t : \sigma$ y $x \notin \mathrm{FV}(t)$, entonces, $\Gamma, x : \tau \vdash t : \sigma$. □

Lema 4.2.7 (stregthening)**.** Si $\Gamma, x : \tau \vdash t : \sigma$ y $x \notin \mathrm{FV}(t)$, entonces, $\Gamma \vdash t : \sigma$. □

Ambos lemas se pueden demostrar mediante inducción sobre la derivación de tipos de t.

Finalmente, enunciamos el último lema necesario para llevar a cabo la demostración de subject reduction.

Lema 4.2.8 (Lema de sustitución)**.** Si $\Gamma, x : \tau \vdash t : \sigma$ y $\Delta \vdash r : \tau$, entonces $\Gamma, \Delta \vdash t[r/x] : \sigma$.

Demostración. Por inducción en t:

$t = x$*:* Por lema 4.2.5 (variable), existen tipo τ, conjunto de variables de tipo V con $\tau \prec^t_{V,\Gamma} \sigma$ tales que $x : \tau \in \Gamma$. Por lema 4.2.6, $\Gamma, \Delta \vdash r : \tau$. Por definición 4.2.1 $\Gamma, \Delta \vdash r : \sigma$. Notar que $t[r/x] = r$.

$t = y \neq x$*:* Entonces por lemas 4.2.6 y 4.2.7, $\Gamma, \Delta \vdash y : \sigma$. Notar que $t[r/x] = t$.

$t = \lambda y.s$*:* Entonces $\Gamma, x : \tau \vdash \lambda y.s : \sigma$ con $y \neq x$. Por lema 4.2.5 (abs), existen tipos γ_1, γ_2 y conjunto de variables de tipo V con $\gamma_1 \multimap \gamma_2 \preceq^t_{V,\Gamma} \sigma$ tal que $\Gamma, x : \tau, y : \gamma_1 \vdash s : \gamma_2$. Por hipótesis inductiva, $\Gamma, \Delta, y : \gamma_1 \vdash s[r/x] : \gamma_2$. Como $y \notin \mathrm{FV}(r)$, aplicando la regla $\multimap_i$ nuevamente tenemos $\Gamma, \Delta \vdash \lambda y.s[r/x] : \gamma_1 \multimap \gamma_2$. Por definición 4.2.1 llegamos a $\Gamma, \Delta \vdash \lambda y.s[r/x] : \sigma$.

$t = t_1 t_2$*:* Por lema 4.2.5 (app), existen tipos τ, σ', conjunto de variables V con $\sigma' \preceq^t_{V,\Gamma} \sigma$, tales que $\Gamma_1 \vdash t : \tau \multimap \sigma'$ y $\Gamma_2 \vdash r : \tau$. Con $\Gamma_1, \Gamma_2 = \Gamma, x : \tau$.

- $x : \tau \in \Gamma_1$, entonces por hipótesis inductiva: $\Gamma_1 \setminus \{x : \tau\} \vdash t_1[r/x] : \gamma \multimap \sigma$. Por la regla $\multimap_e$, $\Gamma_1 \setminus \{x : \tau\}, \Gamma_2 \vdash t_1[r/x]t_2 : \sigma$. Notar que $\Gamma_1 \setminus \{x : \tau\}, \Gamma_2 = \Gamma$ y $t_1[r/x]t_2 = (t_1 t_2)[r/x]$.
- $x : \tau \in \Gamma_2$, entonces por hipótesis inductiva: $\Gamma_2 \setminus \{x : \tau\} \vdash t_2[r/x] : \gamma$. Por la regla $\multimap_e$, $\Gamma_1, \Gamma_2 \setminus \{x : \tau\} \vdash t_1 t_2[r/x] : \sigma$. Notar que $\Gamma_1, \Gamma_2 \setminus \{x : \tau\} = \Gamma$ y $t_1 t_2[r/x] = (t_1 t_2)[r/x]$.

$t = \rho^n$*:* Entonces lemas 4.2.6 y 4.2.7, $\Gamma, \Delta \vdash \rho^n : \sigma$. Notar que $t[r/x] = t$

$t = U^m s$*:* Por lema 4.2.5 (unitary), existe n tipo, conjunto de variables de tipo V con $n \preceq^t_{V,\Gamma} \sigma$, tales que $\Gamma, x : \tau \vdash s : n'$. Por hipótesis inductiva $\Gamma, \Delta \vdash s[r/x] : n$, y por regla u, $\Gamma, \Delta \vdash U^m s[r/x] : n$. Por definición 4.2.1, Por regla u, $\Gamma, \Delta \vdash U^m s[r/x] : \sigma$. Notar que $U^m s[r/x] = (U^m s)[r/x]$.

$t = \pi^m s$*:* Por lema 4.2.5 (measurement), existe (m, n) tipo, conjunto de variables de tipo V con $(m, n) \preceq^t_{V,\Gamma} \sigma$, tales que $\Gamma, x : \tau \vdash s : n$. Por hipótesis inductiva $\Gamma, \Delta \vdash s[r/x] : n$, y por regla m, $\Gamma, \Delta \vdash \pi^m s[r/x] : (m, n)$. Por definición 4.2.1, $\Gamma, \Delta \vdash \pi^m s[r/x] : \sigma$. Notar que $\pi^m s[r/x] = (\pi^m s)[r/x]$.

$t = t_1 \otimes t_2$*:* Por lema 4.2.5 (tensor), existen tipos n, m, conjunto de variables V con $n + m \preceq^t_{V,\Gamma} \sigma$, tales que $\Gamma_1 \vdash t : n$ y $\Gamma_2 \vdash r : m$. Con $\Gamma_1, \Gamma_2 = \Gamma, x : \tau$.

- $x : \tau \in \Gamma_1$, entonces $x \notin \mathrm{FV}(t_2)$. Por hipótesis inductiva, $\Gamma_1 \setminus \{x : \tau\} \vdash t_1[r/x] : n$. Por la regla $\otimes$, $\Gamma_1 \setminus \{x : \tau\}, \Gamma_2 \vdash t_1[r/x] \otimes t_2 : n + m$. Por definición 4.2.1 obtenemos $\Gamma_1 \setminus \{x : \tau\}, \Gamma_2 \vdash t_1[r/x] \otimes t_2 : \sigma$. Notar que $\Gamma_1 \setminus \{x : \tau\}, \Gamma_2 = \Gamma$ y $t_1[r/x] \otimes t_2 = (t_1 \otimes t_2)[r/x]$.
- $x : \tau \in \Gamma_2$, entonces $x \notin \mathrm{FV}(t_1)$. Por hipótesis inductiva, $\Gamma_2 \setminus \{x : \tau\} \vdash t_2[r/x] : m$. Por la regla $\otimes$, $\Gamma_1, \Gamma_2 \setminus \{x : \tau\} \vdash t_1 \otimes t_2[r/x] : n + m$. Por definición 4.2.1 obtenemos $\Gamma_1, \Gamma_2 \setminus \{x : \tau\} \vdash t_1 \otimes t_2[r/x] : \sigma$. Notar que $\Gamma_1, \Gamma_2 \setminus \{x : \tau\} = \Gamma$ y $t_1 \otimes t_2[r/x] = (t_1 \otimes t_2)[r/x]$.

$t = (b^m, \rho^n)$*:* Entonces lemas 4.2.6 y 4.2.7, $\Gamma, \Delta \vdash (b^m, \rho^n) : \sigma$. Notar que $t[r/x] = t$

$t = \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$*:* Por lema 4.2.5 (letcase) existen tipos $\sigma', (m, n)$ y conjunto de variables de tipo V con $\sigma' \leq^t_{V,(\Gamma)} \sigma$ tal que $\Delta, y : n \vdash t_i : \sigma'$ y $\Gamma' \vdash s : (m, n)$. Con $\Gamma', \Delta = \Gamma$, tenemos 2 casos:

- $x : \tau \in \Gamma'$, entonces $x \notin \mathrm{FV}(t_i)$. Por hipótesis inductiva, $\Gamma' \setminus \{x : \tau\} \vdash s[r/x] : (m, n)$. Por la regla lc, $\Gamma' \setminus \{x : \tau\}, \Delta' \vdash \mathsf{letcase}\ y = s[r/x]\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma'$. Notar que $\Gamma' \setminus \{x : \tau\}, \Delta' = \Gamma, \Delta$ y $\mathsf{letcase}\ y = s[r/x]\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} = (\mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x]$. Por definición 4.2.1 $\Gamma, \Delta \vdash \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x] : \sigma$.
- $x : \tau \in \Delta'$, entonces $x \notin \mathrm{FV}(s)$. Por hipótesis inductiva: para todo $i = 0, \cdots, 2^{m-1}$, $\Delta' \setminus \{x : \tau\} \vdash t_i[r/x] : \sigma'$. Por la regla lc, $\Gamma', \Delta' \setminus \{x : \tau\} \vdash \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\} : \sigma'$. Notar que $\Gamma', \Delta' \setminus \{x : \tau\} = \Gamma, \Delta$ y $\mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}\}[r/x] = (\mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x]$. Por definición 4.2.1 $\Gamma, \Delta \vdash \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x] : \sigma$. □

Con estos lemas definidos, tenemos las piezas para demostrar la propiedad de *Subject Reduction* para $\lambda_\rho 2$.

Demostración de *Subject Reduction*

Teorema 4.2.9 (Subject reduction para $\lambda_\rho 2$)**.** *Para todo par de términos t y t', contexto Γ y tipo σ, si $t \to_p t'$ y $\Gamma \vdash t : \sigma$, entonces $\Gamma \vdash t' : \sigma$.*

Demostración. Demostración por inducción sobre $\to_p$.

- $t = (\lambda x.s)r$ y $t' = t[r/x]$.

  $\Gamma \vdash (\lambda x.s)r : \sigma$. Por lema 4.2.5 (app) tenemos que existen tipos γ, τ y conjunto de variables de tipo V_1 con $\gamma \leq^t_{V_1,(\Gamma,\Delta)} \sigma$ tales que $\Gamma' \vdash \lambda x.s : \tau \multimap \gamma$ y $\Delta \vdash r : \tau$ con $\Gamma', \Delta = \Gamma$.

  Por lema 4.2.5 (abs) para $\Gamma' \vdash \lambda x.s : \tau \multimap \gamma$ tenemos que existen tipos γ', τ', conjunto de variables de tipo V_2 con $\tau' \multimap \gamma' \leq^{\lambda x.s}_{V_2,\Gamma} \tau \multimap \gamma$ tales que $\Gamma', x : \tau' \vdash s : \gamma'$.

  Por lema 4.2.4 existen tipos $\vec{\chi}$ y variables de tipo $\vec{X} \in V$ tales que $\gamma = \gamma'[\vec{\chi}/\vec{X}]$ y $\tau = \tau'[\vec{\chi}/\vec{X}]$.

  Además, como $\vec{X} \notin FV(\Gamma), \Gamma'[\vec{\chi}/\vec{X}] = \Gamma'$. Entonces por definición 4.2.1 $\Gamma', x : \tau \vdash s : \gamma$ y por lema 4.2.8 $\Gamma', \Delta \vdash s[r/x] : \gamma$. Por lema 4.2.2, tenemos que $\Gamma', \Delta \vdash s[r/x] : \sigma$.

- $t = U^m \rho^n$ y $t' = \rho'^n$.

  $\Gamma \vdash U^m \rho^n : \sigma$. Por lema 4.2.5 (unitary), existen n tipo y conjunto de variables V con $n \preceq^t_{V,\Gamma} \sigma$ tales que $\Gamma \vdash \rho^n : n$. Por ax_ρ, $\Gamma \vdash \rho'^n : n$. Por lema 4.2.2 $n \preceq^{t'}_{V,\Gamma} \sigma$ y, por definición 4.2.1, $\Gamma \vdash \rho'^n : \sigma$.

- $t = \pi^m \rho^n$ y $t' = (b^m, \rho'^n)$.

  $\Gamma \vdash \pi^m \rho^n : \sigma$. Por lema 4.2.5 (measurement), existen (m, n) tipo y conjunto de variables V con $(m, n) \preceq^t_{V,\Gamma} \sigma$ tales que $\Gamma \vdash \rho^n : n$. Por ax_ρ $\Gamma \vdash \rho'^n : n$ y, por regla m, $\Gamma \vdash (b^m, \rho'^n) : (m, n)$. Por lema 4.2.2 $n \preceq^{t'}_{V,\Gamma} \sigma$ y, por definición 4.2.1, $\Gamma \vdash \rho'^n : \sigma$.

- $t = \rho_1 \otimes \rho_2$ y $t' = \rho'$.

  $\Gamma \vdash \rho_1 \otimes \rho_2 : \sigma$. Por lema 4.2.5 (tensor), existen m, n tipos y conjunto de variables V con $m + n \preceq^t_{V,\Gamma} \sigma$ tales que $\Gamma_1 \vdash \rho_1 : n$ y $\Gamma_2 \vdash \rho_2 : m$ con $\Gamma_1, \Gamma_2 = \Gamma$. Como ρ' es el resultado de tomar $\rho_1 \otimes \rho_2$, su dimensión es la suma de las dimensiones de ρ_1 y ρ_2. Por ax_ρ, $\Gamma \vdash \rho' : n + m$. Por lema 4.2.2 $n + m \preceq^{t'}_{V,\Gamma} \sigma$ y, por definición 4.2.1, $\Gamma \vdash \rho'^n : \sigma$.

- $t = \mathsf{letcase}\ x = (b^m, \rho^n)\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ y $t' = t_{b^m}[\rho^n/x]$.

  $\Gamma \vdash \mathsf{letcase}\ x = (b^m, \rho^n)\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma$. Usando el lema 4.2.5 (letcase) tenemos que existen tipo σ' y conjunto de variables V con $\sigma' \preceq^t_{V,\Gamma} \sigma$ tales que $\Delta, x : n \vdash t_{b^m} : \sigma'$ y $\Gamma' \vdash (b^m, \rho^n) : (m, n)$ con $\Gamma', \Delta = \Gamma$. Por ax_ρ, $\Gamma' \vdash \rho^n : n$.

  Por el lema 4.2.8, llegamos a $\Gamma', \Delta \vdash t_{b^m}[\rho^n/x] : \sigma'$. Finalmente por definición 4.2.1 y lema 4.2.2, vale que $\Gamma', \Delta \vdash t_{b^m}[\rho^n/x] : \sigma$.

Continuamos con los casos contextuales. Sea $s \to_p s'$:

- $t = \lambda x.s$ y $t' = \lambda x.s'$.

  $\Gamma \vdash \lambda x.s : \sigma$. Por lema 4.2.5 (abs), existen tipos τ, γ y conjunto de variables de tipo V tales que $\tau \multimap \gamma \preceq^t_{V,\Gamma} \sigma$ y $\Gamma, x : \tau \vdash s : \gamma$. Por HI, $\Gamma, x : \tau \vdash s' : \gamma$. Aplicando la introducción de la abstracción llegamos a $\Gamma \vdash \lambda x.s' : \tau \multimap \gamma$. Por definición 4.2.1 y lema 4.2.2 obtenemos $\Gamma \vdash \lambda x.s' : \sigma$.

- $t = sr$ y $t' = s'r$.

  $\Gamma_1 \vdash rs : \sigma$. Por el lema 4.2.5 (app), existen tipos τ, γ y conjunto de variables de tipo V tal que $\gamma \preceq^t_{V,(\Gamma_1,\Gamma_2)} \sigma$ y $\Gamma_1 \vdash s : \tau \multimap \gamma$ y $\Gamma_2 \vdash r : \gamma$ con $\Gamma_1, \Gamma_2 = \Gamma$. Por HI, $\Gamma_1 \vdash s' : \tau \multimap \gamma$. Por regla $\to_e$, $\Gamma_1, \Gamma_2 \vdash s'r : \gamma$. Luego, por definición 4.2.1 y lema 4.2.2 llegamos a $\Gamma_1, \Gamma_2 \vdash rs' : \sigma$.

- $t = rs$ y $t' = rs'$.

  $\Gamma \vdash rs : \sigma$. Por el lema 4.2.5 (app), existen tipos τ, γ y conjunto de variables de tipo V tales que $\gamma \preceq^t_{V,\Gamma} \sigma$ y $\Gamma_1 \vdash r : \tau \multimap \gamma$ y $\Gamma_2 \vdash s : \tau$ con $\Gamma_1, \Gamma_2 = \Gamma$. Por HI, $\Gamma_2 \vdash s' : \tau$. Por regla $\to_e$, $\Gamma_1, \Gamma_2 \vdash rs' : \gamma$. Finalmente por definición 4.2.1 y lema 4.2.2 llegamos a $\Gamma_1, \Gamma_2 \vdash rs' : \sigma$.

- $t = U^m s$ y $t' = U^m s'$.

  $\Gamma \vdash U^m s : \sigma$. Por lema 4.2.5 (unitary), existen τ tipo y conjunto de variables de tipo V tales que $\tau \prec^t_{V,\Gamma} \sigma$ y $\Gamma \vdash s : \tau$. Por HI, $\Gamma \vdash s' : \tau$. Por regla u, $\Gamma \vdash U^m s' : \tau$. Por

definición 4.2.1 y lema 4.2.2, tenemos que $\Gamma \vdash U^m s' : \sigma$.

- $t = \pi^m s$ y $t' = \pi^m s'$.

  $\Gamma \vdash U^m s : \sigma$. Por lema 4.2.5 (measurement), existen τ tipo y conjunto de variables de tipo V tales que $\tau \preceq^t_{V,\Gamma} \sigma$ y $\Gamma \vdash s : \tau$. Por HI, $\Gamma \vdash s' : \tau$. Por regla m, $\Gamma \vdash \pi^m s' : \tau$. Por definición 4.2.1 y lema 4.2.2, tenemos que $\Gamma \vdash \pi^m s' : \sigma$.

- $t = s \otimes r$ y $t' = s' \otimes r$.

  $\Gamma \vdash r \otimes s : \sigma$. Por el lema 4.2.5 (tensor), existen tipos n, m y conjunto de variables de tipo V tales que $n + m \preceq^t_{V,\Gamma} \sigma$ y $\Gamma_1 \vdash r : n$ y $\Gamma_2 \vdash s : m$ con $\Gamma_1, \Gamma_2 = \Gamma$. Por HI, $\Gamma_1 \vdash r' : n$. Por regla $\otimes$, $\Gamma_1, \Gamma_2 \vdash r' \otimes s : n + m$. Finalmente por definición 4.2.1 y lema 4.2.2 llegamos a $\Gamma_1, \Gamma_2 \vdash r' \otimes s : \sigma$.

- $t = r \otimes s$ y $t' = r \otimes s'$.

  $\Gamma \vdash r \otimes s : \sigma$. Por el lema 4.2.5 (tensor), existen tipos n, m y conjunto de variables de tipo V tales que $n + m \preceq^t_{V,\Gamma} \sigma$ y $\Gamma_1 \vdash r : n$ y $\Gamma_2 \vdash s : m$ con $\Gamma_1, \Gamma_2 = \Gamma$. Por HI, $\Gamma_2 \vdash s' : m$. Por regla $\otimes$, $\Gamma_1, \Gamma_2 \vdash r \otimes s' : n + m$. Finalmente por definición 4.2.1 y lema 4.2.2 llegamos a $\Gamma_1, \Gamma_2 \vdash r \otimes s' : \sigma$.

- $t = \mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ y $t' = \mathsf{letcase}\ x = s'\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$.

  $\Gamma \vdash \mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m} - 1\} : \sigma$. Por el lema 4.2.5 (letcase), existen τ tipo y conjunto de variables de tipo V con $\tau \preceq^t_{V,\Gamma} \sigma$ tales que $\Gamma' \vdash s : (m, n)$ y para todo $i = 0, \cdots, 2^{m-1}$, $\Delta, x : n \vdash t_i : \tau$ con $\Gamma', \Delta = \Gamma$. Por HI, $\Gamma' \vdash s' : (m, n)$. Luego por regla lc, $\Gamma, \Delta \vdash \mathsf{letcase}\ x = s'\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \tau$. Por definición 4.2.1 y lema 4.2.2 tenemos $\Gamma, \Delta \vdash \mathsf{letcase}\ x = s'\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma$. □

4.2.2. $\lambda_\rho^\circ 2$

Para el caso de $\lambda_\rho^\circ 2$ vamos a tomar la misma estrategia que en la sección anterior, probando para cada lema los casos que no se encuentran contemplados en las demostraciones anteriores. Vale aclarar que la definición de $\prec$ es la misma para los dos cálculos.

Lemas auxiliares

Los lemas enunciados en la secciones anteriores que tratan sobre la relación $\preceq$, siguen aplicando para el caso de $\lambda_\rho^\circ 2$. Primero agregamos el caso de la suma a los lemas de generación, la demostración también se consigue mediante inducción sobre los juicios de tipado.

Lema 4.2.10 (Lemas de generación)**.**

sum $\Gamma \vdash \sum_i p_i t_i : \sigma$ entonces, existen tipo τ, conjunto de variables de tipo V con $\tau \preceq^{\sum_i p_i t_i}_{V,\Gamma} \sigma$, tales que $\Gamma \vdash t_i : \tau$.

Luego adaptamos el lema de sustitución con los casos agregados por $\lambda_\rho^\circ 2$.

Lema 4.2.11 (Lema de sustitución)**.** Si $\Gamma, x : \tau \Vdash t : \sigma$ y $\Delta \Vdash r : \tau$, entonces $\Gamma, \Delta \Vdash t[r/x] : \sigma$.

Demostración. Al igual que para $\lambda_\rho 2$ hacemos inducción sobre t. Es decir, descartamos el caso de la medición explícita $t = (b^m, \rho^n)$ y agregamos la sumatoria de términos.

$t = \sum_i p_i t_i$: Por lema 4.2.10 (sum), existen tipo σ', conjunto de variables de tipo V con $\sigma' \preceq^t_{V,\Gamma,x:\tau} \sigma$ con $\Gamma, x : \tau \Vdash t_i : \sigma'$. Por hipótesis inductiva, $\Gamma \Vdash t_i[r/x] : \sigma'$ y por regla $+$ $\sum_i p_i t_i[r/x] : \sigma'$. Finalmente por deficinición 4.2.1, $\sum_i p_i t_i[r/x] : \sigma$. Notar que $\sum_i p_i t_i[r/x] = (\sum_i p_i t_i)[r/x]$.

El resto de los casos son idénticos a los tratados en la sección anterior. □

Demostración de *Subject Reduction*

Teorema 4.2.12 (Subject reduction para $\lambda_\rho 2$)**.** *Para todo par de términos t y t', contexto Γ y tipo σ, si $t \rightsquigarrow t'$ y $\Gamma \Vdash t : \sigma$, entonces $\Gamma \Vdash t' : \sigma$.*

Demostración. Similarmente al caso anterior, realizamos inducción sobre $\rightsquigarrow$. Tenemos que tener en cuenta las diferentes reducciones que involucran la sumatoria de términos.

- $t = \mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ y $t' = \sum_i p_i t_i[\rho^n_i/x]$.

  $\Gamma \Vdash \mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma$. Por lema 4.2.5 (letcase), existen tipo τ y conjunto de variables de tipo V con $\tau \preceq^t_{V,\Gamma} \sigma$ tales que $\Delta, x : n \Vdash t_i : \tau\ \forall 0 \leq i < 2^m$ y $\Gamma' \Vdash \pi^m \rho^n : (m, n)$ con $\Gamma', \Delta = \Gamma$.

  Por la regla $+$ podemos concluir $\Delta, x : n \Vdash \sum_i p_i t_i : \tau$ donde $p_i = \mathrm{tr}(\overline{\pi_i}^\dagger \overline{\pi_i} \rho^n)$. Por ax_ρ tenemos que $\Gamma' \Vdash \rho^n_i : n$, donde $\rho^n_i = \frac{\overline{\pi_i} \rho^n \overline{\pi_i}^\dagger}{p_i}$.

  Entonces por lema 4.2.11 $\Gamma, \Delta \Vdash \sum_i p_i t_i[\rho^n_i/x] : \tau$. Finalmente, por definición 4.2.1 y lema 4.2.2 llegamos a $\Gamma, \Delta \Vdash \sum_i p_i t_i[\rho^n_i/x] : \sigma$.

- $t = \sum_i p_i \rho_i$ y $t' = \rho'$ con $\rho' = \sum_i p_i \rho_i$.

  $\Gamma \Vdash \sum_i p_i \rho_i : \sigma$ por lema 4.2.10 (sum) existen tipo τ y conjunto de variables de tipo V con $\tau \preceq^t_{V,\Gamma} \sigma$ tales que $\Gamma \Vdash \rho_i : \tau$.

  Por lema 4.2.5 (rho), Existe n tipo y V' variables de tipo con $n \preceq^{\rho_i}_{V',\Gamma}$ tales que $\Gamma \Vdash \rho_i : n$. Como los ρ_i tienen dimensión n y $\rho' = \sum_i p_i \rho_i$, por regla ax_ρ $\Gamma \Vdash \rho' : n$. Finalmente por definición 4.2.1 y lema 4.2.2, llegamos a $\Gamma \Vdash \rho' : \sigma$

- $t = \sum_i p_i s$ y $t' = s$.

  Por lema 4.2.10 (sum) existen tipo τ y conjunto de variables de tipo V con $\tau \preceq^t_{V,\Gamma} \sigma$ tales que $\Gamma \Vdash s : \tau$. Por lemas 4.2.2 y 4.2.1, $\Gamma \Vdash s : \sigma$.

- $t = (\sum_i p_i t_i) r$ y $t' = \sum_i p_i (t_i r)$.

  $\Gamma \Vdash (\sum_i p_i t_i) r : \sigma$. Por lema 4.2.5 (app), existen tipos τ, γ y conjunto de variables de tipo V con $\tau \preceq^t_{V,\Gamma} \sigma$ tales que $\Gamma' \Vdash (\sum_i p_i t_i) : \gamma \multimap \tau$ y $\Delta \Vdash r : \gamma$ con $\Gamma', \Delta = \Gamma$.

Por lema 4.2.10 (sum) existen tipo τ' y conjunto de variables de tipo V' con $\tau' \leq^{\sum p_i t_i}_{V',\Gamma} \gamma \multimap \tau$ tales que $\Gamma \Vdash t_i : \tau'$. Por definición 4.2.1 $\Gamma \vdash t_i : \gamma \multimap \tau$ y, por regla $\multimap_e$, $\Gamma, \Delta \Vdash t_i r : \tau$ para cada i. Aplicando la regla + llegamos a $\Gamma, \Delta \Vdash \sum_i p_i (t_i r) : \tau$. Usando la definición 4.2.1 y lema 4.2.2, llegamos a $\Gamma, \Delta \Vdash \sum_i p_i (t_i r) : \sigma$.

El único caso faltante es caso contextual para la sumatoria.

- $t = \sum_i p_i t_i$ y $t' = \sum_i p_i r_i$, con $t_j \rightsquigarrow r_j$ y $\forall i \neq j,\ t_i = r_i$.

  $\Gamma \Vdash \sum_i p_i t_i : \sigma$. Por lema 4.2.10 (sum) existen tipo τ y conjunto de variables de tipo V con $\tau \leq^t_{V,\Gamma} \sigma$ tales que $\Gamma \Vdash t_i : \tau$. Por hipótesis inductiva $\Gamma \Vdash r_i : \tau$ y por la regla de la suma tenemos que $\Gamma \Vdash \sum_i p_i r_i : \tau$. finalmente por definición 4.2.1, llegamos a $\Gamma \Vdash \sum_i p_i r_i : \sigma$. □

4.3. Normalización Fuerte

4.3.1. $\lambda_\rho 2$

La demostración de normalización fuerte para $\lambda_\rho 2$ tiene la misma forma que para System F. Primero dar una interpretación de tipos que sean candidatos de reducibilidad. Luego mostrar que todos los términos pertenecen a las interpretaciones de sus tipos. Ya que los candidatos de reducibilidad están incluidos en el conjunto de los términos fuertemente normalizantes, mostramos que todos los terminos tipables están en ese mismo conjunto.

Lemas útiles

En este caso vamos a agregar el letcase a la lista de términos neutrales. Por lo tanto, para $\lambda_\rho 2$ definimos como términos neutrales a las variables aplicaciones y letcase.

Adicionalmente, definimos $\mathrm{Red}(t) = \{t' \mid t \to_p t'\}$.

Consideramos que un conjunto de términos R de λ_ρ es un candidato de reducibilidad (notado $R \in \mathrm{CR}$) si cumple las mismas condiciones:

CR1: $R \subseteq \mathrm{SN}$.

CR2: Si $t \in R$ y $R \to_p t'$, entonces $t' \in R$.

CR3: Si t neutral y $\mathrm{Red}(t) \subseteq R$, entonces $t \in R$.

Incluimos a la interpretación de tipos el caso de n y (m, n). Los interpretamos como el conjunto de términos fuertemente normalizantes.

$$
\begin{aligned}
[\![X]\!]_\alpha &= \alpha(X) && \text{Donde } \alpha \text{ es una valuación tal que } \alpha : V \to \mathrm{CR}.\\
[\![n]\!]_\alpha &= \mathrm{SN}\\
[\![(m,n)]\!]_\alpha &= \mathrm{SN}\\
[\![\sigma \multimap \tau]\!]_\alpha &= [\![\sigma]\!]_\alpha \to [\![\tau]\!]_\alpha && \text{Donde } R_1 \to R_2 = \{t \mid \forall v \in R_1, tv \in R_2\}.\\
[\![\forall X.\sigma]\!]_\alpha &= \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha, X=R}
\end{aligned}
$$

Lema 4.3.1. Para todo tipo σ, $[\![\sigma]\!]_\alpha \in \mathrm{CR}$.

Demostración. Probamos por inducción en σ:

- $[\![n]\!]_\alpha = [\![(m,n)]\!]_\alpha = \mathrm{SN}$.

  CR1: Se cumple trivialmente.

  CR2: $t \in \mathrm{SN}$. Luego no puede existir $t \to_p t'$ tal que $t' \notin \mathrm{SN}$.

  CR3: $\mathrm{Red}(t) \subseteq \mathrm{SN}$. Entonces $\forall t \to_p t',\ t' \in \mathrm{SN}$. Entonces, ninguna reducción de t admite una cadena infinita de reducciones. Luego, t tampoco. Por lo tanto $t \in \mathrm{SN}$.

- $[\![\sigma \multimap \tau]\!]_\alpha = \{t \mid \forall v \in [\![\sigma]\!]_\alpha,\ tv \in [\![\tau]\!]_\alpha\}$.

  CR1: $tv \in [\![\tau]\!]_\alpha$. Por HI $[\![\tau]\!]_\alpha \in \mathrm{CR}$. Entonces $tv \in \mathrm{SN}$ luego, $t \in \mathrm{SN}$.

  CR2: $t \in [\![\sigma \multimap \tau]\!]_\alpha$. Entonces $\forall v \in [\![\sigma]\!]_\alpha,\ tv \in [\![\tau]\!]_\alpha$. Por HI $\forall v \in [\![\sigma]\!]_\alpha,\ t'v \in [\![\tau]\!]_\alpha$. Luego $t' \in [\![\sigma \multimap \tau]\!]_\alpha$.

  CR3: $\mathrm{Red}(t) \subseteq [\![\sigma \multimap \tau]\!]_\alpha$ y t neutral. Entonces $\forall t' \in \mathrm{Red}(t)$ y $v \in [\![\sigma]\!]_\alpha, t'v \in [\![\tau]\!]_\alpha$. Por HI $[\![\sigma]\!]_\alpha \in \mathrm{CR}$. Por lo tanto, $v \in \mathrm{SN}$.

  Sea $|v|$ la máxima cantidad de pasos hasta llegar a forma normal. Razonando por inducción en $|v|$, $\forall v \in [\![\sigma]\!]_\alpha$, tv reduce a:

  1. $t'v$ con t' a un paso de t, pero $t' \in [\![\sigma \multimap \tau]\!]_\alpha$. Entonces, $t'v \in [\![\tau]\!]_\alpha$.
  2. tv' con $|v'| < |v|$. Por la segunda HI, $tv' \in [\![\tau]\!]_\alpha$.

  Dado que t es neutral, las anteriores son las únicas reducciones posibles. Entonces $\mathrm{Red}(tv) \subseteq [\![\tau]\!]_\alpha$ y como es una aplicación tv es neutral. Entonces por la primer HI (CR3) $\forall v \in [\![\sigma]\!]_\alpha,\ tv \in [\![\tau]\!]_\alpha$. Entonces, $t \in [\![\sigma \multimap \tau]\!]_\alpha$.

- $[\![X]\!]_\alpha = \alpha(X)$ y por definición $\alpha(X) \in \mathrm{CR}$.

- $[\![\forall X.\sigma]\!]_\alpha = \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha, X=R}$.

  CR1: Por HI, $\forall R \in \mathrm{CR}\ [\![\sigma]\!]_{\alpha,X=R} \subseteq \mathrm{SN}$. Entonces $\bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha,X=R} \subseteq \mathrm{SN}$.

  CR2: $\forall R \in \mathrm{CR},\ t \in [\![\sigma]\!]_{\alpha,X=R}$. Por HI $\forall R \in \mathrm{CR},\ t' \in [\![\sigma]\!]_{\alpha,X=R}$. Entonces, $t' \in \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha,X=R}$. Luego, $t' \in [\![\forall X.\sigma]\!]_\alpha$.

CR3: $\forall R \in \mathrm{CR}$, $\mathrm{Red}(t) \subseteq [\![\sigma]\!]_{\alpha,X=R}$. Por HI $\forall R \in \mathrm{CR}$, $t \in [\![\sigma]\!]_{\alpha,X=R}$. Entonces, $t \in \bigcap_{R\in\mathrm{CR}} [\![\sigma]\!]_{\alpha,X=R}$. Luego, $t \in [\![\forall X.\sigma]\!]_\alpha$. □

Con ese lema tenemos que las interpretaciones de los tipos definen candidatos de reducibilidad. Lo siguiente es demostrar que las variables pertenecen a las interpretaciones de todos los tipos. Al igual que en System F, los candidatos de reducibilidad nunca son vacios.

Lema 4.3.2. Para toda variable x y tipo σ, $x \in [\![\sigma]\!]_\alpha$.

Demostración. La variable x es neutra y $\mathrm{Red}(x) = \varnothing \subseteq [\![\sigma]\!]_\alpha$. Por CR3, $x \in [\![\sigma]\!]_\alpha$. □

Dado un contexto Γ, decimos que una sustitución χ satisface Γ con la valuación α (Notado $\chi, \alpha \vDash \Gamma$) cuando $x : \sigma \in \Gamma$ implica $\chi(x) \in [\![\sigma]\!]_\alpha$. Un juicio de tipado $\Gamma \vdash t : \sigma$ se dice válido (Notado $\Gamma \vDash t : \sigma$) si para cada valuación α y sustitución χ que satisfacen Γ tenemos que $\chi(t) \in [\![\sigma]\!]_\alpha$.

Antes de demostrar adecuación, vamos a necesitar un lema auxiliar para el caso de $\forall_e$.

Lema 4.3.3. Para todo tipo σ y τ y toda valuación α definida en $\mathrm{FV}(\sigma) \setminus \{X\} \cup \mathrm{FV}(\tau)$,

$$[\![\sigma[\tau/X]]\!]_\alpha = [\![\sigma]\!]_{\alpha,X=[\![\tau]\!]_\alpha}$$

Demostración. Inducción sobre σ.

$\sigma = n$
$[\![n[\tau/X]]\!]_\alpha = [\![n]\!]_\alpha$. Podemos redefinir α de manera tal que $X = [\![\tau]\!]_\alpha$, $[\![n]\!]_\alpha = [\![n]\!]_{\alpha,X=[\![\tau]\!]_\alpha}$.

$\sigma = (m, n)$
$[\![(n,m)[\tau/X]]\!]_\alpha = [\![(n,m)]\!]_\alpha$. Podemos redefinir α de manera tal que $X = [\![\tau]\!]_\alpha$, $[\![(n,m)]\!]_\alpha = [\![(n,m)]\!]_{\alpha,X=[\![\tau]\!]_\alpha}$.

$\sigma = \sigma_1 \multimap \sigma_2$
$[\![(\sigma_1 \multimap \sigma_2)[\tau/X]]\!]_\alpha = [\![\sigma_1[\tau/X] \multimap \sigma_2[\tau/X]]\!]_\alpha = [\![\sigma_1[\tau/X]]\!]_\alpha \to [\![\sigma_2[\tau/X]]\!]_\alpha$. Por hipótesis inductiva, es igual a $[\![\sigma_1]\!]_{\alpha,X=[\![\tau]\!]_\alpha} \to [\![\sigma_2]\!]_{\alpha,X=[\![\tau]\!]_\alpha} = [\![\sigma_1 \multimap \sigma_2]\!]_{\alpha,X=[\![\tau]\!]_\alpha}$.

$\sigma = X$
$[\![X[\tau/X]]\!]_\alpha = [\![\tau]\!]_\alpha$. Podemos redefinir α de manera tal que $X = [\![\tau]\!]_\alpha$, $[\![\tau]\!]_\alpha = [\![X]\!]_{\alpha,X=[\![\tau]\!]_\alpha}$.

$\sigma = Y$ con $Y \neq X$
$[\![Y[\tau/X]]\!]_\alpha = [\![Y]\!]_\alpha$. Podemos redefinir α de manera tal que $X = [\![\tau]\!]_\alpha$, $[\![Y]\!]_\alpha = [\![Y]\!]_{\alpha,X=[\![\tau]\!]_\alpha}$.

$\sigma = \forall Y.\sigma'$ con $Y \neq X$ y $Y \notin \mathrm{FV}(\tau)$
$[\![(\forall Y.\sigma')[\tau/X]]\!]_\alpha = [\![\forall Y.\sigma'[\tau/X]]\!]_\alpha = \bigcap_{R\in CR} [\![\sigma'[\tau/X]]\!]_{\alpha,Y=R}$. Aplicando la hipótesis inductiva, llegamos a $\bigcap_{R\in CR} [\![\sigma']\!]_{\alpha,Y=R,X=[\![\tau]\!]_\alpha} = [\![\forall Y.\sigma']\!]_{\alpha,X=[\![\tau]\!]_\alpha}$. □

Ya tenemos las herramientas para demostrar el lema de adecuación.

Lema 4.3.4 (Adecuación)**.** Todo juicio de tipado es válido. Es decir, para todo contexto Γ, término t y tipo σ tales que $\Gamma \vdash t : \sigma$, se tiene $\Gamma \vDash t : \sigma$.

Demostración. Probamos por inducción la derivación del juicio de tipado.

$\dfrac{}{\Gamma, x : \sigma \vdash x : \sigma}$

Si $\chi, \alpha \vDash \Gamma, x : \sigma$. Entonces $\chi(x) \in [\![\sigma]\!]_\alpha$. Cumple por definición.

$\dfrac{\Gamma, x : \sigma \vdash t : \tau}{\Gamma \vdash \lambda x.t : \sigma \multimap \tau}$

Sean $\chi, \alpha \vDash \Gamma$. Para probar que $\chi(\lambda x.t) \in [\![\sigma \multimap \tau]\!]_\alpha$, hay que ver que $\forall r \in [\![\sigma]\!]_\alpha$, $\chi(\lambda x.t)r \in [\![\tau]\!]_\alpha$.

Si $\mathrm{Red}(\chi(\lambda x.t)r) \subseteq [\![\tau]\!]_\alpha$, dado que el término es neutral podemos concluir por CR3 que $\chi(\lambda x.t)r \in [\![\tau]\!]_\alpha$. Las siguientes son las reducciones posibles razonando por inducción en $|r| + |t|$.

- $\chi(\lambda x.t)r = (\lambda x.\chi(t))r \to_1 [r/x], \chi(t)$. Como $\chi, \alpha \vDash \Gamma$ entonces, $[r/x], \chi, \alpha \vDash \Gamma, x : \sigma$. Por hipótesis inductiva $\Gamma, x : \sigma \vDash t : \tau$, luego $[r/x], \chi(t) \in [\![\tau]\!]_\alpha$.
- Reducción interna dentro de la abstracción, $\chi(\lambda x.t)r \to_p \chi(\lambda x.t')r$ con t' a un paso de t. Entonces $|t| > |t'|$ y por segunda hipótesis inductiva $\chi(\lambda x.t')r \in [\![\tau]\!]_\alpha$.
- Reducción interna en r, $\chi(\lambda x.t)r \to_p \chi(\lambda x.t)r'$ con r' a un paso de r. Entonces $|r| > |r'|$ y por segunda hipótesis inductiva $\chi(\lambda x.t)r' \in [\![\tau]\!]_\alpha$.

Todas las reducciones pertenecen a $[\![\tau]\!]_\alpha$, entonces por CR3 $\chi(\lambda x.t) \in [\![\sigma \multimap \tau]\!]_\alpha$.

$\dfrac{\Gamma \vdash t : \sigma \multimap \tau \quad \Delta \vdash r : \sigma}{\Gamma, \Delta \vdash tr : \tau}$

Sean $\chi, \alpha \vDash \Gamma, \Delta$. Entonces $\chi, \alpha \vDash \Gamma$ y $\chi, \alpha \vDash \Delta$. Por HI, $\chi(t) \in [\![\sigma \multimap \tau]\!]_\alpha$ y $\chi(r) \in [\![\sigma]\!]_\alpha$. Además $\chi(tr) = \chi(t)\chi(r)$, con lo cual $\chi(tr) \in [\![\tau]\!]_\alpha$ por definición de $\to$.

$\dfrac{}{\Gamma \vdash \rho^n : n}$

$\chi(\rho^n) = \rho^n$. ρ^n está en forma normal, entonces $\rho^n \in \mathrm{SN}$. Luego, $\rho^n \in [\![n]\!]_\alpha$.

$\dfrac{\Gamma \vdash t : n}{\Gamma \vdash U^m t : n}$

Sean $\chi, \alpha \vDash \Gamma$. Por HI $\chi(t) \in [\![n]\!]_\alpha$. Entonces $\chi(t) \in \mathrm{SN}$. Como $\chi(U^m t) = U^m \chi(t)$ y, $\chi(t) \in \mathrm{SN}$ hay 2 posibilidades para reducir:

- Reducción a la cabeza, la cual produce una matriz de densidad ρ^n que está en forma normal.
- Reducción interna, hay una cantidad acotada de estas ya que $\chi(t) \in \mathrm{SN}$.

Por lo tanto, hay una cantidad acotada de reducciones para $\chi(U^m t)$. Entonces $\chi(U^m t) \in \mathrm{SN} = [\![n]\!]_\alpha$.

$\dfrac{\Gamma \vdash t : n}{\Gamma \vdash \pi^m t : (m, n)}$

Sean $\chi, \alpha \vDash \Gamma$. Por HI $\chi(t) \in [\![n]\!]_\alpha$. Entonces $\chi(t) \in \mathrm{SN}$. Como $\chi(\pi^m t) = \pi^m \chi(t)$ y, $\chi(t) \in \mathrm{SN}$ hay 2 posibilidades para reducir:

- Reducción a la cabeza, la cual produce un resulrado de medición (b^m, ρ^n) que está en forma normal.
- Reducción interna, hay una cantidad acotada de estas ya que $\chi(t) \in \mathrm{SN}$.

Por lo tanto, hay una cantidad acotada de reducciones para $\chi(\pi^m t)$. Entonces $\chi(\pi^m t) \in \mathrm{SN} = [\![(n, m)]\!]_\alpha$.

$$\frac{\Gamma \vdash t : n \quad \Delta \vdash r : m}{\Gamma, \Delta \vdash t \otimes r : n + m}$$

Sean $\chi, \alpha \vDash \Gamma, \Delta$. Entonces $\chi, \alpha \vDash \Gamma$ y $\chi, \alpha \vDash \Delta$. Por HI, $\chi(t) \in [\![n]\!]_\alpha$ y $\chi(r) \in [\![m]\!]_\alpha$. Por lo tanto $\chi(t)$ y $\chi(r) \in \mathrm{SN}$. Entonces $\chi(t \otimes r) = \chi(t) \otimes \chi(r) \in \mathrm{SN}$. Finalmente, $\chi(t \otimes r) \in \mathrm{SN} = [\![n + m]\!]_\alpha$.

$$\frac{}{\Gamma \vdash (b^m, \rho^n) : (m, n)}$$

$\chi((b^m, \rho^n)) = (b^m, \rho^n)$. (b^m, ρ^n) está en forma normal, entonces $(b^m, \rho^n) \in \mathrm{SN}$. Luego, $(b^m, \rho^n) \in [\![(m, n)]\!]_\alpha$.

$$\frac{\Delta, x : n \vdash t_0 : \sigma \quad \cdots \quad \Delta, x : n \vdash t_{2^m-1} : \sigma \quad \Gamma \vdash r : (m, n)}{\Gamma, \Delta \vdash \mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} : \sigma}$$

Sean $\chi, \alpha \vDash \Gamma, \Delta$, en particular $\chi, \alpha \vDash \Gamma$. Por HI, $\chi(r) \in [\![(m, n)]\!]_\alpha$ Luego, $\chi(r)$ pertenece a SN.

Si $\mathrm{Red}(\chi(\mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})) \subseteq [\![\sigma]\!]_\alpha$, dado que el término es neutral, por CR3 podemos concluir que $\chi(\mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}) \in [\![\sigma]\!]_\alpha$. Las siguientes son las reducciones posibles, razonando por inducción en $|\chi(r)|$. Notar que $\chi(\mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})) = \mathsf{letcase}\ x = \chi(r)\ \mathsf{in}\ \{\chi(t_0), \cdots, \chi(t_{2^m-1})\})$.

1. $\mathrm{Red}(\mathsf{letcase}\ x = r'\ \mathsf{in}\ \{\chi(t_0), \cdots, \chi(t_{2^m-1})\}))$. Donde $\chi(r) \to_p r'$. Dado que $|r'| < |\chi(r)|$, por la segunda HI, $\mathrm{Red}(\mathsf{letcase}\ x = r'\ \mathsf{in}\ \{\chi(t_0), \cdots, \chi(t_{2^m-1})\}) \in [\![\sigma]\!]_\alpha$
2. $\chi(r)$ está en forma normal (k, ρ^n_k) con $0 \le k \le 2^m - 1$. Entonces el término reduce a $\chi[\rho^n_k/x](t_k)$. Pero $\chi[\rho^n_k/x], \alpha \vDash \Delta, x : n$. Luego $\chi[\rho^n_k/x](t_k) \in [\![\sigma]\!]_\alpha$
3. $\chi(r)$ está en forma normal distinta de (k, ρ^n_k). En ese caso, el término entero está en forma normal y $\mathrm{Red}(\chi(\mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}))) = \varnothing \subseteq [\![\sigma]\!]_\alpha$.

Mostramos que $\mathrm{Red}(\chi(\mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, ..., t_{2^m-1}\})) \subseteq [\![\sigma]\!]_\alpha$. Por CR3, $\chi(\mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}) \in [\![\sigma]\!]_\alpha$

$$\frac{X \notin FV(\Gamma) \quad \Gamma \vdash t : \sigma}{\Gamma \vdash t : \forall X.\sigma}$$

Sean $\chi, \alpha \vDash \Gamma$, entonces como $X \notin \mathrm{FV}(\Gamma)$, tenemos que $\forall R \in \mathrm{CR}$, $\chi, (\alpha, X = R) \vDash \Gamma$. Por lo tanto por HI $\forall R \in \mathrm{CR}$, $\chi(t) \in [\![\sigma]\!]_{\alpha, X=R}$. Finalmente, $t \in \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha, X=R} = [\![\forall X.\sigma]\!]_\alpha$

$$\frac{\Gamma \vdash t : \forall X.\sigma}{\Gamma \vdash t : \sigma[\tau/X]}$$

Sean $\chi, \alpha \vDash \Gamma$, por HI, $\chi(t) \in [\![\forall X.\sigma]\!]_\alpha = \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha, X=R}$. En particular $t \in [\![\sigma]\!]_{\alpha, X=[\![\tau]\!]_\alpha}$. Por el lema 4.3.3, $t \in [\![\sigma[\tau/X]]\!]_\alpha$. □

La normalización fuerte de $\lambda_\rho 2$ es un corolario directo del lema anterior:

Teorema 4.3.5. *Todo término tipable en $\lambda_\rho 2$ es fuertemente normalizante.*

Demostración. Si un término t es tipable para un tipo σ en un contexto Γ, dado que la sustitución identidad y cualquier valuación α satisfacen trivialmente Γ, $t \in [\![\sigma]\!]_\alpha$. Por CR1, $[\![\sigma]\!]_\alpha \subseteq \mathrm{SN}$. Entonces $t \in \mathrm{SN}$. □

4.3.2. $\lambda_\rho^\circ 2$

Para el caso de $\lambda_\rho^\circ 2$ agregamos la siguiente condición sobre los candidatos de reducibilidad:

CR4: Si $t_i \in R$ y $\sum_i p_i = 1$, entonces $\sum_i p_i t_i \in R$.

Probamos los lemas de la sección anterior considerando esta nueva condición.

Lema 4.3.6. Para todo tipo σ, $[\![\sigma]\!]_\alpha \in \mathrm{CR}$.

Demostración. Probamos por inducción en σ. La única diferencia con el caso de λ_ρ es la adición de CR4:

- $[\![n]\!]_\alpha = [\![(m,n)]\!]_\alpha = \mathrm{SN}$.

  CR4: Sea $t = \sum_i p_i t_i$ con $\sum_i p_i = 1$ y $t_i \in \mathrm{SN}$. Hay 3 reducciones posibles para t:

  - $t \rightsquigarrow \rho$. Donde $\rho = \sum_i p_i t_i$. $\rho \in \mathrm{SN}$.
  - Si $\forall t_i,\ t_i = r,\ t \rightsquigarrow r$. Por hipótesis, $r \in \mathrm{SN}$.
  - $\sum_i p_i t_i \rightsquigarrow \sum_i p_i r_i$. Donde $t_j \rightsquigarrow r_j$ y $\forall i \neq j,\ t_i = r_i$; hay una cantidad finita de estas reducciones. Si hubiesen infinitas, existiría k tal que un subtérmino t_k tiene reducciones infinitas. Absurdo porque $\forall i,\ t_i \in \mathrm{SN}$.

  Como todas las reducciones de t tienen cadenas de reducción finitas, $t \in \mathrm{SN}$.

- $[\![\sigma \multimap \tau]\!]_\alpha = \{t \mid \forall v \in [\![\sigma]\!]_\alpha,\ tv \in [\![\tau]\!]_\alpha\}$.

  CR4: Sea $t = \sum_i p_i t_i$ con $\sum_i p_i = 1$ y $t_i \in [\![\sigma \multimap \tau]\!]_\alpha$. Sea $v \in [\![\sigma]\!]_\alpha$. Quiero probar que $tv \in [\![\tau]\!]_\alpha$. Como tv es un término neutral, basta ver que $\mathrm{Red}(tv) \subseteq [\![\tau]\!]_\alpha$ y concluir por CR3. Hay 3 reducciones posibles.

  - $(\sum_i p_i t_i)v \rightsquigarrow \sum_i p_i (t_i v)$. Como $t_i \in [\![\sigma \multimap \tau]\!]_\alpha$ y $v \in [\![\sigma]\!]_\alpha$, $t_i v \in [\![\tau]\!]_\alpha$. Por HI, $\sum_i p_i (t_i v) \in [\![\tau]\!]_\alpha$.
  - Como $v \in [\![\sigma]\!]_\alpha,\ v \in \mathrm{SN}$. Sea $|v|$ la máxima cantidad de pasos hasta llegar a forma normal. Entonces podemos razonar por inducción en $|v|$. Si $tv \rightsquigarrow tv'$ con $v \rightsquigarrow v'$, entonces $|v'| < |v|$. Por la segunda HI, $tv' \in [\![\tau]\!]_\alpha$.
  - Como $\forall i, t_i \in [\![\sigma \multimap \tau]\!]_\alpha,\ t_i \in \mathrm{SN}$ por CR1. Con el mismo razonamiento del punto anterior, se puede ver que $\sum_i p_i t_i \in \mathrm{SN}$. Si $\sum_i p_i t_i \rightsquigarrow \sum_i p_i r_i$. Donde $t_j \rightsquigarrow r_j$ y $\forall i \neq j,\ t_i = r_i$. De la misma manera que el caso de la reducción de v, podemos argumentar por inducción que $(\sum_i p_i r_i)v \in [\![\tau]\!]_\alpha$.

  Como $\mathrm{Red}(tv) \subseteq [\![\tau]\!]_\alpha\ \forall v \in [\![\sigma]\!]_\alpha$ y tv es un término neutral, por CR3 $\sum_i p_i t_i \in [\![\sigma \multimap \tau]\!]_\alpha$.

- $[\![X]\!]_\alpha = \alpha(X)$ y por definición $\alpha(X) \in \mathrm{CR}$.
- $[\![\forall X.\sigma]\!]_\alpha = \bigcap_{R \in \mathrm{CR}} [\![\sigma]\!]_{\alpha, X=R}$.

CR4: $\forall i,\ t_i \in [\![\forall X.\sigma]\!]_\alpha$. Eso implica que para todo $R \in \mathrm{CR},\ t_i \in [\![\sigma]\!]_{\alpha,X=R}$. Por HI, $\sum_i p_i t_i \in [\![\sigma]\!]_{\alpha,X=R},\ \forall R \in \mathrm{CR}$. Entonces, $\sum_i p_i t_i \in \bigcap_{R\in\mathrm{CR}} [\![\sigma]\!]_{\alpha,X=R}$. Luego, $\sum_i p_i t_i \in [\![\forall X.\sigma]\!]_\alpha$. □

La única diferencia restante con $\lambda_\rho 2$ se encuentra en el lema de adecuación. Los casos son los mismos salvando la ausencia del juicio $\mathrm{ax}_{\mathrm{am}}$ y la inclusión de la regla $(+)$.

Lema 4.3.7 (Adecuación)**.** Todo juicio de tipado es válido. Es decir, para todo contexto Γ, término t y tipo σ tales que $\Gamma \Vdash t : \sigma$, se tiene $\Gamma \vDash t : \sigma$.

Demostración. Probamos por inducción en el juicio de tipado. El único caso nuevo es la regla $(+)$.

$$\frac{\Gamma \Vdash t_i : \sigma \quad \sum_i p_i = 1}{\Gamma \Vdash \sum_i p_i t_i : \sigma}$$

$\chi(\sum_i p_i t_i) = \sum_i p_i \chi(t_i)$. Por HI, $\chi(t_i) \in [\![\sigma]\!]_\alpha$ y, además $\sum_i p_i = 1$. Por CR4, $\sum_i p_i \chi(t_i) \in [\![\sigma]\!]_\alpha$. Entonces $\chi(\sum_i p_i t_i) \in [\![\sigma]\!]_\alpha$. □

Teniendo el lema de adecuación nuevamente podemos probar la normalización fuerte de $\lambda^\circ_\rho 2$ como un corolario de este.

Teorema 4.3.8 (Normalización fuerte para $\lambda^\circ_\rho 2$)**.** *Todo término tipable en $\lambda^\circ_\rho 2$ es fuertemente normalizante.* □

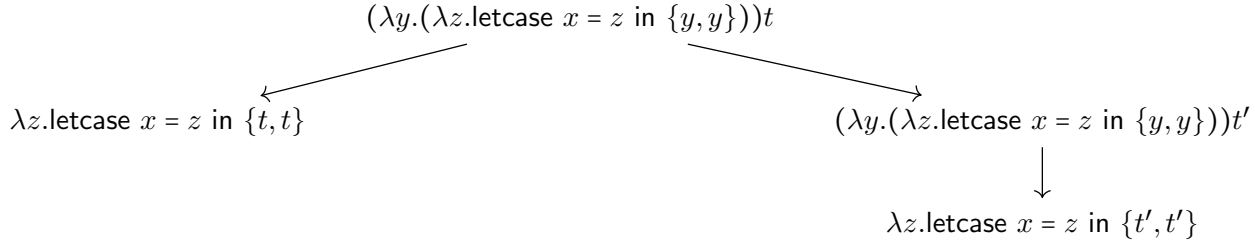
4.4. Confluencia

4.4.1. $\lambda^\circ_\rho 2$

Vamos a utilizar la misma estrategia que utilizamos con System F para demostrar la confluencia de $\lambda^\circ_\rho 2$. Analizar todos los pares críticos para ver que confluyen y probar WCR (ver definición 2.2.16). Luego, gracias al lema 2.2.17 y al hecho que demostramos normalización fuerte en la sección anterior, tenemos que el cálculo es confluente.

Weak Church-Rosser

Comenzamos con los lemas auxiliares que vamos a utilizar. Para demostrar estos lemas, es necesaria una regla auxiliar que reduzca dentro de las ramas del letcase. Usualmente, se evita esta clase de reducciones porque solo una de las ramas se conserva al final, el resto es trabajo de más. Sin embargo, sin esta regla el sistema es trivialmente no confluente. Por ejemplo:



Donde $t \rightsquigarrow t'$. Este contraejemplo es fácilmente salvable con la siguiente regla:

$$\frac{t_i \rightsquigarrow r_i}{\mathsf{letcase}^\circ\ x = s\ \mathsf{in}\ \{t_0, \cdots, t_i, \cdots, t_{2^m-1}\} \rightsquigarrow \mathsf{letcase}^\circ\ x = s\ \mathsf{in}\ \{t_0, \cdots, r_i, \cdots, t_{2^m-1}\}}\ \text{inner letcase aux}$$

Partimos por uno de los lemas clásicos de sustitución:

Lema 4.4.1 (Sustitución)**.** Si $y \notin \mathrm{FV}(r)$, entonces $t[q/y][r/x] = t[r/x][q[r/x]/y]$.

Demostración. Por inducción en t:

***t* = *x*:** Se tiene que:

$$x[q/y][r/x] = x[r/x] = r.$$

Por otro lado:

$$x[r/x][q[r/x]/y] = r[q[r/x]/y] = r \text{ porque } y \notin \mathrm{FV}(r).$$

t* = *y *con* $y \neq x$*:* Por un lado:

$$y[q/y][r/x] = q[r/x].$$

Además,

$$y[r/x][q[r/x]/y] = y[q[r/x]/y] = q[r/x].$$

***t* = *z*:** Con $z \neq x$ y $z \neq y$. Primero, se tiene que:

$$z[q/y][r/x] = z.$$

Por otro lado,

$$z[r/x][q[r/x]/y] = z.$$

***t* = *λz.s*:** $z \neq x$ y $z \neq y$

$$\begin{aligned}(\lambda z.s)[q/y][r/x] &= (\lambda z.s[q/y][r/x]) \text{ Por convención de variables } z \notin \mathrm{FV}(r) \cup \mathrm{FV}(q)\\ &=^{\mathrm{HI}} (\lambda z.s[r/x][q[r/x]/y])\\ &= (\lambda z.s)[r/x][q[r/x]/y] \text{ Porque } z \notin \mathrm{FV}(r) \cup \mathrm{FV}(q).\end{aligned}$$

t* = *s*₁*s*₂*: Se tiene que:

$$(s_1 s_2)[q/y][r/x] = s_1[q/y][r/x]s_2[q/y][r/x].$$

Por hipótesis inductiva, el término es igual a:

$$s_1[r/x][q[r/x]/y]s_2[r/x][q[r/x]/y] = (s_1 s_2)[r/x][q[r/x]/y].$$

t* = *ρ*ⁿ*: Primero, se tiene que:

$$\rho^n[q/y][r/x] = \rho^n.$$

Por otro lado,

$$\rho^n[r/x][q[r/x]/y] = \rho^n.$$

$\boldsymbol{t = U^n s}$: Se tiene:

$$(U^n s)[q/y][r/x] = U^n s[q/y][r/x].$$

Por hipótesis inductiva, es igual a:

$$U^n s[r/x][q[r/x]/y] = (U^n s)[r/x][q[r/x]/y].$$

$\boldsymbol{t = \pi^n s}$: Se tiene:

$$(\pi^n s)[q/y][r/x] = \pi^n s[q/y][r/x].$$

Por hipótesis inductiva, es igual a:

$$\pi^n s[r/x][q[r/x]/y] = (\pi^n s)[r/x][q[r/x]/y].$$

$\boldsymbol{t = s_1 \otimes s_2}$: Se tiene que:

$$(s_1 \otimes s_2)[q/y][r/x] = s_1[q/y][r/x] \otimes s_2[q/y][r/x].$$

Por hipótesis inductiva, el término es igual a:

$$s_1[r/x][q[r/x]/y] \otimes s_2[r/x][q[r/x]/y] = (s_1 \otimes s_2)[r/x][q[r/x]/y].$$

$\boldsymbol{t = \sum_i p_i s_i}$: Se tiene:

$$(\sum_i p_i s_i)[q/y][r/x] = \sum_i p_i s_i[q/y][r/x].$$

Por hipótesis inductiva, es igual a:

$$\sum_i p_i s_i[r/x][q[r/x]/y] = (\sum_i p_i s_i)[r/x][q[r/x]/y].$$

$\boldsymbol{t = \mathsf{letcase}^\circ\ z = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}}$

$(\mathsf{letcase}^\circ\ z = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[q/y][r/x] =$

$(\mathsf{letcase}^\circ\ z = s[q/y][r/x]\ \mathsf{in}\ \{t_0[q/y][r/x], \cdots, t_{2^m-1}[q/y][r/x]\}.$

Por convención de variables $z \notin \mathrm{FV}(r) \cup \mathrm{FV}(q)$.

$=^{\mathrm{HI}} (\mathsf{letcase}^\circ\ z = s[r/x][q[r/x]]\ \mathsf{in}\ \{t_0[r/x][q[r/x]], \cdots, t_{2^m-1}[r/x][q[r/x]]\}$

$= (\mathsf{letcase}^\circ\ z = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x][q[r/x]/y]$ Porque $z \notin \mathrm{FV}(r) \cup \mathrm{FV}(q)$. □

Utilizamos los siguientes lemas para probar que la sustitución se comporta de manera esperada junto a la reducción.

Lema 4.4.2. Si $t \rightsquigarrow t'$, entonces $t[r/x] \rightsquigarrow t'[r/x]$.

Demostración. Inducción sobre t.

$\boldsymbol{t = \lambda y.s}$: con $y \neq x$ y $y \notin \mathrm{FV}(r)$

$\lambda y.s \rightsquigarrow \lambda y.s'$. Entonces quiero probar que $(\lambda y.s)[r/x] \rightsquigarrow (\lambda y.s')[r/x]$.

$(\lambda y.s)[r/x] = \lambda y.s[r/x] \rightsquigarrow^{\mathrm{HI}} \lambda y.s'[r/x] = (\lambda y.s')[r/x]$.

$t = s_1 s_2$: Hay dos casos: Reducción en la raíz y reducción interna.

- Hay dos casos posibles para reducción a la raíz:
  - $s_1 = (\lambda y.q)$ y $t' = p[s_2/y]$ con $y \neq x$ y $y \notin \mathrm{FV}(r)$.

    $$\begin{aligned} t[r/x] &= ((\lambda y.q)s_2)[r/x] \\ &= (\lambda y.q[r/x])s_2[r/x] \\ &\rightsquigarrow q[r/x][s_2[r/x]/y] \text{ por lema 4.4.1} \\ &= q[s_2/y][r/x] \quad y \notin \mathrm{FV}(r) \text{ por convención de variables.} \end{aligned}$$

  - $s_1 = (\sum_i p_i s_i)s_2$ y $t' = \sum_i p_i(s_i s_2)$.

    $$\begin{aligned} ((\sum_i p_i s_i)s_2)[r/x] &= (\sum_i p_i s_i[r/x])s_2[r/x] \\ &\rightsquigarrow \sum_i p_i(s_i[r/x]s_2[r/x]) \\ &= (\sum_i p_i(s_i s_2))[r/x]. \end{aligned}$$

- Reducción interna: $s_1 s_2 \rightsquigarrow s_1' s_2$ con $s_1 \rightsquigarrow s_1'$.

  $(s_1 s_2)[r/x] = s_1[r/x]s_2[r/x] \rightsquigarrow^{\mathrm{HI}} s_1'[r/x]s_2[r/x] = (s_1' s_2)[r/x]$.

  Similar para el caso simétrico.

$t = U^n s$: hay 2 casos para considerar:

- Si $s = \rho$, entonces $U^n\rho[r/x] = U^n\rho \rightsquigarrow \rho' = \rho'[r/x]$.
- Si $s \rightsquigarrow s'$, $(U^n s)[r/x] = U^n s[r/x] \rightsquigarrow^{\mathrm{HI}} U^n s'[r/x] = (U^n s')[r/x]$.

$t = \pi^n s$: con $s \rightsquigarrow s'$ es similar al caso de $U^n s$.

$t = s_1 \otimes s_2$: Hay dos casos: Reducción a la raíz y reducción interna.

- Reducción en la raíz. $s_1 = \rho_1$ y $s_2 = \rho_2$ y $t' = \rho'$ con $\rho' = \rho_1 \otimes \rho_2$.

  $(\rho_1 \otimes \rho_2)[r/x] = \rho_1 \otimes \rho_2 \rightsquigarrow \rho' = \rho'[r/x]$.

- Reducción interna. $s_1 \otimes s_2 \rightsquigarrow s_1' \otimes s_2$ con $s_1 \rightsquigarrow s_1'$.

  $(s_1 \otimes s_2)[r/x] = s_1[r/x] \otimes s_2[r/x] \rightsquigarrow^{\mathrm{HI}} s_1'[r/x] \otimes s_2[r/x] = (s_1' \otimes s_2)[r/x]$. Similar para el caso simétrico.

$t = \sum_i p_i t_i$: Hay dos casos reducción a la raíz y reducción interna.

- Hay dos posibles reducciones a la raíz:
  - $t = \sum_i p_i s$ y $t' = s$.

    $(\sum_i p_i s)[r/x] = \sum_i p_i s[r/x] \rightsquigarrow s[r/x]$.

  - $t = \sum_i p_i \rho_i$ y $t' = \rho'$

    $(\sum_i p_i \rho_i)[r/x] = \sum_i p_i \rho_i[r/x] = \sum_i p_i \rho_i \rightsquigarrow \rho' = \rho'[r/x]$.

- Reducción interna. $t = \sum_i p_i s_i$ y $t' = \sum_i p_i s'_i$ con $\forall i \neq j,\ s_i = s'_i$ y $s_j \rightsquigarrow s'_j$.

  $(\sum_i p_i s_i)[r/x] = \sum_i p_i s_i[r/x] \rightsquigarrow^{\text{HI}} \sum_i p_i s'_i[r/x] = (\sum_i p_i s'_i)[r/x]$.

$t = \mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$: con $y \neq x$ y $y \notin \mathrm{FV}(r)$. Hay 2 casos: Reducción en la raíz e interna:

- Reducción en la raíz. $t = \mathsf{letcase}^\circ\ y = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ y $t' = \sum_i p_i t_i[\rho_i^n/y]$.

  $$\begin{aligned} t[r/x] &= (\mathsf{letcase}^\circ\ y = \pi^m\rho^n\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x] \\ &= \mathsf{letcase}^\circ\ y = \pi^m\rho^n\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\} \\ &\rightsquigarrow \sum_i p_i(t_i[r/x][\rho_i^n/y]) \\ &= \sum_i p_i(t_i[\rho_i^n/y][r[\rho^n/y]/x]) \text{ Por lema 4.4.1} \\ &= \sum_i p_i(t_i[\rho_i^n/y][r/x]) \ y \notin \mathrm{FV}(r) \text{ por convención de variables} \\ &= (\sum_i p_i t_i[\rho_i^n/y])[r/x]. \end{aligned}$$

- Reducción interna. $t = \mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ y $t' = \mathsf{letcase}^\circ\ y = s'\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ con $s \rightsquigarrow s'$.

  $$\begin{aligned} t[r/x] &= (\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x] \\ &= \mathsf{letcase}^\circ\ y = s[r/x]\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\} \\ &\rightsquigarrow^{\text{HI}} \mathsf{letcase}^\circ\ y = s'[r/x]\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\} \\ &= (\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x]. \end{aligned}$$

  Similar para el caso donde se reduce una de las ramas del letcase. □

El siguiente lema a demostrar asegura que la reducción es consistente con la sustitución.

Lema 4.4.3. Si $r \rightsquigarrow r'$, entonces $t[r/x] \rightsquigarrow\!\!\!\!\rightarrow t[r'/x]$.

Demostración. Demostramos por induccion en t:

$t = y$: Hay dos casos posibles:

- $y = x$ en cuyo caso: $x[r/x] = r \rightsquigarrow r' = x[r'/x]$.
- $y \neq x$, entonces $y[r/x] = y = y[r'/x]$.

$t = \lambda y.s$: con $y \neq x$ y $y \notin \mathrm{FV}(r)$. Como la reducción no introduce variables libres, $y \notin \mathrm{FV}(r) \implies y \notin \mathrm{FV}(r')$

$$\begin{aligned} (\lambda y.s)[r/x] &= \lambda y.s[r/x] \\ &\rightsquigarrow\!\!\!\!\rightarrow \lambda y.s[r'/x] \text{ Por HI} \\ &= (\lambda y.s)[r'/x]. \end{aligned}$$

$t = s_1 s_2$:

$$\begin{aligned} (s_1 s_2)[r/x] &= s_1[r/x]s_2[r/x] \\ &\rightsquigarrow\!\!\!\!\rightarrow s_1[r'/x]s_2[r'/x] \text{ Por HI} \\ &= (s_1 s_2)[r'/x]. \end{aligned}$$

$\boldsymbol{t = \rho^n}$: $\rho^n[r/x] = \rho^n = \rho^n[r'/x]$

$\boldsymbol{t = U^n s}$:

$$\begin{aligned}(U^n s)[r/x] &= U^n s[r/x] \\ &\twoheadrightsquigarrow U^n s[r'/x] \text{ Por HI} \\ &= (U^n s)[r'/x].\end{aligned}$$

$\boldsymbol{t = \pi^n s}$:

$$\begin{aligned}(\pi^n s)[r/x] &= \pi^n s[r/x] \\ &\twoheadrightsquigarrow \pi^n s[r'/x] \text{ Por HI} \\ &= (\pi^n s)[r'/x].\end{aligned}$$

$\boldsymbol{t = s_1 \otimes s_2}$:

$$\begin{aligned}(s_1 \otimes s_2)[r/x] &= s_1[r/x] \otimes s_2[r/x] \\ &\twoheadrightsquigarrow s_1[r'/x] \otimes s_2[r'/x] \text{ Por HI} \\ &= (s_1 \otimes s_2)[r'/x].\end{aligned}$$

$\boldsymbol{t = \sum_i p_i s_i}$:

$$\begin{aligned}(\sum_i p_i s_i)[r/x] &= \sum_i p_i s_i[r/x] \\ &\twoheadrightsquigarrow \sum_i p_i s_i[r'/x] \text{Por HI} \\ &= (\sum_i p_i s_i)[r'/x].\end{aligned}$$

$\boldsymbol{t = \mathsf{letcase}^\circ\ z = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}}$: con $y \neq x$ y $y \notin \mathrm{FV}(r)$. Como la reducción no introduce variables libres, $y \notin \mathrm{FV}(r) \implies y \notin \mathrm{FV}(r')$

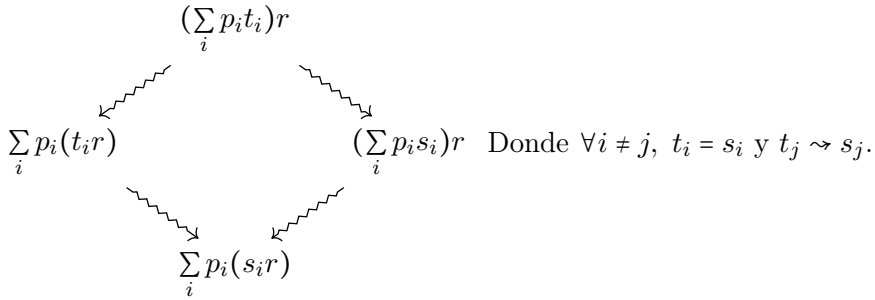
$$\begin{aligned}(\mathsf{letcase}^\circ\ z = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x] &= \mathsf{letcase}^\circ\ z = s[r/x]\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\} \\ &\twoheadrightsquigarrow \mathsf{letcase}^\circ\ z = s[r'/x]\ \mathsf{in}\ \{t_0[r'/x], \cdots, t_{2^m-1}[r'/x]\} \text{ Por HI} \\ &= \mathsf{letcase}^\circ\ z = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r'/x].\end{aligned}$$

En este caso, utilizamos la regla auxiliar en el paso inductivo. De esa forma, podemos reducir dentro de las ramas del letcase.

□

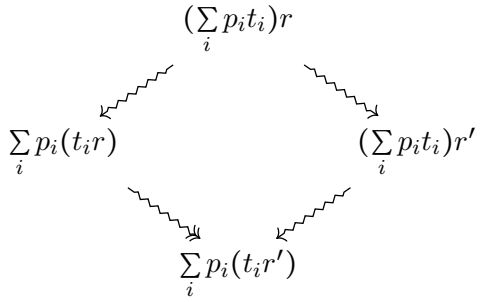
Teorema 4.4.4. *$\lambda^\circ_\rho 2$ es WCR.*

Demostración. La demostración pasa por analizar los pares críticos de $\lambda^\circ_\rho 2$ y mostrar que son confluentes. Luego por el lema 2.2.18, tenemos que el cálculo es WCR.

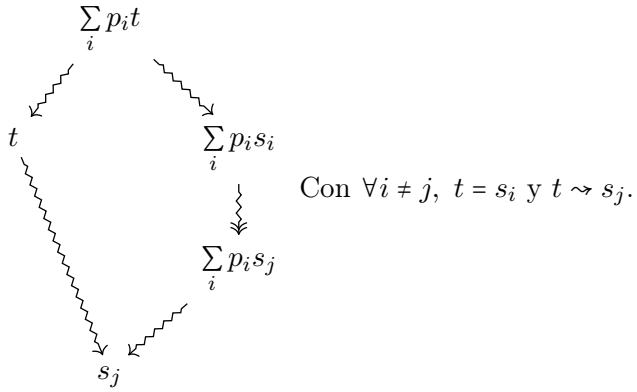


Donde $\forall i \neq j,\ t_i = s_i$ y $t_j \rightsquigarrow s_j$.

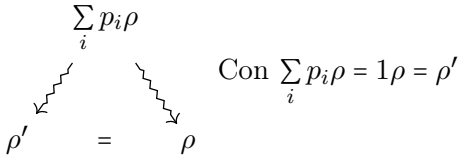
Por la rama izquierda, se cierra el diagrama reduciendo dentro de la aplicación interna $t_j \rightsquigarrow s_j$. Por la derecha, distribuyendo r sobre la sumatoria.



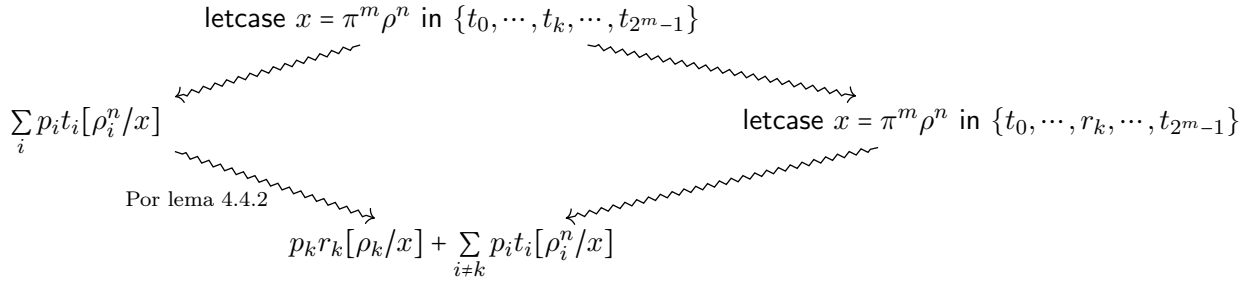
Por la rama izquierda, se cierra el diagrama reduciendo r en cada término de la sumatoria. Por la derecha, distribuyendo r' sobre la sumatoria.



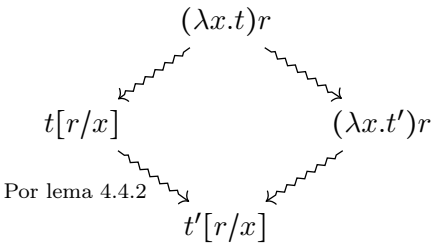
Por la rama izquierda, se cierra el diagrama reduciendo t. Por la derecha, reduciendo t en cada subtérmino y luego simplificando la sumatoria.



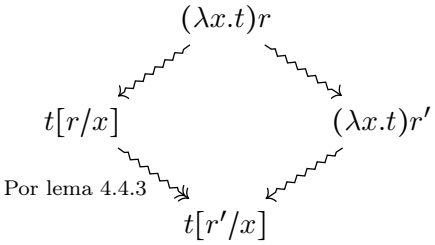
En este caso, ambas reducciones derivan en la misma matriz de densidad.



La rama izquierda de este par cierra usando el lema 4.4.2. La derecha mediante una reducción a la cabeza del letcase.



La rama izquierda de este par cierra usando el lema 4.4.2. La derecha mediante una β-reducción.



La rama izquierda de este par cierra usando el lema 4.4.3. La derecha mediante una β-reducción. Finalmente probamos que todos los pares críticos son confluentes. □

Dado que todos los pares críticos confluyen, podemos afirmar que $\lambda_\rho^\circ 2$ es localmente confluente. Para conseguir la confluencia global, tan solo hay que considerar la regla auxiliar del letcase agregada en las demostraciones de normalización fuerte.

4.4.2. $\lambda_\rho 2$

Introducción

Para analizar el caso de confluencia de $\lambda_\rho 2$, utilizamos los modelos definidos en la sección 2.3 de este trabajo, Los PARS y su determinización. Mapeamos cada regla de reducción a su correspondiente regla en el PARS. Queda entonces definido de esta manera:

$$\frac{}{(\lambda x.t)r \mapsto [(1, t[r/x])]} \text{ PARS } \beta \qquad \frac{\rho'^n = \overline{U^m}\rho^n\overline{U^m}^\dagger}{U^m\rho^n \mapsto [(1,\rho'^n)]} \text{ PARS U} \qquad \frac{p_i = \mathsf{tr}(\overline{\pi_i}^\dagger\overline{\pi_i}\rho^n) \quad \rho_i'^n = \frac{\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger}{p_i}}{\pi^m\rho^n \mapsto [(p_i,\rho_i'^n)]_i} \text{ PARS } \pi$$

$$\frac{\rho' = \rho_1 \otimes \rho_2}{\rho_1 \otimes \rho_2 \mapsto [(1,\rho')]_i} \text{ PARS } \otimes \qquad \frac{t \mapsto [(p_i, r_i)]_i}{\lambda x.t \mapsto [(p_i, \lambda x.r_i)]_i} \text{ PARS inner } \lambda$$

$$\frac{}{\mathsf{letcase}\ y = (b^m, \rho^n)\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} \mapsto [(1, t_{b^m}[\rho^n/x])]} \text{ PARS letcase}$$

$$\frac{t \mapsto [(p_i, r_i)]_i}{ts \mapsto [(p_i, r_i s)]_i} \text{ PARS left app} \qquad \frac{t \mapsto [(p_i, r_i)]_i}{st \mapsto [(p_i, s r_i)]_i} \text{ PARS right app}$$

$$\frac{t \mapsto [(p_i, r_i)]_i}{U^n t \mapsto [(p_i, U^n r_i)]_i} \text{ PARS inner U} \qquad \frac{t \mapsto [(p_i, r_i)]_i}{\pi^n t \mapsto [(p_i, \pi^n r_i)]_i} \text{ PARS inner } \pi$$

$$\frac{t \mapsto [(p_i, r_i)]_i}{t \otimes s \mapsto [(p_i, r_i \otimes s)]_i} \text{ PARS } \otimes \text{ left} \qquad \frac{t \mapsto [(p_i, r_i)]_i}{s \otimes t \mapsto [(p_i, s \otimes r_i)]_i} \text{ PARS } \otimes \text{ right}$$

$$\frac{t \mapsto [(p_i, r_i)]_i}{\mathsf{letcase}\ x = t\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} \mapsto [(p_i, \mathsf{letcase}\ x = r_i\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})]_i} \text{ PARS inner letcase}$$

Lo primero a tener en cuenta es que el cálculo $\lambda_\rho 2$ no es probabilísticamente confluente. Tomamos por ejemplo el término cerrado: $(\lambda y.(\lambda z.\mathsf{letcase}\ x = z\ \mathsf{in}\ \{y, y\}))(\pi^1|+\rangle\langle+|)$. Este término tiene 2 posibles reducciones.

$$(\lambda y.(\lambda z.\mathsf{letcase}\ x = z\ \mathsf{in}\ \{y, y\}))(\pi^1|+\rangle\langle+|)$$

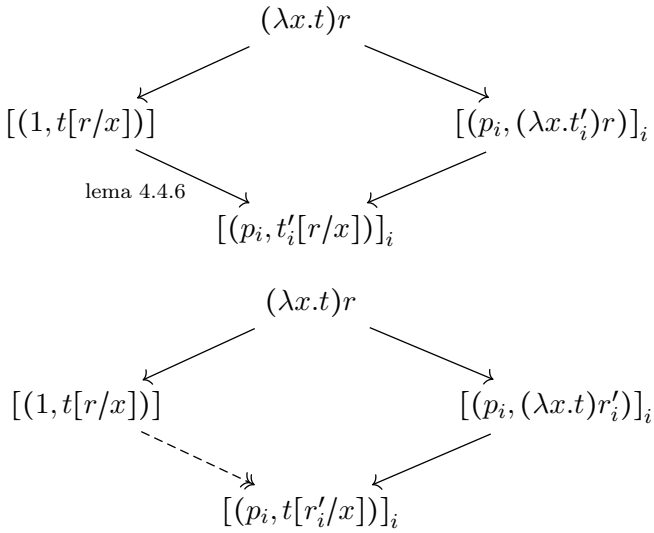
$$\big[(1, \lambda z.\mathsf{letcase}\ x = z\ \mathsf{in}\ \{\pi^1|+\rangle\langle+|, \pi^1|+\rangle\langle+|\}\big] \qquad \left[\begin{array}{l}(1/2, (\lambda y.\lambda z.\mathsf{letcase}\ x = z\ \mathsf{in}\ \{y, y\})|0\rangle\langle 0|, \\ (1/2, (\lambda y.\lambda z.\mathsf{letcase}\ x = z\ \mathsf{in}\ \{y, y\})|1\rangle\langle 1|\end{array}\right]$$

$$\left[\begin{array}{l}(1/2, \lambda z.\mathsf{letcase}\ x = z\ \mathsf{in}\ \{|0\rangle\langle 0|, |0\rangle\langle 0|\}), \\ (1/2, \lambda z.\mathsf{letcase}\ x = z\ \mathsf{in}\ \{|1\rangle\langle 1|, |1\rangle\langle 1|\})\end{array}\right]$$

Estos PARS son irreconciliables dado que no podemos efectuar reducciones sobre las ramas del letcase. Es decir, no es posible reducir la medición en la rama de la izquierda. Incluso agregando una regla auxiliar que permita reducir los términos internos del letcase análoga al inner letcase aux introducida en la sección anterior, no hay forma de cerrar el diagrama. Esto es porque en la rama izquierda daría lugar a términos como $(\lambda z.\mathsf{letcase}\ x = z\ \mathsf{in}\ \{|0\rangle\langle 0|, |1\rangle\langle 1|\})$ que no pueden aparecer en la rama derecha.

Para llegar a la confluencia sobre λ_ρ, vamos a considerar tres enfoques distintos.

Primero observamos que en el cálculo hay dos pares críticos:



Es posible demostrar que el primer par crítico converge. Los tres enfoques distintos difieren en como lidian con el segundo par.

En primer lugar buscamos demostrar el lema que nos permite cerrar el primer par, para eso definimos la siguiente notación. Para una distribución $D = [(p_i, s_i)]_i$, término t y variable x, notamos $D[t/x] = [(p_i, s_i[t/x])]_i$. De la misma manera, notamos $t[D/x] = [(p_i, t[s_i/x])]_i$. Luego, probamos el lema auxiliar de sustitución presentado en la sección anterior.

Lema 4.4.5 (Sustitución)**.** Si $y \notin \mathrm{FV}(r)$, entonces $t[q/y][r/x] = t[r/x][q[r/x]/y]$.

Demostración. Por inducción en t, el único caso no contemplado en $\lambda^\circ_\rho 2$ es el del resultado de la medición:

$$(b^m, \rho^n)[q/y][r/x] = (b^m, \rho^n) = (b^m, \rho^n)[r/x][q[r/x]/y]$$

□

Con ese lema auxiliar, es posible demostrar que el primer par crítico cierra.

Lema 4.4.6. Si $t \mapsto D$ entonces $t[r/x] \mapsto D[r/x]$.

Demostración. Demostración por inducción en t:

***t* = *λy.s*:** con $y \neq x$, $y \notin \mathrm{FV}(r)$ y $s \mapsto [(p_i, s_i)]_i$.

$(\lambda y.s)[r/x] = \lambda y.s[r/x]$.

Por HI $s[r/x] \mapsto [(p_i, s_i[r/x])]_i$. Por lo tanto por regla PARS inner λ,

$$\lambda y.s[r/x] \mapsto [(p_i, \lambda y.s_i[r/x])]_i = [(p_i, (\lambda y.s_i)[r/x])]_i .$$

***t* = *t*₁*t*₂:** Hay dos casos posibles:

- Reducción en la raíz: $t_1 = \lambda y.s$ y $D = [(1, r[t_2/y])]$. Con $y \neq x$, $y \notin \mathrm{FV}(r)$
  $t[r/x] = ((\lambda y.s)t_2)[r/x]$
  $= (\lambda y.s[r/x])t_2[r/x]$ Por convención de variables.
  $\mapsto [(1, s[r/x][t_2[r/x]/y])]$
  $= [(1, s[t_2/y][r/x])]$ Por lema 4.4.5.
- Reducción interna: $t_1 t_2 \mapsto [(p_i, s_i t_2)]_i$ con $t_1 \mapsto [(p_i, s_i)]_i$.
  $t[r/x] = t_1[r/x]t_2[r/x]$.

  Por HI $t_1[r/x] \mapsto [(p_i, s_i[r/x])]_i$. Por lo tanto por regla PARS left app,

  $$t_1[r/x]t_2[r/x] \mapsto [(p_i, s_i[r/x]t_2[r/x])]_i = [(p_i, (s_i t_2)[r/x])]_i .$$

  Análogo para $t_1 t_2 \mapsto [(p_i, t_1 s_i)]_i$ cont$t_2 \mapsto [(p_i, s_i)]_i$.

***t* = $U^n s$:** Hay dos casos posibles:

- Reducción en la raíz: $t = U^m \rho^n \mapsto [(1, \rho'^n)]$.
  $t[r/x] = U^m \rho^n [r/x]$
  $= U^m \rho^n$
  $\mapsto \left[(1, \rho'^n)\right]$
  $= \left[(1, \rho'^n [r/x])\right]$.
- Reducción interna: $U^n s \mapsto [(p_i, U^n s_i)]_i$ con $s \mapsto [(p_i, s_i)]_i$.
  $(U^m s)[r/x] = U^m s[r/x]$.

  Por HI $s[r/x] \mapsto [(p_i, s_i[r/x])]_i$. Por lo tanto por regla PARS inner U,

  $$U^m s[r/x] \mapsto [(p_i, U^m s_i[r/x])]_i = [(p_i, (U^m s_i)[r/x])]_i .$$

***t* = $\pi^n s$:** Hay dos casos posibles:

- Reducción en la raíz: $t = \pi^m \rho^n \mapsto [(p_i, \rho_i'^n)]_i$.
  $t[r/x] = \pi^m \rho^n [r/x]$
  $= \pi^m \rho^n$
  $\mapsto \left[(p_i, \rho'^n)\right]_i$
  $= \left[(p_i, \rho'^n [r/x])\right]_i$.
- Reducción interna: $\pi^m s \mapsto [(p_i, \pi^m s_i)]_i$ con $s \mapsto [(p_i, s_i)]_i$.
  $t[r/x] = \pi^m s[r/x]$.

  Por HI $s[r/x] \mapsto [(p_i, s_i[r/x])]_i$. Por lo tanto por regla PARS inner π,

  $$\pi^m s[r/x] \mapsto [(p_i, \pi^m s_i[r/x])]_i = [(p_i, (\pi^m s_i)[r/x])]_i .$$

***t* = $t_1 \otimes t_2$:** Hay dos casos posibles:

- Reducción en la raíz: $t = \rho_1 \otimes \rho_2 \mapsto [(1, \rho')]$.
  $t[r/x] = (\rho_1 \otimes \rho_2)[r/x]$
  $= \rho_1 \otimes \rho_2$
  $\mapsto \left[(1, \rho')\right]$
  $\mapsto \left[(1, \rho'[r/x])\right]$.
- Reducción interna: $t_1 \otimes t_2 \mapsto [(p_i, s_i \otimes t_2)]_i$ con $t_1 \mapsto [(p_i, s_i)]_i$.
  $t[r/x] = t_1[r/x] \otimes t_2[r/x]$.

  Por HI $t_1[r/x] \mapsto [(p_i, s_i[r/x])]_i$. Por lo tanto por regla PARS $\otimes$ left,

  $t_1[r/x] \otimes t_2[r/x] \mapsto [(p_i, s_i[r/x] \otimes t_2[r/x])]_i$
  $= [(p_i, (s_i \otimes t_2)[r/x])]_i$.

  Análogo para $t_1 \otimes t_2 \mapsto [(p_i, t_1 \otimes s_i)]_i$ con $t_2 \mapsto [(p_i, s_i)]_i$.

$t = \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$: Con $y \neq x$ y $y \notin \mathrm{FV}(r)$, hay dos casos posibles:

- Reducción en la raíz: $t = \mathsf{letcase}\ y = (b^m, \rho^n)\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$ y $D = [(1, t_{b^m}[\rho^n/y])]$.
  $t[r/x] = (\mathsf{letcase}\ y = (b^m, \rho^n)\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x]$
  $= \mathsf{letcase}\ y = (b^m, \rho^n)[r/x]\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\}$
  $= \mathsf{letcase}\ y = (b^m, \rho^n)\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\}$
  $\mapsto [(1, t_{b^m}[r/x][\rho^n/y])]$
  $= [(1, t_{b^m}[\rho^n/y][r/x])]$. Por lema 4.4.5
- Reducción interna: $t = \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} \mapsto [(p_i, \mathsf{letcase}\ y = s'\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}]$ con $s \mapsto [(p_i, s_i)]_i$.
  $t[r/x] = \mathsf{letcase}\ y = s[r/x]\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\}$.

  Por HI $s[r/x] \mapsto [(p_i, s_i[r/x])]_i$. Por lo tanto por regla PARS inner letcase,
  $\mathsf{letcase}\ y = s[r/x]\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\}$
  $\mapsto [(p_i, \mathsf{letcase}\ y = s_i[r/x]\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\})]_i$
  $= [(p_i, (\mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x])]_i$.

□

A continuación describimos distintas opciones para lograr la confluencia del cálculo λ_ρ. El problema surge al combinar reducciones probabilísticas, una falta de estrategia de reducción y variables con más de una aparición como es el caso en distintas ramas del letcase.

Para mitigar esto, podemos probar eliminando uno de los elementos y mantener los otros dos. Si tomamos reducciones no probabilísticas, llegamos al cálculo $\lambda_\rho^\circ 2$ que ya probamos que es confluente. Las otras dos opciones involucran definir una estrategia de reducción o volver a restringir los contextos para las distintas ramas del letcase como en su presentación original.

Estrategia de reducción *Call-by-base* (CBB)

Podemos modificar la regla de β-reducción de la siguiente manera:

$$(\lambda x.t)v \to_1 t[v/x]$$

donde v está en forma normal.

De esta forma, dado que no existe v' tal que $v \to_p v'$, no es posible construir el segundo par crítico. En ese caso, las únicas reducciones posibles son la β-reducción y la reducción interna dentro del λ. Este par crítico es el del primer caso y ya queda demostrado que es confluente. La desventaja radica en que restringimos las reducciones y siempre es necesario reducir el argumento de un λ, se use o no.

Forzar afinidad

La segunda estrategia consiste en modificar el tipado del letcase para no permitir que se repita una variable en distintas ramas. Logramos esta condición poniendo restricciones sobre los contextos. La regla de tipado queda de esta manera:

$$\frac{\Delta_0, x : n \vdash t_0 : \sigma \ , \cdots, \ \Delta_{2^m-1}, x : n \vdash t_{2^m-1} : \sigma \ \Gamma \vdash r : (m, n)}{\Delta_0, \cdots, \Delta_{2^m-1}, \Gamma \vdash \text{letcase } x = r \text{ in } \{t_0, \cdots, t_{2^m-1}\} : \sigma}$$

De esta forma logramos un cálculo afín, donde cada variable aparece a lo sumo una vez. Bajo esta condición es posible demostrar que el segundo par crítico converge, y la regla sigue siendo más permisiva que en su versión original.

Lo último que queda para cerrar la demostración de confluencia probabilística es agregar una regla auxiliar al cálculo para reducir las expresiones dentro del letcase. Junto a esa regla, agregamos su correspondiente regla del PARS. Usualmente, no se suele tener en cuenta reducciones dentro de las ramas de los condicionales para evitar reducciones superfluas en ramas que se descartan. En este caso, las consideramos para completar la demostración. Las reglas auxiliares son:

$$\frac{t_j \to_{p_j} r_j}{\mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, t_i, \cdots t_{2^m-1}\} \to_p \mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, r_i, \cdots, t_{2^m-1}\})} \text{ aux letcase}$$

$$\frac{t_j \mapsto [(p_{ji}, r_{ji})]_i}{\mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, t_j, \cdots, t_{2^m-1}\} \mapsto [(p_{ji}, \mathsf{letcase}\ x = s\ \mathsf{in}\ \{t_0, \cdots, r_{ji}, \cdots, t_{2^m-1}\})]_i} \text{ PARS aux letcase}$$

Finalmente definimos una extensión para la relación $\mapsto$ sobre la cual se basa la demostración. La relación $\mapsto$ toma un término t y devuelve la distribución de términos a los que reduce. Sin embargo, hay puntos para los cuales queremos obtener una distribución de Dirac sin necesariamente reducirlos. Con ese fin definimos $\mapsto_0$ de la siguiente manera:

$$\frac{t \mapsto D}{t \mapsto_0 D} \qquad \frac{}{t \mapsto_0 [(1, t)]}$$

Es fácil ver que $\mapsto \subset \mapsto_0$. Con esta relación y la regla auxiliar, están todas las piezas para demostrar el lema que cierra el segundo par crítico.

Lema 4.4.7. Si $r \mapsto D$ y $\Gamma \vdash t : \sigma$ entonces $t[r/x] \mapsto_0 t[D/x]$.

Demostración. Inducción sobre t. Asumimos que $r \mapsto [(p_i, r_i)]_i$.

***t* = *z*:** Hay dos casos.

- $z = x$.
  $$\begin{aligned} x[r/x] &= r \\ &\mapsto [(p_i, r_i)]_i \\ &= [(p_i, x[r_i/x])]_i . \end{aligned}$$
- $z \neq x$.
  $$\begin{aligned} z[r/x] &= z \\ &\mapsto_0 [(1, z)] \\ &\approx [(p_i, z])]_i \\ &= [(p_i, z[r_i/x])]_i . \end{aligned}$$
  Notar que $\approx$ es la relación de equivalencia de distribuciones presentada en 2.3.1

***t* = *λy.s*:** con $y \neq x$, $y \notin \mathrm{FV}(r)$
$t[r/x] = \lambda y.s[r/x]$.

Por HI $s[r/x] \mapsto [(p_i, s[r_i/x])]_i$. Por lo tanto por regla PARS inner λ,

$$\begin{aligned} \lambda y.s[r/x] &\mapsto [(p_i, \lambda y.s[r_i/x])]_i \\ &= [(p_i, (\lambda y.s)[r_i/x])]_i . \end{aligned}$$

***t* = *$s_1 s_2$*:**
$t[r/x] = s_1[r/x]s_2[r/x]$.

Como el sistema de tipos es afín $\mathrm{FV}(s_1) \cap \mathrm{FV}(s_2) = \varnothing$. Asumiendo que $x \in \mathrm{FV}(s_1)$, por HI $s_1[r/x] \mapsto [(p_i, s_1[r_i/x])]_i$. Por lo tanto por regla PARS left app,

$$\begin{aligned} s_1[r/x]s_2 &\mapsto [(p_i, s_1[r_i/x]s_2)]_i \\ &= [(p_i, (s_1 s_2)[r_i/x])]_i . \end{aligned}$$

El caso $x \in \mathrm{FV}(s_2)$ es análogo.

***t* = *ρ*:**
$$\begin{aligned} \rho[r/x] &= \rho \\ &\mapsto_0 [(1, \rho)] \\ &\approx [(p_i, \rho])]_i \\ &= [(p_i, \rho[r_i/x])]_i . \end{aligned}$$

***t* = *$U^m s$*:**
$t[r/x] = U^m s[r/x]$.

Por HI $s[r/x] \mapsto [(p_i, s[r_i/x])]_i$. Por lo tanto por regla PARS inner U,

$$\begin{aligned} U^m s[r/x] &\mapsto [(p_i, U^m s[r_i/x])]_i \\ &= [(p_i, (U^m s)[r_i/x])]_i . \end{aligned}$$

***t* = *$\pi^m s$*:**
$t[r/x] = \pi^m s[r/x]$.

Por HI $s[r/x] \mapsto [(p_i, s[r_i/x])]_i$. Por lo tanto por regla PARS inner π,

$$\begin{aligned}\pi^m s[r/x] &\mapsto [(p_i, \pi^m s[r_i/x])]_i \\ &= [(p_i, (\pi^m s)[r_i/x])]_i .\end{aligned}$$

$t = s_1 \otimes s_2$:

$t[r/x] = s_1[r/x] \otimes s_2[r/x]$.

Como el sistema de tipos es afín $\mathrm{FV}(s_1) \cap \mathrm{FV}(s_2) = \varnothing$. Asumiendo que $x \in \mathrm{FV}(s_1)$, por HI $s_1[r/x] \mapsto [(p_i, s_1[r_i/x])]_i$. Por lo tanto por regla PARS $\otimes$ left,

$$\begin{aligned}s_1[r/x] \otimes s_2 &\mapsto [(p_i, s_1[r_i/x] \otimes s_2)]_i \\ &= [(p_i, (s_1 \otimes s_2)[r_i/x])]_i .\end{aligned}$$

El caso $x \in \mathrm{FV}(s_2)$ es análogo.

$t = (m, n)$:

$$\begin{aligned}(m,n)[r/x] &= (m,n) \\ &\mapsto_0 [(1, (m,n))] \\ &\approx [(p_i, (m,n)])]_i \\ &= [(p_i, (m,n)[r_i/x])]_i .\end{aligned}$$

$t = \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$: Hay dos casos:

- $x \in \mathrm{FV}(s)$:
  $t[r/x] = \mathsf{letcase}\ y = s[r/x]\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\}$.

  Por HI $s[r/x] \mapsto [(p_i, s[r_i/x])]_i$. Por lo tanto por regla PARS inner letcase,

  $$\begin{aligned}&\mathsf{letcase}\ y = s[r/x]\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\} \\ &\qquad \mapsto [(p_i, \mathsf{letcase}\ y = s[r_i/x]\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})]_i \\ &\qquad = [(p_i, (\mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r_i/x])]_i .\end{aligned}$$

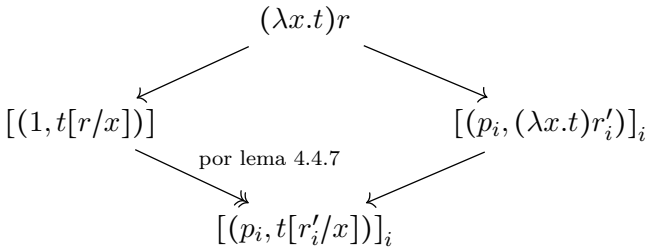
- $x \in \mathrm{FV}(\bigcup_{i=0}^{2^m-1} t_i)$:
  $(\mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r/x] = \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\}$.

  En este caso entra en juego el hecho de que los contextos son disjuntos para cada t en las ramas del letcase. La variable x puede aparecer libre en a lo sumo un término entre t_0 y t_{2^m-1}. Asumiendo que ocurre en t_j, por HI $t_j[r/x] \mapsto [(p_i, t_j[r_i/x])]_i$. Por lo tanto por regla PARS aux letcase,

  $$\begin{aligned}&\mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0[r/x], \cdots, t_{2^m-1}[r/x]\} \\ &\qquad \mapsto [(p_i, \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_j[r_i/x], \cdots, t_{2^m-1}\})]_i \\ &\qquad = [(p_i, \mathsf{letcase}\ y = s\ \mathsf{in}\ \{t_0, \cdots, t_{2^m-1}\})[r_i/x])]_i .\end{aligned}$$

□

De esta forma tenemos que la rama izquierda del par crítico cierra por el lema anterior:



Dado que ambos pares críticos son confluentes, el sistema es localmente confluente. Con extender la demostración de normalización fuerte incluyendo el caso auxiliar del letcase, por el lema 2.2.17, podemos concluir que también es globalmente confluente. Un punto a destacar es que el cálculo λ_ρ presentado originalmente en [6] está contenido en esta categoría. Tomando los contextos $\Delta_0, \cdots, \Delta_{2^m-1}$ vacíos, se obtiene λ_ρ. De esta forma, probamos su confluencia.

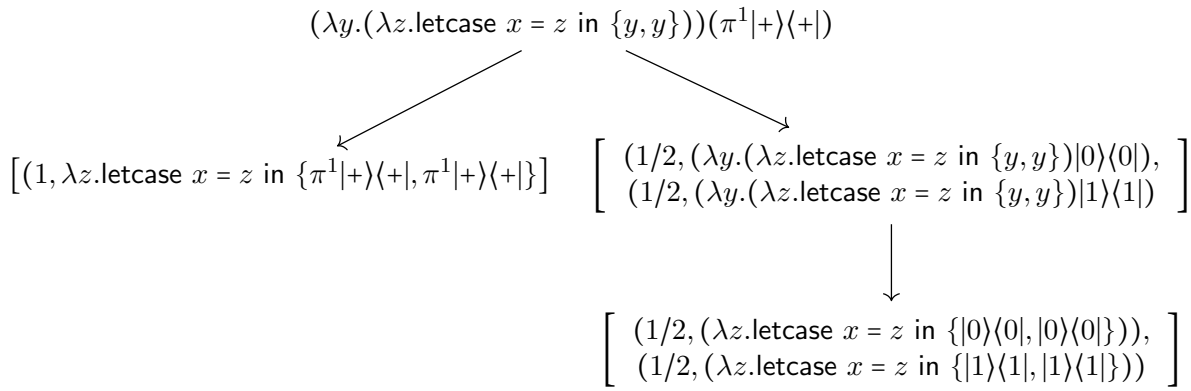
5. CONCLUSIONES Y TRABAJO FUTURO

En esta tesis definimos $\lambda_\rho 2$ y $\lambda_\rho^\circ 2$ como extensiones de los cálculos λ_ρ y λ_ρ° presentados en [6]. Probamos que se mantienen las propiedades de subject reduction y que cumplen con normalización fuerte. Para el caso de la confluencia, probamos que $\lambda_\rho^\circ 2$ y los cálculos base cumplen con la propiedad. Además, mostramos que una definición naïve de $\lambda_\rho 2$ rompe la confluencia probabilística y dimos definiciones alternativas confluentes.

5.1. Trabajo futuro

En [6] hay un enfásis importante en la interpretación de los tipos y los términos en conjuntos de matrices y matrices de densidad. Una línea de trabajo posible es expandir la interpretación del tipado presentado en esta tésis y comprobar que se siguen manteniendo las propiedades. En particular creemos que una interpretación similar a la de candidatos de reducibilidad donde $\forall X.\sigma$ se define como la intersección de las interpretaciones puede llegar a servir.

Otra línea de trabajo es continuar el análisis de confluencia de $\lambda_\rho 2$. Si bien mostramos que su primera definición no cumple estrictamente la propiedad, creemos que cumple una suerte de "confluencia semántica": hay un par crítico que no cierra, pero los programas que produce parecen ser equivalentes ya que producen los mismos resultados para los mismos inputs. Tomemos por ejemplo el término $(\lambda y.(\lambda z.\mathsf{letcase}\ x = z\ \mathsf{in}\ \{y, y\}))(\pi^1|+\rangle\langle+|)$ que mostramos como contraejemplo a la confluencia.



En la rama izquierda, cualquiera sea el argumento del letcase termina reduciendo a $\pi^1|+\rangle\langle+|$ que tiene probabilidad $\frac{1}{2}$ de reducir a $|0\rangle\langle 0|$ y la misma probabilidad a $|1\rangle\langle 1|$. Por otro lado en la rama derecha, hay dos reducciones posibles con probabilidad $\frac{1}{2}$ de reducir a un letcase que devuelve $|0\rangle\langle 0|$ o $|1\rangle\langle 1|$, con probabilidad 1 respectivamente. Es decir que para cada medición, el término reduce a los mismos resultados.

A nuestro conocimiento, no hay un cálculo que combine reducciones probabilísticas, falta de estrategia y variables no afines, manteniendo confluencia. Sin embargo, $\lambda_\rho 2$ está muy cerca de esas condiciones. Se deja para trabajo futuro un análisis más en profundidad.

Bibliografía

[1] Pablo Arrighi, Alejandro Díaz-Caro, and Benoît Valiron. The vectorial lambda-calculus. *Information and Computation*, 254(1):105–139, 2017.

[2] Pablo Arrighi and Gilles Dowek. Lineal: a linear-algebraic lambda-calculus. *Logical Methods in Computer Science*, 13(1:8), 2017.

[3] Henk Barendregt. *The lambda calculus: its syntax and semantics*, volume 103 of *Studies in logic and the foundations of Mathematics*. North Holland, revised edition, 1985.

[4] Henk Barendregt. Lambda calculi with types. In Samsom Abramsky, Dov M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science: Volume 2. Background: Computational Structures*. Clarendon Press, 1993.

[5] Agustın Borgna. Simulación del lambda cálculo de matrices de densidad en el lambda cálculo cuántico de selinger y valiron. Tesis de Licenciatura. Universidad de Buenos Aires, 2019.

[6] Alejandro Díaz-Caro. A lambda calculus for density matrices with classical and probabilistic controls. In Bor-Yuh Evan Chang, editor, *Programming Languages and Systems (APLAS 2017)*, volume 10695 of *Lecture Notes in Computer Science*, pages 448–467. Springer, Cham, 2017.

[7] Alejandro Díaz-Caro and Gilles Dowek. Typing quantum superpositions and measurement. In Carlos Martín-Vide, Roman Neruda, and Miguel A. Vega-Rodríguez, editors, *Theory and Practice of Natural Computing (TPNC 2017)*, volume 10687 of *Lecture Notes in Computer Science*, pages 281–293. Springer, Cham, 2017.

[8] Alejandro Díaz-Caro, Mauricio Guillermo, Alexandre Miquel, and Benoît Valiron. Realizability in the unitary sphere. In *Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2019)*, pages 1–13, 2019.

[9] Alejandro Díaz-Caro and Octavio Malherbe. A concrete categorical semantics for lambda-s. In Beniamino Accattoli and Carlos Olarte, editors, *Proceedings of the 13th Workshop on Logical and Semantic Frameworks with Applications (LSFA'18)*, volume 344 of *Electronic Notes in Theoretical Computer Science*, pages 83–100. Elsevier, 2019.

[10] Alejandro Díaz-Caro and Octavio Malherbe. A categorical construction for the computational definition of vector spaces. Por aparecer en Applied Categorical Structures. arXiv preprint 1905.01305, 2020.

[11] Jean-Yves Girard. *Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur*. PhD thesis, Université Paris-Diderot, 1972.

[12] Alexander S Green, Peter LeFanu Lumsdaine, Neil J Ross, Peter Selinger, and Benoît Valiron. Quipper: a scalable quantum programming language. *ACM SIGPLAN Notices*, 48(6):333–342, 2013. (POPL'13).

[13] Malena Ivnisky. Agregando punto fijo a una extensión cuántica de lambda cálculo con matrices de densidad. Thesis de Licenciatura. Universidad de Buenos Aires., 2020.

[14] Guido Martínez. Confluencia en sistemas de reescritura probabilista. Tesis de Licenciatura. Universidad Nacional de Rosario, 2017.

[15] Michael Nielsen and Isaac Chuang. *Quantum computation and quantum information.* Cambridge University Press, 2000.

[16] Michele Pagani, Peter Selinger, and Benoît Valiron. Applying quantitative semantics to higher-order quantum computing. *ACM SIGPLAN Notices*, 49(1):647–658, 2014. (POPL'14).

[17] John C. Reynolds. Towards a theory of type structure. In *Programming Symposium*, pages 408–425. Springer, 1974.

[18] Peter Selinger. Towards a quantum programming language. *Theoretical Structures in Science*, 14(4):527–586, 2004.

[19] Peter Selinger and Benoit Valiron. A lambda calculus for quantum computation with classical control. *Mathematical Structures in Computer Science*, 16(3):527–552, 2006.

[20] TeReSe. *Term rewriting systems.* Cambridge University Press, 2003.

[21] André van Tonder. A lambda calculus for quantum computation. *SIAM Journal on Computing*, 33(5):1109–1135, 2004.

[22] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[23] Mingsheng Ying. *Foundations of Quantum Programming.* Morgan Kaufmann, 2016.

[24] Margherita Zorzi. On quantum lambda calculi: a foundational perspective. *Mathematical Structures in Computer Science*, 26(7):1107–1195, 2016.