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

Agregando punto fijo a una extensión cuántica de lambda cálculo con matrices de densidad

Tesis de Licenciatura en Ciencias de la Computación

Malena Ivnisky

Director: Alejandro Díaz-Caro
Codirector: Hernán Melgratti
Buenos Aires, 2020

AGREGANDO UN OPERADOR DE PUNTO FIJO A UNA EXTENSIÓN CUÁNTICA DE LAMBDA CÁLCULO CON MATRICES DE DENSIDAD

El cálculo λ_ρ presentado por Díaz-Caro en 2017 es una extensión cuántica del lambda cálculo que usa matrices de densidad. Estas matrices permiten representar estados mixtos de conjuntos de bits cuánticos. El cálculo modificado λ_ρ° generaliza las matrices de densidad a sumatorias algebraicas de términos. Ambos cálculos tienen definida una semántica denotacional compartida.

Este trabajo representa un primer paso hacia el agregado de punto fijo al cálculo λ_ρ°. Definimos una extensión con punto fijo en el límite y otra intermedia, con punto fijo incremental. La semántica denotacional fue redefinida respecto a la original para dar a los dominios estructura de orden parcial completo sobre matrices positivas. La demostración de adecuación depende de dos conjeturas dejadas para trabajo futuro.

Suponiendo correcta la definición de la semántica, esto permite probar la existencia del límite del punto fijo incremental gracias a la estructura de orden parcial completo. La interpretación del punto fijo puede definirse entonces como el límite de una secuencia creciente y acotada de interpretaciones de términos en el dominio.

Palabras clave: Punto fijo, lambda cálculo, computación cuántica, matrices de densidad, orden parcial completo.

ADDING A FIXED-POINT OPERATOR TO A QUANTUM EXTENSION TO THE LAMBDA CALCULUS WITH DENSITY MATRICES

The λ_ρ calculus presented by Díaz-Caro in 2017 is a quantum extension to lambda calculus that uses density matrices. These matrices allow us to represent sets of quantum bits' mixed quantum states. The modified calculus λ_ρ° generalizes density matrices to algebraic sums of terms. Both calculi share their denotational semantics.

This work represents a first step towards adding fixed-point to the λ_ρ° calculus. We define an extension with fixed-point as a limit, and an intermediate one with an incremental fixed-point. The denotational semantics were redefined in respect to the original one, in order for the domains to have a complete partial order structure over positive matrices. The proof of adequacy depends on two conjectures, left for future work.

Supposing that the denotational semantics is sound and well defined, this allows us to prove the existence of the limit for the fixed-point inside the domains, thanks to the complete partial order structure. The fixed-point semantics can then be defined as the limit of an increasing bounded sequence of term interpretations inside the domain.

Keywords: Fixed-point, lambda calculus, quantum computing, density matrices, complete partial order.

AGRADECIMIENTOS

A Jano y Hernán, por estar siempre dispuestos a ayudarme a avanzar y por responder todas mis dudas.

A Pablo y Santiago, por tomarse el tiempo de leer la tesis y por las correcciones que fueron muy útiles.

A Benoît y Octavio por ayudarme con mis dudas con los temas más complicados.

A mis amigues, a mi mamá, a mi papá, a Gonza y a las michis, por estar siempre bancándome en todas ♡

A mi familia y amigues.

Índice general

INTRODUCCIÓN

En los últimos quince años se han investigado muchas extensiones cuánticas del lambda cálculo, como por ejemplo [vT04, SV05, PSV14, Zor16, ADCV17, AD17, DCD17]. En todos estos casos los estados cuánticos están representados mediante vectores en el espacio de Hilbert. Sin embargo esta representación también puede hacerse mediante matrices de densidad. Las matrices de densidad permiten la descripción no sólo de los estados, sino también de mezclas estadísticas de ellos, representando así nuestro desconocimiento sobre el estado del sistema mediante una distribución de probabilidad para los estados precisos. Usar esta representación lleva a una formulación alternativa de los postulados de la mecánica cuántica, y por lo tanto también puede ser usada para la computación cuántica.

En [Sel04] Selinger introdujo un lenguaje de diagramas de flujo cuánticos, interpretados en un orden parcial completo de matrices de densidad. A partir de la publicación de este paper las matrices de densidad comenzaron a ser mucho más usadas como forma de representación de datos en computación cuántica, como por ejemplo en [DP06, FDY11, Yin12, FYY13, YYW17]. Incluso el libro "Foundations of Quantum Programming" [Yin16] fue escrito por completo usando matrices de densidad.

Además de la clasificación de los lenguajes según la forma de representación de los estados, estos también pueden ser distinguidos según su forma de control. Este puede ser tanto clásico como cuántico. La idea de combinar datos cuánticos con control clásico de [Sel04] fue usada en [SV05] para definir λ_q, una de las primeras extensiones cuánticas de lambda cálculo. Luego este cálculo fue la base para el lenguaje de programación cuántico Quipper [GLR$^+$13]. El paradigma de datos cuánticos con control clásico considera una computadora clásica con programas clásicos, y un procesador cuántico adicional al cual esta puede acceder. Mediante instrucciones clásicas al procesador cuántico se pueden realizar operaciones sobre los bits cuánticos, realizar mediciones sobre estos y obtener los resultados. De esta forma es el procesador cuántico el que se encarga de actuar sobre los qubits. Muchos trabajos están enmarcados dentro de este paradigma, como [SV05, AG05, GLR$^+$13, PSV14, Zor16].

El paradigma de datos cuánticos con control cuántico supone la idea de proveer definiciones computacionales para las nociones de espacio vectorial y funciones bilineales. Existen varias definiciones de lenguajes cuánticos de alto nivel que usan control cuántico, por ejemplo en [AG05, YYF12, YYF14, BP15]. Recientemente fue introducida la primera extensión de lambda cálculo con control cuántico [DCGMV19], siguiendo la línea de investigación de trabajos anteriores [ADC12, ADCV17, AD17, ADCP$^+$14, DCP12].

En [DC17] Díaz-Caro introduce los cálculos λ_ρ y λ_ρ°, las primeras dos extensiones cuánticas al lambda cálculo sobre matrices de densidad. El cálculo λ_ρ se encuentra enmarcado en el paradigma del control clásico, representando los datos cuánticos sobre matrices de densidad. λ_ρ° es una generalización de esta extensión donde se generalizan las matrices de densidad al control clásico, es decir que luego de realizar las mediciones se combinan los términos de todas las posibles reducciones de λ_ρ en una matriz de densidad generalizada de términos. Este control no es cuántico, ya que los términos no se superponen en este sentido, sino que podría considerarse como un tipo de control probabilístico.

El objetivo de esta tesis es agregar punto fijo al cálculo λ_ρ°, definiendo una semántica

adecuada para su interpretación. El punto fijo permite escribir programas recursivos, lo cual no es posible en la formulación original del cálculo.

Para lograrlo se definieron dos extensiones, $\lambda_\rho^{\mu_n}$ y λ_ρ^{μ}. La primera agrega mínimo punto fijo incremental en n pasos y la segunda agrega el mínimo punto fijo en el límite. Se redefinió completamente la semántica con respecto de la original que tenía λ_ρ° en [DC17], para pasar a interpretar cualquier término tipable como una matriz de densidad generalizada. Los dominios de interpretación fueron definidos como órdenes parciales completos, al igual que en [Sel04]. Para lograrlo, las funciones son interpretadas en forma similar a las de [SV08] como mapas completos positivos, aunque con la diferencia de que en este lenguaje las funciones son afines y no lineales. Para terminar de demostrar que los dominios y las interpretaciones de funciones sobre estos cumplen las propiedades requeridas para ser órdenes parciales completos fue necesario agregar dos conjeturas, que por falta de tiempo no pudieron ser demostradas y quedan como trabajo futuro.

La estructura de la tesis es la siguiente:

- En el capítulo 1 se definen los conceptos matemáticos que serán usados en el trabajo. Además se hace una introducción breve a mecánica cuántica sobre matrices de densidad.
- En el capítulo 2 se presentan los cálculos λ_ρ y λ_ρ°.
- En el capítulo 3 se definen los cálculos $\lambda_\rho^{\mu_n}$ y λ_ρ^{μ}, extensiones de λ_ρ°.
- En el capítulo 4 se define la semántica denotacional de los cálculos definidos en el capítulo 3. Para esto se demuestra (asumiendo las conjeturas) que el punto fijo incremental de $\lambda_\rho^{\mu_n}$ tiene límite dentro de los dominios de interpretación.
- En el capítulo 5 se exponen las conclusiones e ideas para trabajo futuro.

1. PRELIMINARES

Este capítulo se divide en dos partes. En la primera se definen algunos conceptos y propiedades sobre matrices, los cuales son necesarios para la segunda parte en la que se introduce la mecánica cuántica sobre matrices de densidad. Además se definen conceptos relacionados con los órdenes parciales completos, que van a ser usados en la última parte de la tesis.

1.1. Definiciones y propiedades matemáticas

Se usa la notación $\mathbb{0}_n$ y $\mathbb{1}_n$ para representar las matrices nulas y la identidad en $\mathbb{C}^{n\times n}$, respectivamente.

1.1.1. Traza matricial

Definición 1.1.1 (Traza)**.** Sea A una matriz cuadrada. Su traza $\mathsf{tr}\,(A)$ se define como la suma de los elementos de la diagonal.

Propiedad 1.1.2 (Linealidad de la traza)**.** *Sean A, B en $\mathbb{C}^{n\times n}$ y α en $\mathbb{C}$. Entonces* $\mathsf{tr}\,(A+B) = \mathsf{tr}\,(A) + \mathsf{tr}\,(B)$ *y* $\mathsf{tr}\,(\alpha A) = \alpha \mathsf{tr}\,(A)$.

Propiedad 1.1.3 (Propiedad cíclica de la traza)**.** *Sean A, B y C en $\mathbb{C}^{n\times n}$. Entonces* $\mathsf{tr}\,(ABC) = \mathsf{tr}\,(BCA)$.

1.1.2. Matrices hermíticas y positivas

Definición 1.1.4 (Matriz transpuesta conjugada)**.** Sea A una matriz en $\mathbb{C}^{n\times n}$. $A^\dagger$ simboliza su transpuesta conjugada, es decir la matriz en $\mathbb{C}^{n\times n}$ tal que $(A^\dagger)_{ij} = \overline{A_{ji}}$.

Propiedades 1.1.5. *Sean A, B en $\mathbb{C}^{n\times n}$ y α en $\mathbb{C}$. Entonces:*

1. $(A^\dagger)^\dagger = A$
2. $(A+B)^\dagger = A^\dagger + B^\dagger$
3. $(\alpha A)^\dagger = \alpha^* A^\dagger$
4. $(AB)^\dagger = B^\dagger A^\dagger$

Definición 1.1.6 (Matriz hermítica)**.** Una matriz A en $\mathbb{C}^{n\times n}$ se dice hermítica si y solo si $A^\dagger = A$.

Definición 1.1.7 (Matriz positiva)**.** Una matriz A en $\mathbb{C}^{n\times n}$ se dice positiva si y solo si es hermítica y $u^\dagger A u \geq 0$ para todo u en $\mathbb{C}^n$. Notamos con $\mathcal{P}_n$ al conjunto de matrices positivas en $\mathbb{C}^{n\times n}$.

Observación 1.1.8. Toda matriz positiva es diagonalizable.

Teorema 1.1.9. *Las matrices positivas forman un espacio vectorial sobre $\mathbb{R}_{\geq 0}$.*

Demostración. Sean a, b constantes en $\mathbb{R}_{\geq 0}$ y A, B matrices en $\mathcal{P}_n$. Queremos ver que

$$aA + bB \in \mathcal{P}_n$$

- $aA + bB$ es hermítica:

  Se tiene $(aA + bB)^\dagger = aA^\dagger + bB^\dagger$ pues a y b son reales. Como A y B son hermíticas por hipótesis, $A^\dagger = A$ y $B^\dagger = B$, y por lo tanto $(aA + bB)^\dagger = aA + bB$.

- $aA + bB$ es semidefinida positiva:

  Sea u un vector en $\mathbb{C}^n$. Se tiene $u^\dagger(aA + bB)u = a(u^\dagger Au) + b(u^\dagger Bu)$. Como A y B son positivas, valen $u^\dagger Au \geq 0$ y $u^\dagger Bu \geq 0$ para todo u. Por lo tanto $u^\dagger(aA+bB)u \geq a + b \geq 0$ pues $a, b \in \mathbb{R}_{\geq 0}$.

Por lo tanto $aA + bB$ pertenece a $\mathcal{P}_n$. □

Lema 1.1.10. *Sea M una matriz en $\mathcal{P}_n$, si $\mathsf{tr}\,(M) = 0$ entonces $M = \mathbb{0}_n$.*

Demostración. Como M es positiva, es diagonalizable. Entonces existen P una matriz inversible y D una matriz diagonal tales que

$$M = PDP^{-1}$$

Aplicando la traza se tiene:

$$\mathsf{tr}\,(M) = \mathsf{tr}\left(PDP^{-1}\right) = \mathsf{tr}\left(DP^{-1}P\right) = \mathsf{tr}\,(D)$$

Como $\mathsf{tr}\,(M) = 0$ por hipótesis, se tiene que $\mathsf{tr}\,(D) = 0$. Por ser D diagonal, es nula y por lo tanto M también. □

1.1.3. Producto tensorial

Sean M y N matrices complejas de dimensiones $n \times m$ y $p \times q$ respectivamente, donde $M = (m_{ij})$ y $N = (n_{ij})$. El producto tensorial $M \otimes N$ entre ellas se define como la matriz compleja de dimensión $np \times mq$ tal que:

$$M \otimes N = \begin{pmatrix} m_{11}N & \dots & m_{1m}N \\ \vdots & \ddots & \vdots \\ m_{n1}N & \dots & m_{nm}N \end{pmatrix} = \begin{pmatrix} m_{11}n_{11} & \dots & m_{11}n_{1q} & m_{12}n_{11} & \dots & m_{1m}n_{1q} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ m_{11}n_{p1} & \dots & m_{11}n_{pq} & m_{12}n_{p1} & \dots & m_{1m}n_{pq} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ m_{n1}n_{p1} & \dots & m_{n1}n_{pq} & m_{n2}n_{p1} & \dots & m_{nm}n_{pq} \end{pmatrix}$$

Cuando M y N son vectores columna, el resultado es otro vector columna. Análogamente, si son vectores fila el resultado también lo es.

$$v \otimes w = \begin{pmatrix} v_1 w \\ \vdots \\ v_n w \end{pmatrix} = \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_1 w_p \\ \vdots \\ v_n w_p \end{pmatrix}$$

$$v^t \otimes w^t = \begin{pmatrix} v_1 w & \dots & v_n w \end{pmatrix} = \begin{pmatrix} v_1 w_1 & v_1 w_2 & \dots & v_1 w_p & \dots & v_n w_p \end{pmatrix}$$

Algunas propiedades del producto tensorial:

Propiedades 1.1.11. *Sean A, A' en $\mathbb{C}^{n\times m}$, B, B' en $\mathbb{C}^{p\times q}$, C en $\mathbb{C}^{m\times r}$, D en $\mathbb{C}^{q\times s}$ y α, β en $\mathbb{C}$. Entonces:*

1. $(\alpha A) \otimes (\beta B) = \alpha\beta(A \otimes B)$
2. $A \otimes (B + B') = A \otimes B + A \otimes B'$
   $(A + A') \otimes B = A \otimes B + A' \otimes B$
3. *En general,* $A \otimes B \neq B \otimes A$
4. *Propiedad del producto mixto:* $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$
5. $\mathsf{tr}\,(A \otimes B) = \mathsf{tr}\,(A)\,\mathsf{tr}\,(B)$
6. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$

1.1.4. Matrices unitarias

Definición 1.1.12. $U \in \mathbb{C}^{n\times n}$ es una matriz unitaria si y sólo si $U^\dagger U = UU^\dagger = I_n$.

Lema 1.1.13. *Sea U una matriz unitaria en $\mathbb{C}^{n\times n}$ y V una matriz unitaria en $\mathbb{C}^{m\times m}$. Entonces $U \otimes V$ es una matriz unitaria en $\mathbb{C}^{nm\times nm}$.*

Demostración. Usando que † distribuye respecto a ⊗ y por la propiedad del producto mixto:

$$\begin{aligned}(U \otimes V)(U \otimes V)^\dagger &= (U \otimes V)(U^\dagger \otimes V^\dagger)\\ &= UU^\dagger \otimes VV^\dagger\\ &= I_n \otimes I_m = I_{nm}\end{aligned}$$

$$\begin{aligned}(U \otimes V)^\dagger(U \otimes V) &= (U^\dagger \otimes V^\dagger)(U \otimes V)\\ &= U^\dagger U \otimes V^\dagger V\\ &= I_n \otimes I_m = I_{nm}\end{aligned}$$

□

Teorema 1.1.14. *Sea M en $\mathcal{P}_n$, entonces para cualquier matriz U en $\mathbb{C}^{n\times n}$ se tiene que $UMU^\dagger$ está en $\mathcal{P}_n$. Si además U es unitaria, la traza se preserva.*

Demostración.

- $UMU^\dagger$ es hermítica: por propiedades de † se tiene que $(UMU^\dagger)^\dagger = U(UM)^\dagger = UM^\dagger U^\dagger$. Esto es igual a $UMU^\dagger$ porque $M \in \mathcal{P}_n$.
- $UMU^\dagger$ es semidefinida positiva: sea $v \in \mathbb{C}^{2^n}$. Por propiedades de † se tiene que $vUMU^\dagger v^\dagger = (vU)M(vU)^\dagger$. Como $Uv \in \mathbb{C}^{2^n}$ y M es semidefinida positiva, se tiene que $(vU)M(vU)^\dagger \geq 0$.
- La traza se preserva cuando U es unitaria: por propiedad cíclica de la traza se tiene que $\mathsf{tr}\left(UMU^\dagger\right) = \mathsf{tr}\left(MU^\dagger U\right)$. Como U es unitaria, se tiene $U^\dagger U = I$ y por lo tanto $\mathsf{tr}\left(MU^\dagger U\right) = \mathsf{tr}\,(M)$.

□

1.1.5. Coproducto

El operador $\oplus$ representa la concatenación de matrices. Se puede ver como una matriz definida por bloques de las matrices concatenadas. Por ejemplo:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \oplus \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & 0 & 0 & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 & 0 & 0 \\ 0 & 0 & b_{11} & b_{12} & b_{13} & b_{14} \\ 0 & 0 & b_{21} & b_{22} & b_{23} & b_{24} \\ 0 & 0 & b_{31} & b_{32} & b_{33} & b_{34} \\ 0 & 0 & b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

Se puede ver que la traza distribuye linealmente respecto a $\oplus$: $\mathsf{tr}\,(A \oplus B) = \mathsf{tr}\,(A) + \mathsf{tr}\,(B)$.

1.1.6. Punto fijo en órdenes parciales completos

En esta sección se definen los órdenes parciales completos (CPOs) y se definen monotonía y continuidad de funciones entre CPOs. Finalmente se demuestra la existencia de mínimo punto fijo en el teorema (1.1.18) para funciones que cumplan estas propiedades.

Definición 1.1.15 (Supremo)**.** Sea S un subconjunto no vacío de T, otro conjunto con un orden parcial definido. El supremo de S, si existe, es el mínimo elemento de T tal que todos los elementos de S son menores que él, y se denota $\bigsqcup S$.

Sea (x_n) una sucesión de elementos de T. El supremo de (x_n) es igual al supremo de $\{x_n\}$, el subconjunto de T con todos los elementos de la sucesión, y se denota $\bigsqcup_n x_n$.

Definición 1.1.16 (Orden parcial completo [Win93, p. 70])**.**
El orden parcial $(D, \sqsubseteq)$ es un *orden parcial completo* (abreviado CPO en inglés) si tiene supremos para todas las sucesiones crecientes $d_0 \sqsubseteq d_1 \sqsubseteq \cdots \sqsubseteq d_n \sqsubseteq \ldots$, es decir que cualquier sucesión creciente (d_n) de elementos de D tiene supremo $\bigsqcup_n d_n$.

$(D, \sqsubseteq)$ es un CPO *con bottom* si es un CPO que tiene un elemento mínimo $\bot \in D$ (llamado "bottom").

Definición 1.1.17 (Función continua [Win93, p. 71])**.**
Una función $f : (D, \sqsubseteq_D) \to (E, \sqsubseteq_E)$ entre CPOs $(D, \sqsubseteq_D)$ y $(E, \sqsubseteq_E)$ es monótona si y sólo si

$$\forall d, d' \in D, d \sqsubseteq_D d' \implies f(d) \sqsubseteq_E f(d')$$

Esta función es continua si y sólo si es monótona y para todas las cadenas $d_0 \sqsubseteq_D d_1 \sqsubseteq_D \ldots \sqsubseteq_D d_n \sqsubseteq_D \ldots$ en D se tiene

$$\bigsqcup_{n \in \omega} f(d_n) = f(\bigsqcup_{n \in \omega} d_n)$$

A continuación se transcribe la demostración de un teorema de punto fijo [Win93, Teorema 5.11]. Este será usado más adelante para interpretar los términos de punto fijo en $\lambda_\rho^{\mu_n}$.

Teorema 1.1.18. *Sea $(A, \sqsubseteq)$ un CPO con bottom $\bot$, y sea $f : (A, \sqsubseteq) \to (A, \sqsubseteq)$. Si f es continua, entonces $\bigsqcup_{n \in \omega} f^n(\bot)$ es el mínimo punto fijo de f.*

Demostración. Por continuidad de f se tiene:

$$\begin{aligned} f(\bigsqcup_{n\in\omega} f^n(\bot)) &= \bigsqcup_{n\in\omega} f^{n+1}(\bot) \\ &= (\bigsqcup_{n\in\omega} f^{n+1}(\bot)) \sqcup \{\bot\} \\ &= \bigsqcup_{n\in\omega} f^n(\bot) \end{aligned}$$

Por lo tanto $\bigsqcup_{n\in\omega} f^n(\bot)$ es punto fijo de f.

Falta ver que además es el mínimo punto fijo. Sea d un punto fijo cualquiera de f en $(A, \sqsubseteq)$. Por definición, vale que $\bot \sqsubseteq d$. Como f es monótona, se tiene que $f(\bot) \sqsubseteq f(d)$. Entonces $f(\bot) \sqsubseteq d$, ya que $f(d) = d$ por ser punto fijo de f. Por inducción se tiene que entonces $f^n(\bot) \sqsubseteq d$ para todo n. Por lo tanto $\bigsqcup_{n\in\omega} f^n(\bot) \sqsubseteq d$ y entonces $\bigsqcup_{n\in\omega} f^n(\bot)$ es el mínimo punto fijo de f. □

1.2. Introducción a mecánica cuántica

La mecánica cuántica describe el estado de un sistema como un vector de norma 1 en un espacio vectorial complejo. La dimensión del espacio depende de las características del sistema en cuestión, en el caso de los bits cuánticos, o qubits, la dimensión del espacio vectorial que los describe es 2. Para un sistema de n qubits la dimensión del espacio vectorial en el cual se describe el sistema es 2^n. En el caso más general los sistemas físicos podrían tener características como por ejemplo la posición o la velocidad, que tienen infinitos valores posibles no numerables. Para describir este tipo de sistemas de dimensión infinita se usan los espacios de Hilbert más generales. Sin embargo, para este trabajo se usará sólo el espacio de Hilbert $\mathbb{C}^{2^n}$.

Las matrices de densidad son una forma alternativa de descripción que representa una distribución de probabilidades para un conjunto de estados, es decir una mezcla estadística de estados. También contienen las representaciones de sistemas para los cuales se sabe con certeza cuál es el vector del espacio que representa al estado, recuperando así los sistemas descriptos mediante vectores del espacio.

1.2.1. Notación de Dirac

La notación de Dirac es la notación usual para describir estados de sistemas cuánticos. Los elementos principales son los *kets*, de la forma $|\alpha\rangle$, y los *bras* $\langle\beta|$. α y β son etiquetas de los elementos.

Los kets representan vectores del espacio. El estado de los sistemas se puede descomponer en alguna de las bases de su espacio de representación, donde los vectores de la base se escriben como kets etiquetados. Por ejemplo el sistema conformado por un solo qubit está en $\mathbb{C}^2$ por lo que su base canónica está conformada por:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

El ket $|0\rangle$ representa el estado de un qubit análogo a un bit 0 clásico, y el ket $|1\rangle$ representa el estado de un qubit análogo a un bit 1 clásico. Cualquier combinación lineal compleja de estos dos vectores de la base cuya norma sea 1 representa un estado posible

para un qubit. En este caso se dirá que el qubit está en un estado superposición de $|0\rangle$ y $|1\rangle$.

Otra base usual para este espacio es la base de Hadamard. Esta base está rotada 45 grados respecto a la canónica, y sus kets base se etiquetan con + y −:

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \qquad |-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

Por ejemplo, el vector $|\alpha\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$ en $\mathbb{C}^2$ se puede descomponer en la base canónica como $|\alpha\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$ y en la base de Hadamard como $|\alpha\rangle = \frac{1+i}{2}|+\rangle + \frac{1-i}{2}|-\rangle$. En particular $|+\rangle$ es un vector de la base de Hadamard, el cual visto sobre la base canónica está en superposición.

En el caso de los espacios $\mathbb{C}^{2^n}$ que se usan para describir sistemas de n qubits, se puede pensar a los kets como vectores columna y a los bras como vectores fila. El bra correspondiente al ket $|\alpha\rangle$ es $\langle\alpha| = |\alpha\rangle^\dagger$, es decir el vector fila que resulta de trasponer y conjugar los elementos del ket. De esta forma, los bra correspondientes a los kets anteriores son:

$$\langle 0| = \begin{pmatrix}1 & 0\end{pmatrix} \qquad \langle +| = \tfrac{1}{\sqrt{2}}(\langle 0| + \langle 1|) = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\end{pmatrix}$$

$$\langle 1| = \begin{pmatrix}0 & 1\end{pmatrix} \qquad \langle -| = \tfrac{1}{\sqrt{2}}(\langle 0| - \langle 1|) = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\end{pmatrix}$$

$$\langle\alpha| = \tfrac{1}{\sqrt{2}}\langle 0| - \tfrac{i}{\sqrt{2}}\langle 1| = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\end{pmatrix}$$

Producto ket-bra

La forma de interpretar a un ket seguido de un bra es mediante la multiplicación matricial. Por ejemplo:

$$|0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} \qquad |0\rangle\langle 1| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}$$

$$|0\rangle\langle +| = |0\rangle\tfrac{1}{\sqrt{2}}(\langle 0| + \langle 1|) = \tfrac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1|) = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}$$

$$|+\rangle\langle +| = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}\tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\end{pmatrix} = \tfrac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}$$

De esta forma, la base canónica de $\mathbb{C}^{2\times 2}$ se puede escribir de la siguiente manera:

$$\{|0\rangle\langle 0|, |0\rangle\langle 1|, |1\rangle\langle 0|, |1\rangle\langle 1|\}$$

Producto bra-ket

Los productos bra-ket son equivalentes al producto interno (donde al segundo argumento se lo conjuga) por lo que el resultado es un elemento de $\mathbb{C}$. Los elementos

ortogonales tienen producto interno nulo y el producto interno de un elemento consigo mismo es igual al cuadrado de su norma (que es 1):

$$\langle 1|1\rangle = \begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = 1 \qquad \langle 0|1\rangle = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = 0$$

$$\langle -|1\rangle = \tfrac{1}{\sqrt{2}}(\langle 0| - \langle 1|)|1\rangle = \tfrac{1}{\sqrt{2}}(\langle 0|1\rangle - \langle 1|1\rangle) = \tfrac{1}{\sqrt{2}}$$

Producto tensorial de kets y bras

Los kets también pueden multiplicarse entre sí mediante el producto tensorial. La interpretación del producto tensorial de dos estados es el estado conjunto. Por ejemplo si se tiene un qubit en estado $|0\rangle$ y otro en estado $|1\rangle$, el estado que los describe a ambos como un solo sistema es $|0\rangle \otimes |1\rangle$. La notación usada para este vector es $|01\rangle$. Esto se generaliza a dimensión n, si se tienen qubits en estados $|b_1\rangle$, $|b_2\rangle$, ..., $|b_n\rangle$ entonces su estado conjunto está dado por $|b_1\rangle \otimes |b_2\rangle \otimes \ldots \otimes |b_n\rangle$, que se nota $|b_1 b_2 \ldots b_n\rangle$. De acuerdo a la definición del producto tensorial las bases canónicas para cualquier dimensión van a estar dadas por $\{|0\ldots00\rangle, |0\ldots01\rangle, |0\ldots10\rangle, \ldots, |1\ldots11\rangle\}$.

Análogamente para los bras se tiene que $\langle b_1| \otimes \langle b_2| \otimes \ldots \otimes \langle b_n|$ se nota $\langle b_1 b_2 \ldots b_n|$, donde $|b_1 b_2 \ldots b_n\rangle^\dagger = \langle b_1 b_2 \ldots b_n|$ y viceversa.

Esta notación es útil ya que los operadores que multiplican a izquierda a los kets (y de la misma forma los operadores que multiplican a derecha a los bras) si están escritos en forma de producto tensorial de operadores de la dimensión correcta, operan separadamente sobre los subsistemas. Por ejemplo:

$$\left(\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\right)|00\rangle = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}|0\rangle \otimes \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}|0\rangle = |1\rangle \otimes |0\rangle = |10\rangle$$

$$\langle 10|\left(\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \otimes \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\right) = \langle 1|\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \otimes \langle 0|\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} = \langle 1| \otimes \langle 1| = \langle 11|$$

Estados separables y estados entrelazados

Cuando el estado de un sistema compuesto se puede escribir como producto tensorial entre estados de sus subsistemas se dice que el estado es separable, es decir que se pueden recuperar los sistemas independientes que lo conforman. En caso contrario el estado está entrelazado. Esto significa que las partes que conforman al sistema no son independientes, sino que hay dependencias entre una y otra. Esto resulta en que cambios en el estado de una parte del sistema repercutan en el estado de otra parte del sistema.

Por ejemplo, un sistema de dos qubits cuyo estado se encuentra descripto por el vector

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$$

no puede separarse en un solo producto tensorial, por lo tanto es un estado entrelazado.

1.2.2. Matrices de densidad

Las matrices de densidad representan mezclas estadísticas de estados. Estas mezclas de estados son clásicas, no representan superposiciones. Son matrices positivas (definidas positivas y hermíticas) de traza igual a 1.

Si se tiene una mezcla de estados de la forma $\{p_i, |\psi_i\rangle\}_i$ (donde el sistema tiene probabilidad clásica p_i de estar en estado $|\psi_i\rangle$, y las probabilidades suman 1), entonces la matriz que describe al sistema es:

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

Se puede ver que el requerimiento de que la traza sea igual a 1 es equivalente a pedir que las probabilidades de la mezcla de estados sumen 1, ya que los vectores de estado están normalizados:

$$\begin{aligned}\mathsf{tr}(\rho) &= \sum_i \mathsf{tr}\left(p_i|\psi_i\rangle\langle\psi_i|\right) = \sum_i p_i \mathsf{tr}\left(|\psi_i\rangle\langle\psi_i|\right) = \sum_i p_i \mathsf{tr}\left(|\psi_i\rangle|\psi_i\rangle^\dagger\right) \\ &= \sum_i p_i \langle\psi_i|\psi_i\rangle = \sum_i p_i \left\||\psi_i\rangle\right\|^2 = \sum_i p_i\end{aligned}$$

Por ejemplo, si se tiene un sistema de un qubit cuyo estado tiene probabilidad clásica $\frac{1}{2}$ de ser $|0\rangle$, probabilidad $\frac{1}{4}$ de ser $|1\rangle$ y probabilidad $\frac{1}{4}$ de ser $|+\rangle$, la matriz de densidad que representa el conocimiento sobre el estado del sistema es:

$$\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{4}|1\rangle\langle 1| + \tfrac{1}{4}|+\rangle\langle +| = \tfrac{5}{8}|0\rangle\langle 0| + \tfrac{1}{8}|0\rangle\langle 1| + \tfrac{1}{8}|1\rangle\langle 0| + \tfrac{3}{8}|1\rangle\langle 1| = \begin{pmatrix} \frac{5}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{3}{8} \end{pmatrix}$$

Se dice que una matriz representa un estado puro cuando la mezcla de estados contiene sólo uno, con probabilidad 1. En otro caso, el estado del sistema se llama mixto. Si la matriz ρ describe el estado del sistema, éste es puro si y sólo si $\mathsf{tr}\left(\rho^2\right) = 1$, mientras que si es mixto se tiene $\mathsf{tr}\left(\rho^2\right) < 1$.

1.2.3. Postulados de la mecánica cuántica sobre matrices de densidad

Los cuatro postulados de la mecánica cuántica definen la semántica de la representación de los estados de qubits mediante matrices de densidad.

Postulado de representación

El primer postulado dice que el estado de un sistema puede ser completamente descripto por una matriz de densidad.

Postulado de evolución

El segundo postulado establece la manera de cambiar el estado de un sistema, mediante operadores de evolución. Estos son representados mediante matrices unitarias U de dimensión correspondiente, y su forma de actuar sobre el estado de un sistema descripto por la matriz de densidad ρ es $U\rho U^\dagger$. Esto significa que antes de aplicar el operador U el estado del sistema estaba descripto por la matriz ρ y luego de aplicarlo el estado está descripto por la matriz de densidad $U\rho U^\dagger$. Esta matriz cumple con la definición de matriz de densidad porque U es una matriz unitaria, de acuerdo al teorema (1.1.14). Además por ser U unitaria es inversible, con inversa $U^\dagger$ también unitaria. Esto significa que las evoluciones de estados son reversibles, pudiendo aplicarse el operador inverso para recuperar el estado original.

Postulado de medición

El tercer postulado establece la forma de obtener información del sistema, actuando sobre él. En esta tesis vamos a considerar la medición de qubits sobre la base canónica, por lo tanto la información que podemos obtener de los sistemas van a ser combinaciones de valores 0 y 1. En un caso más general se podría medir sobre una base arbitraria, lo cual sería equivalente a realizar una rotación mediante una evolución unitaria del sistema y luego medir en la base canónica.

Al medir el valor de un qubit en superposición respecto a la base canónica habrá distintas probabilidades de obtener 0 o 1. Además el estado del qubit se verá afectado, quedando colapsado al estado representante del valor obtenido. Es decir que una vez que un qubit es medido, sucesivas mediciones obtendrán el mismo resultado que la primera vez (si no hay evoluciones intermedias).

Los operadores de medición, en el caso general, son conjuntos de proyectores sobre los subespacios de los autovectores asociados al observable (representado por una matriz) que se quiere medir. En el caso de los qubits, para esta tesis nos restringimos a medir su valor como 0 o 1, valores para los cuales los subespacios asociados se generan mediante los vectores $|0\rangle$ y $|1\rangle$. La acción de proyectar el estado sobre un subespacio en general afecta al estado, y cambia su traza. Por lo tanto es necesario renormalizar las matrices luego de ser medidas.

El proyector sobre el subespacio asociado al valor 0 es $\pi_0 = |0\rangle\langle 0|$, y el asociado al valor 1 es $\pi_1 = |1\rangle\langle 1|$. Por lo tanto se define el operador de medición de un qubit como el conjunto $\pi^1 = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. Si se tiene un sistema de un qubit cuyo estado está descripto por la matriz de densidad ρ, la probabilidad de obtener el valor 0 al medir está dada por $\mathsf{tr}(\pi_0 \rho \pi_0^\dagger)$ y la probabilidad de obtener el valor 1 está dada por $\mathsf{tr}(\pi_1 \rho \pi_1^\dagger)$. Si al medir se obtiene 0, el estado del sistema pasa a estar descripto por ρ_0, y si se obtiene 1 pasa a estar descripto por ρ_1:

$$\rho_0 = \frac{\pi_0 \rho \pi_0^\dagger}{\mathsf{tr}(\pi_0 \rho \pi_0^\dagger)} \qquad \rho_1 = \frac{\pi_1 \rho \pi_1^\dagger}{\mathsf{tr}(\pi_1 \rho \pi_1^\dagger)}$$

Por ejemplo, para un qubit cuyo estado está descripto por la matriz de densidad $|+\rangle\langle +|$ la probabilidad de obtener 0 o 1 al medirlo es la misma:

$$P(0) = \mathsf{tr}(\pi_0 |+\rangle\langle +| \pi_0^\dagger) = \tfrac{1}{2}\mathsf{tr}\left(|0\rangle\langle 0|\right) = \tfrac{1}{2}$$
$$P(1) = \mathsf{tr}(\pi_1 |+\rangle\langle +| \pi_1^\dagger) = \tfrac{1}{2}\mathsf{tr}\left(|1\rangle\langle 1|\right) = \tfrac{1}{2}$$

Las matrices de densidad correspondientes luego de cada medición son:

$$\rho_0 = |0\rangle\langle 0| \qquad \rho_1 = |1\rangle\langle 1|$$

Si se tiene un sistema compuesto por n qubits y se los mide a todos a la vez, los resultados posibles de esta medición son las 2^n posibles combinaciones de 0 y 1. Esto define 2^n proyectores distintos.

Por ejemplo, en un sistema de dos qubits los resultados posibles serán las combinaciones 00, 01, 10 y 11 de valores para el primer y segundo qubit respectivamente. Los proyectores correspondientes a estos posibles resultados se definen como $\pi_{00} = |00\rangle\langle 00|$,

$\pi_{01} = |01\rangle\langle 01|$, $\pi_{10} = |10\rangle\langle 10|$ y $\pi_{11} = |11\rangle\langle 11|$. De esta manera se define el operador de medición para dos qubits como el conjunto $\pi^2 = \{\pi_{00}, \pi_{01}, \pi_{10}, \pi_{11}\}$. La medición se lleva a cabo de la misma manera que en el caso de un qubit, sólo que con cuatro resultados posibles.

Una diferencia respecto a la evolución es que la proyección no es una operación reversible. Los proyectores no son matrices inversibles y por lo tanto una vez que la medición se lleva a cabo, sea cual sea el operador que se terminó aplicando (correspondiente al resultado obtenido) el estado previo a la medición no puede recuperarse.

Postulado de composición

El cuarto postulado establece la manera de describir dos sistemas al mismo tiempo. Esto se hace mediante el producto tensorial, de forma que si ρ describe el primer sistema y ρ' describe el segundo, la matriz de densidad que describe el sistema compuesto por los dos es $\rho \otimes \rho'$.

Por ejemplo si se tienen dos sistemas de un qubit cada uno cuyos estados están descriptos por las matrices $|0\rangle\langle 0|$ y $|1\rangle\langle 1|$ respectivamente, usando la propiedad de producto mixto, se tiene que el sistema conjunto está descripto por:

$$|0\rangle\langle 0| \otimes |1\rangle\langle 1| = (|0\rangle \otimes |1\rangle)(\langle 0| \otimes \langle 1|) = |01\rangle\langle 01|$$

Si se quiere agregar un tercer qubit cuyo estado está descripto por $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, el estado conjunto de los tres qubits estará representado por:

$$\begin{aligned} |01\rangle\langle 01| \otimes (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|) &= |01\rangle\langle 01| \otimes \tfrac{1}{2}|0\rangle\langle 0| + |01\rangle\langle 01| \otimes \tfrac{1}{2}|1\rangle\langle 1| \\ &= \tfrac{1}{2}(|01\rangle \otimes |0\rangle)(\langle 01| \otimes \langle 0|) + \tfrac{1}{2}(|01\rangle \otimes |1\rangle)(\langle 01| \otimes \langle 1|) \\ &= \tfrac{1}{2}|010\rangle\langle 010| + \tfrac{1}{2}|011\rangle\langle 011| \end{aligned}$$

1.2.4. Teorema de no clonado

Dado un sistema de dos qubits, supongamos que existe una operación que copia el estado del primero en el segundo, es decir:

$$|\psi\rangle \otimes |s\rangle \longmapsto |\psi\rangle \otimes |\psi\rangle$$

Dicha operación no sería reversible para estados arbitrarios. Por lo tanto, no existe ningún operador unitario que la pueda llevar a cabo. Por otra parte tampoco se podría realizar una copia usando mediciones, ya que estas colapsarían el estado sin llegar a caracterizarlo por completo.

Esto significa que dicha operación de copia no puede realizarse, lo cual presenta una restricción adicional en cualquier sistema de computación cuántico en comparación con los clásicos. Los estados arbitrarios no pueden ser duplicados ni medidos más de una vez sin ser destruidos.

Este teorema no prohíbe la creación de diversos qubits en estados conocidos, sino solamente la clonación a ciegas del estado de un qubit. Es posible crear tantos qubits en un mismo estado determinado como se quiera.

Teorema 1.2.1 (No clonado)**.** *No existe ningún operador unitario U tal que para cualquier vector de estado desconocido $|\psi\rangle$ y algún estado inicial $|s\rangle$ se cumpla*

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Demostración. De [NC11, Box 12.1]:

Supongo que tal operador U existe, entonces en particular para los estados puros $|\psi\rangle$ y $|\varphi\rangle$ vale

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

Por lo tanto,

$$(U(|\psi\rangle \otimes |s\rangle))^\dagger U(|\varphi\rangle \otimes |s\rangle) = (|\psi\rangle \otimes |\psi\rangle)^\dagger |\varphi\rangle \otimes |\varphi\rangle$$
$$(\langle\psi| \otimes \langle s|)U^\dagger U(|\varphi\rangle \otimes |s\rangle) = (\langle\psi| \otimes \langle\psi|)(|\varphi\rangle \otimes |\varphi\rangle)$$
$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2$$

Entonces se tiene que $\langle\psi|\varphi\rangle$ vale o bien 0 o bien 1. En el primer caso esto implica que $|\psi\rangle$ y $|\varphi\rangle$ son ortogonales, y en el segundo que son iguales. Por lo tanto U sólo podría clonar estados ortogonales entre sí, y no serviría en el caso general. □

1.2.5. Compuertas lógicas cuánticas

Las compuertas lógicas cuánticas son ejemplos de operadores unitarios de evolución. Su aplicación sobre uno o más qubits cambia su estado, y su aplicación sobre una mezcla probabilística de estados cambia independientemente a cada uno de ellos. Son el análogo cuántico a las compuertas lógicas que actúan sobre bits. Algunos ejemplos son:

***Compuerta* NOT**

Este operador es análogo a la compuerta lógica NOT, invirtiendo las probabilidades asociadas a los estados clásicos $|0\rangle$ y $|1\rangle$.

$$\mathsf{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Las matrices que describen sistemas en estados puros alineados con la base son invertidas mediante este operador.

$$\mathsf{NOT}\ |0\rangle\langle 0|\ \mathsf{NOT}^\dagger = |1\rangle\langle 1| \qquad \mathsf{NOT}\ |1\rangle\langle 1|\ \mathsf{NOT}^\dagger = |0\rangle\langle 0|$$

El operador no tiene efecto sobre el estado del sistema descripto por la matriz $|+\rangle\langle +|$.

$$\mathsf{NOT}\ |+\rangle\langle +|\ \mathsf{NOT}^\dagger = \tfrac{1}{2}\ \mathsf{NOT}\ (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|)\ \mathsf{NOT}^\dagger = |+\rangle\langle +|$$

Compuerta de Hadamard

Este operador rota el estado $|0\rangle$ a $|+\rangle$ y el estado $|1\rangle$ a $|-\rangle$.

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

Se tiene que $H^2 = I$, por lo tanto dos aplicaciones consecutivas de este operador devuelven el estado original.

$$H\ |0\rangle\langle 0|\ H^\dagger = |+\rangle\langle +| \qquad H\ |1\rangle\langle 1|\ H^\dagger = |-\rangle\langle -|$$

$$H\ |+\rangle\langle +|\ H^\dagger = |0\rangle\langle 0| \qquad H\ |-\rangle\langle -|\ H^\dagger = |1\rangle\langle 1|$$

***Compuerta* CNOT**

Este es el operador de NOT controlado. Actúa sobre dos qubits, aplicando el operador NOT al segundo si y sólo si el estado del primer bit es $|1\rangle$, pero sin realizar una medición.

$$\mathsf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Cuando el estado del primer qubit es $|1\rangle$, el estado del segundo qubit se invierte.

$$\mathsf{CNOT}\ |10\rangle\langle 10|\ \mathsf{CNOT}^\dagger = |11\rangle\langle 11| \qquad \mathsf{CNOT}\ |11\rangle\langle 11|\ \mathsf{CNOT}^\dagger = |10\rangle\langle 10|$$

Cuando el estado del primer qubit es $|0\rangle$, el estado del segundo qubit no cambia.

$$\mathsf{CNOT}\ |00\rangle\langle 00|\ \mathsf{CNOT}^\dagger = |00\rangle\langle 00| \qquad \mathsf{CNOT}\ |01\rangle\langle 01|\ \mathsf{CNOT}^\dagger = |01\rangle\langle 01|$$

Operadores de Pauli

Las matrices de Pauli son operadores que forman una base de las matrices hermíticas en $\mathbb{C}^{2\times 2}$ sobre $\mathbb{R}$, es decir que cualquier operador que actúe sobre un qubit se puede descomponer en una combinación lineal real de estos tres. Notar que $\sigma_x = \mathsf{NOT}$.

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

σ_z opera de forma análoga a NOT en la base de Hadamard, es decir $\sigma_z|+\rangle = |-\rangle$ y $\sigma_z|-\rangle = |+\rangle$. Además se tiene que $\sigma_y = i\sigma_x\sigma_z$.

En mecánica cuántica estas matrices representan los observables asociados a cada una de las 3 dimensiones del spin de una partícula, por ejemplo el electrón.

Los operadores unitarios se pueden expandir con identidades o combinar con otros operadores unitarios mediante el producto tensorial, ya que según el lema (1.1.13) estos productos son unitarios. De esta manera pueden aplicarse simultáneamente varias transformaciones unitarias en diferentes subsistemas de los representados por una matriz de densidad.

Por ejemplo, una manera de conseguir un estado entrelazado de dos qubits es mediante la aplicación sucesiva del operador de Hadamard al primer qubit y la compuerta CNOT a un sistema descripto por $|00\rangle\langle 00|$. El operador unitario de evolución que aplica la compuerta de Hadamard al primer qubit y no actúa sobre el segundo es $(H \otimes I_2)$. Entonces se tiene:

$$\begin{aligned} \mathsf{CNOT}\ (H \otimes I_2)\ |00\rangle\langle 00|\ (H \otimes I_2)^\dagger\ \mathsf{CNOT}^\dagger &= \mathsf{CNOT}\ (H|0\rangle \otimes |0\rangle)(\langle 0|H^\dagger \otimes \langle 0|)\ \mathsf{CNOT}^\dagger \\ &= \mathsf{CNOT}\ (|+\rangle \otimes |0\rangle)(\langle +| \otimes \langle 0|)\ \mathsf{CNOT}^\dagger \\ &= \mathsf{CNOT}\ (|+\rangle\langle +| \otimes |0\rangle\langle 0|)\ \mathsf{CNOT}^\dagger \\ &= \tfrac{1}{2}\ \mathsf{CNOT}\ (|00\rangle + |10\rangle)(\langle 00| + \langle 10|)\ \mathsf{CNOT}^\dagger \\ &= \tfrac{1}{2}\ (|00\rangle + |11\rangle)(\langle 00| + \langle 11|) \end{aligned}$$

1.2.6. Operadores de medición extendidos

Dado un sistema de n qubits se pueden definir distintos operadores de medición, dependiendo de cuáles qubits se quiera medir. Si se quieren medir los primeros m qubits del sistema, se define la siguiente notación para $0 \leq i \leq 2^m - 1$, dado el proyector π_i sobre $\mathbb{C}^{2^m}$:

$$\overline{\pi_i} := \pi_i \otimes I_{2^{n-m}}$$

donde cada uno de los $\overline{\pi_i}$ corresponde a cada uno de los resultados posibles en la medición de los primeros m qubits. La notación $\overline{\pi_i}$ es ambigua ya que no se explicita la dimensión del espacio al que pertenece, sin embargo esto estará claro por el contexto.

Por ejemplo, tomando el caso $n = 2$ y $m = 1$ esto significa que se mide el primer qbit de un sistema de dos qbits, y los operadores definidos son entonces:

$$\overline{\pi_0} = |0\rangle\langle 0| \otimes I_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \overline{\pi_1} = |1\rangle\langle 1| \otimes I_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

En el caso de $n = 2$ y $m = 2$, se definen:

$$\overline{\pi_0} = |00\rangle\langle 00| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \overline{\pi_1} = |01\rangle\langle 01| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\overline{\pi_2} = |10\rangle\langle 10| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \overline{\pi_3} = |11\rangle\langle 11| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Por definición resulta que los $\overline{\pi_i}$ son proyectores ortogonales en $\mathbb{C}^{2^n \times 2^n}$. Esto significa que son matrices diagonales con 1 y 0 en la diagonal. En el caso general la forma de $\overline{\pi_i}$ es:

$$\overline{\pi_i} = \begin{pmatrix} \boxed{\mathbb{0}} & & & & \\ & \ddots & & & \\ & & \boxed{\mathbb{1}} & & \\ & & & \ddots & \\ & & & & \boxed{\mathbb{0}} \end{pmatrix}$$

Es decir que $\overline{\pi_i}$ es una matriz diagonal en $\mathbb{R}^{2^n \times 2^n}$ formada por 2^m bloques de matrices en $\mathbb{R}^{2^{n-m} \times 2^{n-m}}$, todos nulos excepto el i-ésimo que es igual a la identidad.

Como es diagonal y real, se tiene que $\overline{\pi_i}^\dagger = \overline{\pi_i}$ para todo i, n y m; es una matriz hermítica.

También es posible combinar los operadores de medición con identidades en cualquier orden. Por la propiedad de producto mixto, sólo se proyectarán las partes del estado correspondientes a los qubits seleccionados para medir. Por ejemplo, para medir el segundo

qubit en un sistema de tres qubits, los operadores correspondientes a los dos resultados posibles son $I_2 \otimes \pi_0 \otimes I_2$ y $I_2 \otimes \pi_1 \otimes I_2$.

Usando estos proyectores extendidos se pueden realizar mediciones parciales en los sistemas. Esto permite ver un ejemplo de las consecuencias del entrelazamiento entre qubits.

Sea un sistema de dos qubits entrelazados, cuyo estado está descripto por la matriz $\rho = \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)$. Se realiza una medición sobre el primer qubit. Si el resultado obtenido es 0, el estado del sistema luego de la medición está dado por ρ_0 y en caso contrario por ρ_1:

$$\rho_0 = \frac{\overline{\pi_0}\rho\overline{\pi_0}^\dagger}{\mathsf{tr}\left(\overline{\pi_0}\rho\overline{\pi_0}^\dagger\right)} = (\pi_0 \otimes I_2)\ (|00\rangle + |11\rangle)(\langle 00| + \langle 11|)\ (\pi_0 \otimes I_2)^\dagger = |00\rangle\langle 00|$$

$$\rho_1 = \frac{\overline{\pi_1}\rho\overline{\pi_1}^\dagger}{\mathsf{tr}\left(\overline{\pi_1}\rho\overline{\pi_1}^\dagger\right)} = (\pi_1 \otimes I_2)\ (|00\rangle + |11\rangle)(\langle 00| + \langle 11|)\ (\pi_1 \otimes I_2)^\dagger = |11\rangle\langle 11|$$

Si luego de realizar esta medición se quiere realizar otra sobre el segundo qubit usando $I_2 \otimes \pi_0$ y $I_2 \otimes \pi_1$, se puede ver que según el estado del sistema esté descripto por ρ_0 o por ρ_1, este tendrá probabilidad 1 de valer 0 o 1, respectivamente. Sin embargo, cuando el sistema estaba en su estado inicial descripto por ρ, las probabilidades de que el segundo qubit valiera 0 o 1 valían $\frac{1}{2}$. Esto significa que la medición realizada sobre el primer qubit afectó el estado de ambos.

A continuación se demuestran unos lemas que van a ser útiles más adelante. El primero dice que cuando se realizan todas las mediciones posibles para un m fijo usando los operadores de medición extendidos y sobre una matriz positiva, se conserva la traza de la matriz original. Esto es necesario ya que en el cálculo con punto fijo los dominios van a estar definidos sobre matrices positivas, con cotas sobre la traza pero sin un valor específico para esta. Que la traza no varíe al considerar todas las mediciones posibles es equivalente a considerar que se están examinando todos los caminos posibles.

Lema 1.2.2. *Sea ρ una matriz en $\mathcal{P}_{2^n}$. Entonces vale que* $\mathsf{tr}\left(\bigoplus_{i=0}^{2^m-1}\left(\overline{\pi_i}\rho\overline{\pi_i}^\dagger\right)\right) = \mathsf{tr}\,(\rho)$ *para todo $m \leq n$.*

Demostración. Primero, distribuyendo, se tiene que

$$\mathsf{tr}\left(\bigoplus_{i=0}^{2^m-1}\left(\overline{\pi_i}\rho\overline{\pi_i}^\dagger\right)\right) = \sum_{i=0}^{2^m-1}\mathsf{tr}\left(\overline{\pi_i}\rho\overline{\pi_i}^\dagger\right)$$

Por la propiedad cíclica de la traza, esto resulta igual a $\sum_{i=0}^{2^m-1}\mathsf{tr}\left(\rho\overline{\pi_i}^\dagger\overline{\pi_i}\right)$. Como $\overline{\pi_i}$ es hermítica y además es un proyector, se tiene que $\overline{\pi_i}^\dagger\overline{\pi_i} = \overline{\pi_i}$, y el término resulta igual a $\sum_{i=0}^{2^m-1}\mathsf{tr}\,(\rho\overline{\pi_i})$. Como $\sum_{i=0}^{2^m-1}\overline{\pi_i} = \mathbb{1}_{2^n}$:

$$\sum_{i=0}^{2^m-1}\mathsf{tr}\,(\rho\overline{\pi_i}) = \mathsf{tr}\left(\sum_{i=0}^{2^m-1}\rho\overline{\pi_i}\right) = \mathsf{tr}\left(\rho\sum_{i=0}^{2^m-1}\overline{\pi_i}\right) = \mathsf{tr}\,(\rho)$$

□

Corolario 1.2.3. *Sea ρ una matriz en $\mathcal{P}_{2^n}$. Para todo $m \leq n$ y $0 \leq i \leq 2^m - 1$ se tiene que* $\mathsf{tr}\left(\overline{\pi_i}\rho\overline{\pi_i}^\dagger\right) \leq \mathsf{tr}\left(\rho\right)$.

Demostración. Se obtiene acotando cada término de la sumatoria por separado. □

También se tiene el resultado de que las matrices positivas, luego de ser medidas con los operadores extendidos, siguen siendo positivas.

Lema 1.2.4. *Sea $\rho \in \mathcal{P}_{2^n}$, tal que* $\mathsf{tr}\left(\rho\right) \leq 1$. *Entonces para todo $m \leq n$, para todo $0 \leq i \leq 2^m - 1$ se tiene que $\overline{\pi_i}\rho\overline{\pi_i}^\dagger$ es positiva y tiene traza acotada por 1.*

Demostración.

- $\overline{\pi_i}\rho\overline{\pi_i}^\dagger$ es hermítica: se tiene $(\overline{\pi_i}\rho\overline{\pi_i}^\dagger)^\dagger = \overline{\pi_i}\rho^\dagger\overline{\pi_i}^\dagger$ por propiedad del operador †. Esto es igual a $\overline{\pi_i}\rho\overline{\pi_i}^\dagger$ porque ρ es hermítica por hipótesis.
- $\overline{\pi_i}\rho\overline{\pi_i}^\dagger$ es positiva: multiplicando a ambos lados por un vector u en $\mathbb{C}^{2^n}$ se tiene que $u^\dagger\overline{\pi_i}\rho\overline{\pi_i}^\dagger u = (u^\dagger\overline{\pi_i})\rho(\overline{\pi_i}^\dagger u)$. Llamando $v = \overline{\pi_i}^\dagger u \in \mathbb{C}^{2^n}$ se tiene que $v^\dagger = (\overline{\pi_i}^\dagger u)^\dagger = u^\dagger\overline{\pi_i}$. Por lo tanto $(u^\dagger\overline{\pi_i})\rho(\overline{\pi_i}^\dagger u) = v^\dagger\rho v \geq 0$ por positividad de ρ.
- La traza de $\overline{\pi_i}\rho\overline{\pi_i}^\dagger$ está acotada por 1: usando el corolario (1.2.3) se tiene que $\mathsf{tr}\left(\overline{\pi_i}\rho\overline{\pi_i}^\dagger\right) \leq \mathsf{tr}\left(\rho\right) \leq 1$. □

2. ESTADO DEL ARTE

Este capítulo presenta los cálculos λ_ρ y λ_ρ° de [DC17], donde la información sobre los sistemas está dada en términos de matrices de densidad. El cálculo λ_ρ es de control clásico y reescritura probabilística, donde las reescrituras con probabilidades distintas de 1 están relacionadas a las mediciones de qubits. El cálculo λ_ρ° no es de reescritura probabilística, pero su control está basado en las probabilidades de las distintas mediciones de qubits.

Al final del capítulo se presentan algunas propiedades de estos cálculos. En [DC17] se demuestra que ambos cálculos cumplen subject reduction y que se pueden interpretar con una única semántica, en [Rom20] se demuestra que son fuertemente normalizantes y confluentes y en [Bor19] se demuestra cierta equivalencia de λ_ρ con el lambda cálculo cuántico λ_q definido en [SV05].

2.1. Cálculo con control clásico y reescritura probabilística

La sintaxis de λ_ρ, en la figura (2.1), está dividida en tres categorías:

- Los términos correspondientes al lambda cálculo usual con variables y abstracciones.
- Cuatro términos correspondientes cada uno a los postulados de mecánica cuántica: representación mediante matrices de densidad, evolución mediante un operador unitario, medición en la base canónica y composición de sistemas.
- Dos términos que determinan el control clásico: (b^m, ρ^n) describe el resultado de una medición, donde b^m es el valor obtenido y ρ^n es la matriz de densidad que describe el estado del sistema luego de dicha medición; y el término de $\mathsf{letcase}$ que controla la ejecución de acuerdo a un par correspondiente a una medición.

$$t := x \mid \lambda x.t \mid tt \qquad \text{(Lambda cálculo estándar)}$$

$$\mid \rho^n \mid U^n t \mid \pi^n t \mid t \otimes t \qquad \text{(Postulados cuánticos)}$$

$$\mid (b^m, \rho^n) \mid \mathsf{letcase}\ x = r\ \mathsf{in}\ \{t, \ldots, t\} \qquad \text{(Control clásico)}$$

donde:
– $n, m \in \mathbb{N}, m \leq n$.
– ρ^n es una matriz de densidad de n qubits.
– $b^m \in \mathbb{N}, 0 \leq b^m < 2^m$.
– $\{t, \ldots, t\}$ contiene 2^m términos.
– U^n es un operador unitario de dimensión $2^n \times 2^n$.
– $\pi^n = \{\pi_0, \ldots, \pi_{2^n-1}\}$, describe una medición cuántica en la base canónica, donde cada π_i es un proyector.

Fig. 2.1: Sintaxis de λ_ρ

El sistema de reescritura para λ_ρ está dado en la figura (2.2), donde la relación $r \longrightarrow_p s$ determina que r reduce a s con probabilidad p. Cuando el operador U^m, que afecta a m qubits, se usa para evolucionar un sistema representado por ρ^n con $m \leq n$, éste es aplicado a los primeros m qubits del sistema. El operador que actúa sobre el sistema completo está extendido con identidades usando la notación $\overline{U^m} = U^m \otimes I_{2^{n-m}}$, definida en la sección (1.2.6). De forma similar π^m simboliza una medición de los primeros m qubits del sistema, que aplicada a la matriz de densidad ρ^n con $m \leq n$ corresponde a los proyectores $\pi_0 \otimes I_{2^{n-m}}, \ldots, \pi_{2^m-1} \otimes I_{2^{n-m}}$.

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

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

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

$$\rho \otimes \rho' \longrightarrow_1 \rho'' \text{ con } \rho'' = \rho \otimes \rho'$$

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

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

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

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

Fig. 2.2: Reglas de reducción de λ_ρ

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

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

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

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

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

Fig. 2.3: Sistema de tipos de λ_ρ

El sistema de tipos de λ_ρ, en la figura (2.3), es afín. Esto significa que las variables

sólo podrán ser usadas una vez, cumpliendo de esta forma con el teorema de no clonado. Hay un solo caso en el que se permite compartir variables, que es en el de la x ligada por el letcase. Esto no rompe no clonado ya que sólo una de las ramas posibles será la que continúe la reducción.

2.2. Cálculo con control probabilístico y reescritura no probabilística

El cálculo λ_ρ° es una versión alternativa de λ_ρ, donde se permiten las combinaciones lineales de términos. Luego de una medición, el sistema pasa a un estado mixto, aprovechando así la descripción en términos de matrices de densidad.

Su sintaxis modificada, dada en la figura (2.4), permite la combinación lineal de términos pesada por probabilidades. Además, en este cálculo no existe el término correspondiente al resultado de una medición, porque todos los resultados posibles son considerados a la vez en el $\mathsf{letcase}^\circ$.

$$t := x \mid \lambda x.t \mid tt \qquad \text{(Lambda cálculo estándar)}$$

$$\mid \rho^n \mid U^n t \mid \pi^n t \mid t \otimes t \qquad \text{(Postulados cuánticos)}$$

$$\mid \textstyle\sum_{i=1}^n p_i t_i \mid \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t, \ldots, t\} \qquad \text{(Control probabilístico)}$$

donde $p_i \in (0, 1], \sum_{i=1}^n p_i = 1$, y $\sum$ es considerada módulo asociatividad y conmutatividad.

Fig. 2.4: Sintaxis de λ_ρ°

El sistema de reescritura para λ_ρ° está dado por la relación $\rightsquigarrow$ en la figura (2.6). En este caso la medición no reduce, excepto como parámetro del $\mathsf{letcase}^\circ$. Las probabilidades de cada resultado son usadas entonces para combinar los términos tomados como parámetro.

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

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

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

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

$$\frac{x : n \Vdash t_0 : A \quad \ldots \quad x : n \Vdash t_{2^m - 1} : A \quad \Gamma \Vdash r : (m, n)}{\Gamma \Vdash \mathsf{letcase}\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} : A}\ \mathsf{m_e}$$

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

Fig. 2.5: Sistema de tipos de λ_ρ°

$$(\lambda x.t)r \rightsquigarrow t[x := r]$$

$$\mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \rightsquigarrow \sum_{i=0}^{2^m-1} p_i t_i[x := \rho_i^n]\ \mathrm{con}\ \begin{cases} p_i = \mathsf{tr}\left(\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger\right) \\ \rho_i^n = \frac{\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger}{p_i} \end{cases}$$

$$U^m\rho^n \rightsquigarrow \rho'^n\ \mathrm{con}\ \rho'^n = \overline{U^m}\rho^n\overline{U^m}^\dagger$$

$$\rho \otimes \rho' \rightsquigarrow \rho''\ \mathrm{con}\ \rho'' = \rho \otimes \rho'$$

$$\sum_i p_i\rho_i \rightsquigarrow \rho'\ \mathrm{con}\ \rho' = \sum_i p_i\rho_i$$

$$\sum_i p_i t \rightsquigarrow t$$

$$(\sum_i p_i t_i)r \rightsquigarrow \sum_i p_i(t_i r)$$

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

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

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

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

Fig. 2.6: Reglas de reducción de λ_ρ°

El sistema de tipos para λ_ρ° está dado en la figura (2.5). Las únicas diferencias con el sistema de tipos de λ_ρ están en la nueva regla para tipar combinaciones lineales y en que se saca la regla que tipaba los resultados de mediciones (b^m, ρ^n), que ya no están en la sintaxis. El sistema de tipos en λ_ρ° deja de ser estrictamente afín, ya que permite compartir variables entre las ramas del $\mathsf{letcase}^\circ$ y por lo tanto entre las ramas de sumatorias, por ser una generalización de λ_ρ.

Ejemplo 2.2.1. Este ejemplo muestra la reducción de un término en λ_ρ, usando las reglas de producto tensorial y aplicación de operadores unitarios. Notar que la reducción de este término es igual en λ_ρ° considerando la relación $\rightsquigarrow$, ya que las reglas aplicadas para este caso son las mismas en ambos cálculos.

$$\begin{aligned} \mathsf{CNOT}^2\ (H^1\ (|0\rangle\langle 0| \otimes |0\rangle\langle 0|)) &\longrightarrow_1 \mathsf{CNOT}^2\ (H^1\ |00\rangle\langle 00|) \\ &\longrightarrow_1 \mathsf{CNOT}^2\ (\tfrac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 10| + |10\rangle\langle 00| + |10\rangle\langle 10|)) \\ &\longrightarrow_1 \tfrac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) \end{aligned}$$

Ejemplo 2.2.2. El ejemplo de la figura (2.7) muestra las diferencias respecto a las reducciones de mediciones y letcase en ambos lenguajes, para un término análogo.

En el caso de λ_ρ el término reduce probabilísticamente y tiene 3 trazas posibles. El término $\pi^1|+\rangle\langle+|$ reduce con probabilidad $\frac{1}{2}$ a $(0, |0\rangle\langle 0|)$ y con probabilidad $\frac{1}{2}$ a $(1, |1\rangle\langle 1|)$.

Luego, según cuál sea el resultado obtenido, el término de letcase reduce con probabilidad 1 al término entre llaves correspondiente al resultado obtenido en la medición.

En el caso de λ_ρ° la reducción no es probabilística. El término $\pi^1|+\rangle\langle+|$ no reduce solo sino adentro del letcase$^\circ$, el cual reduce a una combinación lineal probabilística de los resultados posibles.

Se observa que el resultado conjunto de las trazas de la reducción en λ_ρ es equivalente al resultado de la reducción en λ_ρ°.

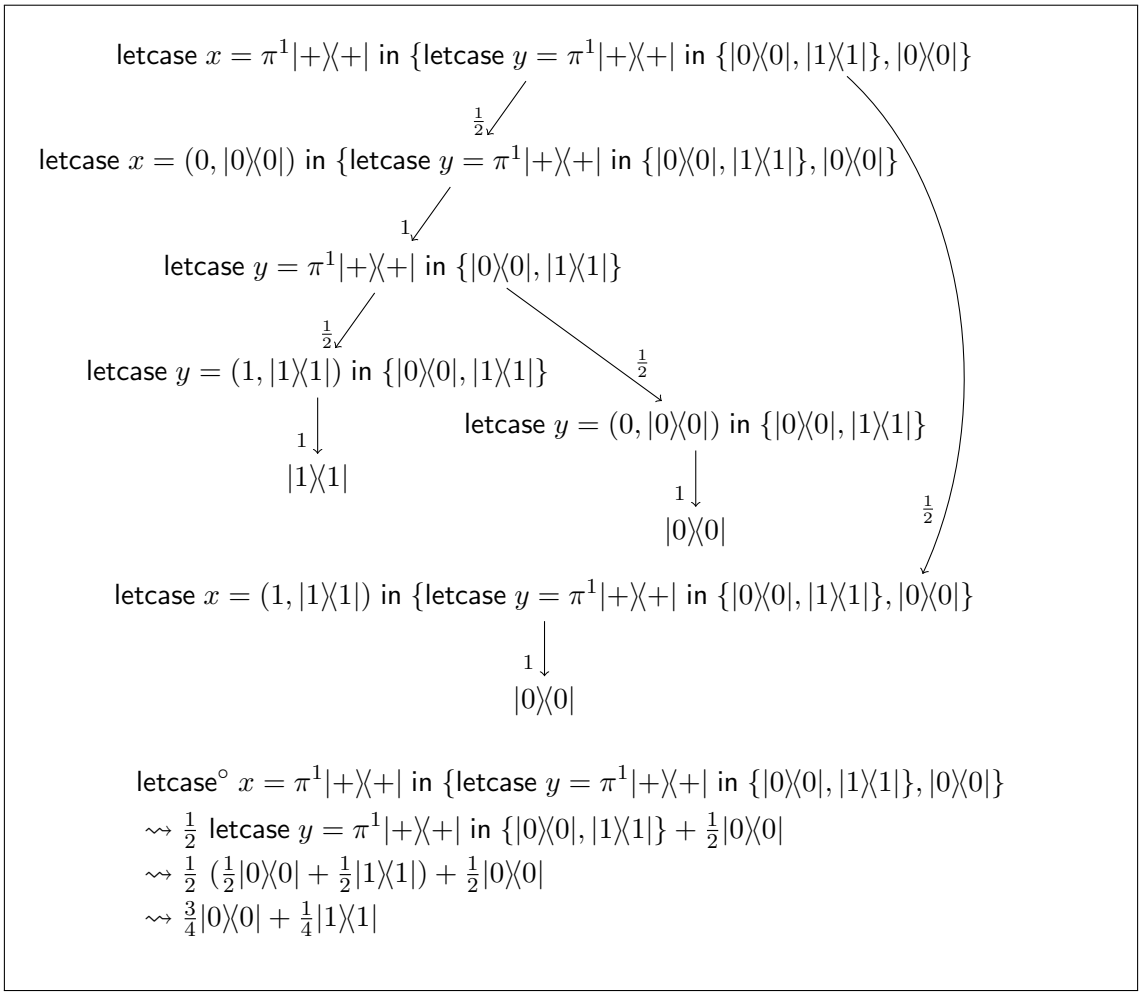

Fig. 2.7: Comparación de la reducción de dos términos análogos en λ_ρ y λ_ρ°

2.3. Propiedades de los cálculos

Subject reduction

Para ambos cálculos se tiene que vale subject reduction [DC17, Lema 4.4].

Lema (Subject reduction en λ_ρ y λ_ρ°)**.**

- *Si* $\Gamma \vdash t : A$, *y* $t \longrightarrow_p r$, *entonces* $\Gamma \vdash r : A$.
- *Si* $\Gamma \Vdash t : A$, *y* $t \rightsquigarrow r$, *entonces* $\Gamma \Vdash r : A$.

Equivalencia con λ_q

λ_q es una extensión cuántica de cálculo lambda introducida en [SV05]. Esta extensión se encuentra dentro del paradigma de datos cuánticos y control clásico, al igual que λ_ρ. Fue usado como base para el lenguaje de programación cuántico Quipper [GLR+13]. Borgna demuestra en [Bor19] cierta equivalencia entre λ_ρ y λ_q.

Normalización fuerte

Romero demuestra normalización fuerte para una extensión polimórfica de λ_ρ [Rom20, Teorema 4.3.5] y para una extensión polimórfica de λ_ρ° [Rom20, Teorema 4.3.8]. Ambas implican normalización fuerte en los cálculos sin extender. Además mediante la equivalencia de λ_ρ con λ_q también se demuestra su normalización fuerte en [Bor19, Corolario 3.1.10].

Teorema (Normalización fuerte en λ_ρ y λ_ρ°)**.** *Los términos bien tipados de λ_ρ y λ_ρ° son fuertemente normalizantes, es decir que no pueden reducir infinitamente.*

Confluencia

Ambos cálculos son confluentes. La extensión polimórfica de λ_ρ° es localmente confluente [Rom20, Teorema 4.4.4], por lo tanto el cálculo no extendido también lo es. Además según el análisis de los pares críticos de la extensión polimórfica de λ_ρ en [Rom20, Sección 4.4.2], aunque su extensión no es localmente confluente, el cálculo original sí lo es. Como ambos cálculos son fuertemente normalizantes el lema de Newman [Ter03, Teorema 1.2.1] implica la confluencia global.

La confluencia probabilística necesaria para el caso de λ_ρ está definida en [Mar17]. La idea intuitiva es que tomando todos los caminos posibles de reducción, siempre se llega a la misma distribución de probabilidad de términos. Además la composición de la relación de reescritura multiplica las probabilidades, es decir que si $r \longrightarrow_p s$ y $s \longrightarrow_{p'} t$, entonces $r \longrightarrow^*_{pp'} t$.

Teorema (Confluencia local de λ_ρ y λ_ρ°)**.**

- *Sea t un término bien tipado de λ_ρ. Para todo s, s', p, p' tales que $t \longrightarrow_p s$ y $t \longrightarrow_{p'} s'$, s y s' reducen a la misma distribución probabilística de términos.*
- *Sea t un término bien tipado de λ_ρ°. Para todo s, s' tales que $t \rightsquigarrow s$ y $t \rightsquigarrow s'$ existe r tal que $s \rightsquigarrow^* r$ y $s' \rightsquigarrow^* r$.*

Teorema (Confluencia global de λ_ρ y λ_ρ°)**.**

- *Sea t un término bien tipado de λ_ρ. Para todo s, s', p, p' tales que $t \longrightarrow^*_p s$ y $t \longrightarrow^*_{p'} s'$, s y s' reducen a la misma distribución probabilística de términos.*
- *Sea t un término bien tipado de λ_ρ°. Para todo s, s' tales que $t \rightsquigarrow^* s$ y $t \rightsquigarrow^* s'$ existe r tal que $s \rightsquigarrow^* r$ y $s' \rightsquigarrow^* r$.*

3. SINTAXIS DEL CÁLCULO CON PUNTO FIJO

Los cálculos λ_ρ^μ y $\lambda_\rho^{\mu_n}$ son extensiones de λ_ρ° al cual se le agregan los términos y reglas de reducción necesarias para tener punto fijo y punto fijo incremental, respectivamente. Esto significa que en $\lambda_\rho^{\mu_n}$ habrá reducciones finitas que tienden al punto fijo, en una cantidad máxima de pasos fijada, mientras que en λ_ρ^μ no habrá normalización fuerte.

Ambas extensiones usan matrices de densidad generalizadas, donde la generalización implica que la restricción de $\mathsf{tr}(\rho) = 1$ que tenían las matrices de λ_ρ° pasa a ser $\mathsf{tr}(\rho) \leq 1$. Estas siguen siendo hermíticas y semidefinidas positivas, y son las matrices usadas en [Sel04]. Esta generalización es necesaria porque las reducciones intermedias del punto fijo pueden incluir términos no normalizados, como se verá en el ejemplo (3.1.1).

El cálculo incremental es necesario como paso intermedio al cálculo con punto fijo, ya que para poder definir la semántica del segundo es necesario demostrar la existencia de un límite en la semántica del primero.

En este capítulo se definen las reglas para estas extensiones y se demuestran los casos necesarios para ver que algunos resultados previos de λ_ρ° siguen valiendo en el cálculo incremental.

3.1. Sintaxis, reglas de tipado y de reducción

En la figura (3.1) se presenta la sintaxis del cálculo $\lambda_\rho^{\mu_n}$. Sus nuevos términos son $\mu_n x.t$, que representa el punto fijo incremental y $\bot_A$. Este término simboliza el elemento nulo de tipo A, y es necesario porque el punto fijo incremental reduce a partir de este término.

Además de estos nuevos términos se agregan las combinaciones lineales de términos con probabilidades que sumen menos que 1. Esto es porque al permitir matrices de densidad con trazas menores a 1 se necesita poder reducir los $\mathsf{letcase}^\circ$ correspondientes a sus mediciones.

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

donde $0 < p_i \leq 1$, $\sum_{i=1}^{n} p_i \leq 1$ y $\sum$ es considerado módulo asociatividad y conmutatividad.

Fig. 3.1: Sintaxis de $\lambda_\rho^{\mu_n}$

La sintaxis de λ_ρ^μ, en la figura (3.2), es igual a la de $\lambda_\rho^{\mu_n}$, excepto que sin el término $\bot_A$ y con el término de punto fijo no etiquetado por n, ya que este no es incremental. Este término es entonces de la forma $\mu x.t$.

$$t := x \mid \lambda x.t \mid tt \mid \mu x.t \qquad \text{(Lambda cálculo estándar)}$$

$$\mid \rho^n \mid U^n t \mid \pi^m t \mid t \otimes t \qquad \text{(Postulados cuánticos)}$$

$$\mid \sum_{i=1}^{n} p_i t_i \mid \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t, \ldots, t\} \qquad \text{(Control probabilístico)}$$

donde $0 < p_i \leq 1$, $\sum_{i=1}^{n} p_i \leq 1$ y $\sum$ es considerado módulo asociatividad y conmutatividad.

Fig. 3.2: Sintaxis de λ_ρ^μ

En la figura (3.3) se presentan las reglas de reducción del cálculo $\lambda_\rho^{\mu_n}$. Se agregaron las reglas de reducción correspondientes a los términos de punto fijo incremental y *bottom*.

La regla $pt + q\bot_A \rightsquigarrow pt$ permite la aparición de sumatorias con probabilidades menores que 1. La regla que simplificaba sumatorias del mismo término se modificó ya que ahora las probabilidades no necesariamente suman 1.

$$(\lambda x.t)r \rightsquigarrow t[x := r]$$

$$\mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \rightsquigarrow \sum_{i=0}^{2^m-1} p_i t_i[x := \rho_i^n] \text{ con } \begin{cases} \rho_i^n = \frac{\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger}{p_i} \\ p_i = \mathsf{tr}\left(\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger\right) \end{cases}$$

$$\mu_0 x.t \rightsquigarrow \bot_A \qquad \mu_{n+1} x.t \rightsquigarrow t[x := \mu_n x.t]$$

$$\bot_n \rightsquigarrow \mathbb{0}_{2^n} \qquad \bot_{(m,n)} \rightsquigarrow \pi^m \mathbb{0}_{2^n} \qquad \bot_{A \multimap B}\ t \rightsquigarrow \bot_B \qquad pt + q\bot_A \rightsquigarrow pt$$

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

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

$$\sum_i p_i \rho_i^n \rightsquigarrow \rho'^n \text{ con } \rho'^n = \sum_i p_i \rho_i^n$$

$$\sum_i (p_i t) \rightsquigarrow (\sum_i p_i) t \qquad (\sum_i p_i t_i) r \rightsquigarrow \sum_i p_i (t_i r)$$

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

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

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

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

Fig. 3.3: Reglas de reducción de $\lambda_\rho^{\mu_n}$

Se sacó la regla de reducción bajo lambda ya que en combinación con la reducción del punto fijo traía problemas con la validez de subject reduction sobre términos cerrados, a causa de la afinidad del sistema de tipos.

La diferencia respecto a las reglas de reducción de λ_ρ^μ, en la figura (3.4), es que las correspondientes a los términos $\mu_0 x.t$ y $\mu_{n+1} x.t$ en $\lambda_\rho^{\mu_n}$ se reemplazan por la única regla $\mu x.t \rightsquigarrow t[x := \mu x.t]$. Además desaparecen las reglas relacionadas con los términos $\bot_A$.

$$(\lambda x.t)r \rightsquigarrow t[x := r]$$

$$\mathsf{letcase}^\circ\ x = \pi^m \rho^n \ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \rightsquigarrow \sum_{i=0}^{2^m-1} p_i t_i[x := \rho_i^n] \text{ con } \begin{cases} \rho_i^n = \frac{\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger}{p_i} \\ p_i = \mathsf{tr}\left(\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger\right) \end{cases}$$

$$\mu x.t \rightsquigarrow t[x := \mu x.t]$$

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

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

$$\sum_i p_i \rho_i^n \rightsquigarrow \rho'^n \text{ con } \rho'^n = \sum_i p_i \rho_i^n$$

$$\sum_i (p_i t) \rightsquigarrow (\sum_i p_i)t \qquad (\sum_i p_i t_i)r \rightsquigarrow \sum_i p_i(t_i r)$$

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

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

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

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

Fig. 3.4: Reglas de reducción de λ_ρ^μ

En la figura (3.5) se presentan las reglas de tipado para el cálculo $\lambda_\rho^{\mu_n}$. Se define para ello la función ℓ sobre tipos como el último tipo a la derecha de la flecha, en forma recursiva.

$$\ell(n) = n$$
$$\ell((m, n)) = (m, n)$$
$$\ell(A \multimap B) = \ell(B)$$

Además de agregar las reglas μ_n y $\bot$ para tipar el punto fijo incremental y *bottom*, se modifican dos reglas de λ_ρ°:

- $+$ se modifica permitiendo tipar combinaciones lineales cuyas probabilidades sumen menos que 1, para poder tipar las nuevas combinaciones definidas por la sintaxis. Además ahora se prohíbe el tipado de sumatorias de mediciones. Este cambio fue hecho para facilitar las pruebas, pero además no restringe la expresividad del lenguaje.

En efecto, los términos de la forma $\pi^m t$, que representan mediciones, sólo se usan dentro de sus destructores $\mathsf{letcase}^\circ$. Los tipos que terminan en mediciones tampoco se pueden sumar ya que aplicarlos conduce a sumatorias de mediciones.

- m_e se modifica introduciendo contextos en las ramas del $\mathsf{letcase}^\circ$ para aumentar la expresividad del lenguaje, permitiendo tipar términos de punto fijo más interesantes. El tipo de los términos de cada rama no puede ser una medición ni una flecha que termine en medición, ya que esto eventualmente reduciría a una suma de mediciones que no tipa por la regla anterior.

La única diferencia respecto a estas reglas de tipado para λ_ρ^μ, en la figura (3.6), es que el término $\mu_n f.t$ cambia por $\mu f.t$, pero estos son tipados de la misma manera, y la regla $\bot$ desaparece ya que el término $\bot_A$ no existe en este cálculo.

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

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

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

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

$$\frac{\Gamma, f : A \vdash t : A}{\Gamma \vdash \mu_n f.t : A}\ \mu \qquad \frac{}{\Gamma \vdash \bot_A : A}\ \bot$$

$$\frac{\Delta_0, x : n \vdash t_0 : A \quad \dots \quad \Delta_{2^m-1}, x : n \vdash t_{2^m-1} : A \quad \Gamma \vdash r : (m,n) \quad \ell(A) \neq (m',n')}{\Delta_0, \dots, \Delta_{2^m-1}, \Gamma \vdash \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \dots, t_{2^m-1}\} : A}\ \mathsf{m}_e$$

$$\frac{\Gamma \vdash t_1 : A \quad \dots \quad \Gamma \vdash t_n : A \quad \sum_{i=1}^n p_i \leq 1 \quad \ell(A) \neq (m,n)}{\Gamma \vdash \sum_{i=1}^n p_i t_i : A}\ +$$

Fig. 3.5: Sistema de tipos de $\lambda_\rho^{\mu_n}$

Ejemplo 3.1.1.
El siguiente término cerrado de $\lambda_\rho^{\mu_n}$ es válido según la nueva sintaxis:

$$\mu_2 x.\mathsf{letcase}^\circ\ z = \pi^1 |+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\}$$

Se puede probar que su tipo es 1:

$$\dfrac{\dfrac{\dfrac{}{x : 1, z : 1 \vdash x : 1}\ \mathsf{ax} \quad \dfrac{}{x : 1, z : 1 \vdash |+\rangle\langle+| : 1}\ \mathsf{ax}_\rho \quad \dfrac{\dfrac{}{\vdash |+\rangle\langle+| : 1}\ \mathsf{ax}_\rho}{\vdash \pi^1 |+\rangle\langle+| : (1,1)}\ \mathsf{m_i}}{x : 1 \vdash \mathsf{letcase}^\circ\ z = \pi^1 |+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\} : 1}\ \mathsf{m_e}}{\vdash \mu_2 x.\mathsf{letcase}^\circ\ z = \pi^1 |+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\} : 1}\ \mu$$

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

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

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

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

$$\frac{\Gamma, f : A \vdash t : A}{\Gamma \vdash \mu f.t : A}\ \mu$$

$$\frac{\Delta_0, x:n \vdash t_0 : A \quad \ldots \quad \Delta_{2^m-1}, x:n \vdash t_{2^m-1} : A \quad \Gamma \vdash r : (m,n) \quad \ell(A) \neq (m',n')}{\Delta_0, \ldots, \Delta_{2^m-1}, \Gamma \vdash \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} : A}\ \mathsf{m}_e$$

$$\frac{\Gamma \vdash t_1 : A \quad \ldots \quad \Gamma \vdash t_n : A \quad \sum_{i=1}^n p_i \leq 1 \quad \ell(A) \neq (m,n)}{\Gamma \vdash \sum_{i=1}^n p_i t_i : A}\ +$$

Fig. 3.6: Sistema de tipos de λ^μ_ρ

El término reduce a $\frac{3}{4}|+\rangle\langle+|$:

$$\begin{aligned}
&\mu_2 x.\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\} \\
\rightsquigarrow\ &\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{\mu_1 x.\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\}, |+\rangle\langle+|\} \\
\rightsquigarrow\ &\tfrac{1}{2}\mu_1 x.\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\} + \tfrac{1}{2}|+\rangle\langle+| \\
\rightsquigarrow\ &\tfrac{1}{2}\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{\mu_0 x.\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\}, |+\rangle\langle+|\} + \tfrac{1}{2}|+\rangle\langle+| \\
\rightsquigarrow\ &\tfrac{1}{2}\left(\tfrac{1}{2}\mu_0 x.\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\} + \tfrac{1}{2}|+\rangle\langle+|\right) + \tfrac{1}{2}|+\rangle\langle+| \\
\rightsquigarrow\ &\tfrac{1}{2}\left(\tfrac{1}{2}\bot_1 + \tfrac{1}{2}|+\rangle\langle+|\right) + \tfrac{1}{2}|+\rangle\langle+| \rightsquigarrow \tfrac{1}{4}|+\rangle\langle+| + \tfrac{1}{2}|+\rangle\langle+| \rightsquigarrow \tfrac{3}{4}|+\rangle\langle+|
\end{aligned}$$

Se puede ver que si aumenta la cantidad de iteraciones (la n del punto fijo) las reescrituras se van aproximando cada vez más a $|+\rangle\langle+|$:

$$\mu_n x.\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\} \rightsquigarrow^* \tfrac{1}{2^n}\bot_1 + (1 - \tfrac{1}{2^n})|+\rangle\langle+| \rightsquigarrow (1 - \tfrac{1}{2^n})|+\rangle\langle+|$$

El término análogo en λ^μ_ρ es el siguiente:

$$\mu x.\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\}$$

Su tipo coincide con el anterior, ya que las reglas son las mismas. En este caso el

término reduce infinitamente:

$$
\begin{aligned}
&\mu x.\mathsf{letcase}^{\circ}\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\}\\
&\rightsquigarrow\ \mathsf{letcase}^{\circ}\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{\mu x.\mathsf{letcase}^{\circ}\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\}, |+\rangle\langle+|\}\\
&\rightsquigarrow\ \tfrac{1}{2}\mu x.\mathsf{letcase}^{\circ}\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\} + \tfrac{1}{2}|+\rangle\langle+|\\
&\rightsquigarrow\ \tfrac{1}{2}\mathsf{letcase}^{\circ}\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{\mu x.\mathsf{letcase}^{\circ}\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\}, |+\rangle\langle+|\} + \tfrac{1}{2}|+\rangle\langle+|\\
&\rightsquigarrow\ \tfrac{1}{2}\left(\tfrac{1}{2}\mu x.\mathsf{letcase}^{\circ}\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\} + \tfrac{1}{2}|+\rangle\langle+|\right) + \tfrac{1}{2}|+\rangle\langle+|\\
&\rightsquigarrow^{*}\ \tfrac{1}{2}(\tfrac{1}{2}\ldots(\tfrac{1}{2}\mu x.\mathsf{letcase}^{\circ}\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\} + \tfrac{1}{2}|+\rangle\langle+|)\ldots + \tfrac{1}{2}|+\rangle\langle+|) + \tfrac{1}{2}|+\rangle\langle+|\\
&\rightsquigarrow\ \ldots
\end{aligned}
$$

3.2. Resultados previos

Normalización fuerte, el lema de sustitución y subject reduction ya fueron demostrados para λ°_{ρ} en [DC17] y [Rom20]. Normalización fuerte sigue valiendo en $\lambda^{\mu_n}_{\rho}$, pero subject reduction sólo vale para términos cerrados, a causa del término de punto fijo.

Teorema 3.2.1 (Normalización fuerte)**.** *Los términos bien tipados de $\lambda^{\mu_n}_{\rho}$ son fuertemente normalizantes, es decir que no pueden reducir infinitamente.*

Demostración. La demostración para λ°_{ρ} está dada por [Rom20, Teorema 4.3.8]. Vale trivialmente para extensión $\lambda^{\mu_n}_{\rho}$ ya que sólo se agregan los términos con punto fijo incremental, que reducen finitamente, y *bottom*. Consideramos que no parece ser muy complicado extender la demostración agregando estos términos. □

Lema 3.2.2 (Sustitución)**.** *Si $\Gamma, x : A \vdash t : B$ $y \vdash r : A$ entonces $\Gamma \vdash t[x := r] : B$.*

Demostración. Por inducción en t.

- Sea $t = x$. Entonces valen $A = B$ y $x[x := r] = r$, por lo tanto se cumple.
- Sea $t = y$. Entonces se tienen $(y : B) \in \Gamma$ y $y[x := r] = y$, por lo tanto vale $\Gamma \vdash y : B$.
- Sea $t = \lambda y.s$. Entonces $B = C \multimap D$, y por inversión $\Gamma, x : A, y : C \vdash s : D$. Por hipótesis inductiva vale $\Gamma, y : C \vdash s[x := r] : D$, y por la regla $\multimap_i$ se tiene que $\Gamma \vdash (\lambda y.s)[x := r] : C \multimap D$.
- Sea $t = t_1 t_2$. Sean $\Gamma_1, \Gamma_2 = \Gamma, x : A$ disjuntas, tales que $\Gamma_1 \vdash t_1 : C \multimap B$ y $\Gamma_2 \vdash t_2 : C$.
  - Si $(x : A) \in \Gamma_1$, entonces por hipótesis inductiva $\Gamma_1 \backslash \{x : A\} \vdash t_1[x := r] : C \multimap B$. Por lo tanto usando la regla $\multimap_e$ se tiene que $\Gamma \vdash (t_1[x := r])t_2 : B$, y vale $(t_1 t_2)[x := r] = (t_1[x := r])t_2$, ya que x no aparece libre en t_2.
  - Si $(x : A) \in \Gamma_2$, entonces por hipótesis inductiva $\Gamma_2 \backslash \{x : A\} \vdash t_2[x := r] : C$. Por lo tanto usando la regla $\multimap_e$ se tiene que $\Gamma \vdash t_1(t_2[x := r]) : B$, y vale $(t_1 t_2)[x := r] = t_1(t_2[x := r])$, ya que x no aparece libre en t_1.
- Sea $t = \mu_n y.s$. En este caso se tiene $\Gamma, x : A \vdash \mu_n y.s : B$. Esto solo puede pasar si $\Gamma, x : A, y : B \vdash s : B$. Por hipótesis inductiva se tiene entonces que $\Gamma, y : B \vdash s[x := r] : B$. Entonces por la regla μ vale $\Gamma \vdash (\mu_n y.s)[x := r] : B$.

- Sea $t = \bot_A$. Este caso es trivial ya que $\bot_A$ no tiene variables libres.
- Sea $t = \rho^n$. Este caso es análogo al anterior.
- Sea $t = U^m s$. En este caso $B = n$ y por inversión $\Gamma, x : A \vdash s : n$. Por hipótesis inductiva se tiene que $\Gamma \vdash s[x := r] : n$ y por la regla u_i vale $\Gamma \vdash (U^m s)[x := r] : n$.
- Sea $t = \pi^m s$. Entonces $B = (m, n)$ y por inversión se tiene $\Gamma, x : A \vdash s : n$. Por hipótesis inductiva vale $\Gamma \vdash s[x := r] : n$ y por la regla m_i, $\Gamma \vdash (\pi^m s)[x := r] : (m, n)$.
- Sea $t = t_1 \otimes t_2$. En este caso $B = n + m$, y sean $\Gamma_1, \Gamma_2 = \Gamma, x : A$ disjuntas, tales que $\Gamma_1 \vdash t_1 : n$ y $\Gamma_2 \vdash t_2 : m$.
  - Si $(x : A) \in \Gamma_1$ entonces por hipótesis inductiva $\Gamma_1 \backslash \{x : A\} \vdash t_1[x := r] : n$. Por lo tanto usando la regla $\otimes$ se tiene que $\Gamma \vdash t_1[x := r] \otimes t_2 : n + m$, y vale $(t_1 \otimes t_2)[x := r] = t_1[x := r] \otimes t_2$ ya que x no aparece libre en t_2.
  - Si $(x : A) \in \Gamma_2$ entonces por hipótesis inductiva $\Gamma_2 \backslash \{x : A\} \vdash t_2[x := r] : m$. Por lo tanto usando la regla $\otimes$ se tiene que $\Gamma \vdash t_1 \otimes t_2[x := r] : n + m$, y vale $(t_1 \otimes t_2)[x := r] = t_1 \otimes t_2[x := r]$ ya que x no aparece libre en t_1.
- Sea $t = \sum_i p_i t_i$. Entonces se tiene que $\Gamma, x : A \vdash t_i : B$ para todo i. Por hipótesis inductiva, $\Gamma \vdash t_i[x := r] : B$ para todo i, con $\ell(B) \neq (m, n)$. Entonces por la regla $+$ se tiene $\Gamma \vdash (\sum_i p_i t_i)[x := r] : B$. Notar que x sólo puede estar libre en uno de los t_i.
- Sea $t = \mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$. Sean $\Gamma_1, \ldots, \Gamma_{2^m-1}, \Gamma' = \Gamma, x : A$, disjuntas. Entonces se tiene $\Gamma_i, y : n \vdash t_i : B$ para todo i, $\Gamma' \vdash s : (m, n)$ y $\ell(B) \neq (m', n')$.
  - Si $(x : A) \in \Gamma_j$ para alguna j, entonces por hipótesis inductiva $\Gamma_j \backslash \{x : A\} \vdash t_j[x := r] : B$, y por la regla m_e vale $\Gamma \vdash \mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_j[x := r], \ldots, t_{2^m-1}\} : B$, que es lo mismo que $\Gamma \vdash (\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\})[x := r] : B$ porque x no aparece libre en los demás t_i ni en s.
  - Si $(x : A) \in \Gamma'$, entonces por hipótesis inductiva $\Gamma' \backslash \{x : A\} \vdash s[x := r] : (m, n)$, y por la regla m_e vale $\Gamma \vdash \mathsf{letcase}^\circ\ y = s[x := r]\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} : B$, que es lo mismo que $\Gamma \vdash (\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\})[x := r] : B$ porque x no aparece libre en ningún t_i. □

Teorema 3.2.3 (Subject reduction)**.** *Si* $\vdash t : A$ *y* $t \rightsquigarrow r$ *entonces* $\vdash r : A$.

Demostración. Por inducción en $\rightsquigarrow$.

- Sean $t = (\lambda x.t')s$ y $r = t'[x := s]$. Entonces $\vdash (\lambda x.t')s : A$, por lo tanto $\vdash \lambda x.t' : B \multimap A$ y $\vdash s : B$. Se tiene $x : B \vdash t' : A$, y por el lema (3.2.2) $\vdash t'[x := s] : A$.
- Sean $t = \mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$ y $r = \sum_i p_i t_i[x := \rho_i^n]$, con $p_i = \mathsf{tr}\left(\overline{\pi_i} \rho^n \overline{\pi_i}^\dagger\right)$ y $\rho_i^n = \frac{\overline{\pi_i} \rho^n \overline{\pi_i}^\dagger}{p_i}$. Entonces por inversión se tiene que $x : n' \vdash t_i : A$ para todo i, $\vdash \pi^m \rho^n : (m, n')$ y $\ell(A) \neq (m', n'')$. Por inversión nuevamente, $\vdash \rho^n : n'$ y por la regla ax_ρ, $n = n'$. Por el lema (3.2.2) se tiene que $\vdash t_i[x := \rho_i^n] : A$ y por la regla $+$, $\vdash \sum_i p_i t_i[x := \rho_i^n] : A$.
- Sean $t = \mu_0 x.s$ y $r = \bot_A$. Siempre vale $\vdash \bot_A : A$.

- Sean $t = \mu_{n+1}x.s$ y $r = s[x := \mu_n x.s]$. Se tiene que $\vdash \mu_{n+1}x.s : A$, y por inversión $x : A \vdash s : A$. Usando la regla μ vale $\vdash \mu_n x.s : A$, y por el lema (3.2.2) se tiene que $\vdash s[x := \mu_n x.s] : A$.

- Sean $t = \bot_n$ y $r = \mathbb{0}_{2^n}$. En este caso $A = n$ y $\Gamma \vdash \mathbb{0}_{2^n} : n$ porque es la matriz constante nula en $2^n \times 2^n$.

- Sean $t = \bot_{(m,n)}$ y $r = \pi^m \mathbb{0}_{2^n}$. En este caso $A = (m, n)$ y como $\Gamma \vdash \mathbb{0}_{2^n} : n$ se tiene $\Gamma \vdash \pi^m \mathbb{0}_{2^n} : (m, n)$ por la regla m_i.

- Sean $t = \bot_{C \multimap D} s$ y $r = \bot_D$. Se tiene $\vdash \bot_{C \multimap D} s : A$, y por inversión vale $A = D$. Además siempre vale $\vdash \bot_D : D$.

- Sean $t = pt + q\bot_A$ y $r = pt$. Por inversión se tiene $\Gamma \vdash t : A$ y por lo tanto $\Gamma \vdash pt : A$, considerando la sumatoria con un solo elemento.

- Sean $t = U^m \rho^n$ y $r = \rho'^n$, con $\overline{U^m} \rho^n \overline{U^m}^\dagger = \rho'^n$. Entonces $A = n$, y por la regla ax_ρ se tiene $\vdash \rho'^n : n$.

- Sean $t = \rho_1^n \otimes \rho_2^m$ y $r = \rho$, con $\rho = \rho_1^n \otimes \rho_2^m$. Entonces $A = n + m$ con $\vdash \rho_1^n : n$ y $\vdash \rho_2^m : m$. Como ρ es una matriz de densidad que representa $n + m$ qubits se tiene $\vdash \rho : n + m$.

- Sean $t = \sum_i p_i \rho_i^n$ y $r = \rho'$, con $\rho' = \sum_i p_i \rho_i^n$. Entonces se tiene $A = n$ y por la regla $\mathsf{ax}_\rho, \vdash \rho' : n$.

- Sean $t = \sum_i (p_i s)$ y $r = (\sum_i p_i)s$. Por inversión se tiene $\vdash s : A$ y por lo tanto considerando la sumatoria con un único elemento y probabilidad $\sum_i p_i$ vale $\vdash (\sum_i p_i)s : A$.

- Sean $t = (\sum_i p_i t_i)s$ y $r = \sum_i p_i (t_i s)$. Por inversión se tiene que $\vdash \sum_i p_i t_i : B \multimap A$, $\vdash s : B$ y $\ell(A) \neq (m, n)$. Por inversión nuevamente $\vdash t_i : B \multimap A$ para todo i, por lo tanto por la regla $\multimap_e$ se tiene $\vdash t_i s : A$. Usando la regla $+$, como $\ell(A) \neq (m, n)$, se tiene $\vdash \sum_i p_i (t_i s) : A$.

Casos contextuales: Sean s y s' tal que $s \rightsquigarrow s'$.

- Sean $t = st'$ y $r = s't'$. Se tiene $\vdash st' : A$, por inversión $\vdash s : B \multimap A$ y $\vdash t' : B$. Por hipótesis inductiva $\vdash s' : B \multimap A$, y por la regla $\multimap_e$ se tiene $\vdash s't' : A$.

- Sean $t = t's$ y $r = t's'$. Se tiene $\vdash t's : A$, por inversión $\vdash t' : B \multimap A$ y $\vdash s : B$. Por hipótesis inductiva $\vdash s' : B$, y por la regla $\multimap_e$ se tiene $\vdash t's' : A$.

- Sean $t = U^m s$ y $r = U^m s'$. Se tiene $A = n$, y por inversión $\vdash s : n$. Por hipótesis inductiva vale $\vdash s' : n$, y por la regla u_i se tiene $\vdash U^m s' : n$.

- Sean $t = \pi^m s$ y $r = \pi^m s'$. Se tiene $A = (m, n)$ y por inversión $\vdash s : n$. Por hipótesis inductiva se tiene que $\vdash s' : n$ y por la regla m_i vale $\vdash \pi^m s' : (m, n)$.

- Sean $t = s \otimes t'$ y $r = s' \otimes t'$. En este caso $A = n + m$ y por inversión $\vdash s : n$ y $\vdash t' : m$. Por hipótesis inductiva vale que $\vdash s' : n$ y por lo tanto $\vdash s' \otimes t' : n + m$.

- Sean $t = t' \otimes s$ y $r = t' \otimes s'$. En este caso $A = n + m$ y por inversión $\vdash t' : n$ y $\vdash s : m$. Por hipótesis inductiva vale que $\vdash s' : m$ y por lo tanto $\vdash t' \otimes s' : n + m$.

- Sean $t = \sum_i p_i t_i$ y $r = \sum_i p_i r_i$, con $t_j \rightsquigarrow r_j$ y para todo $i \neq j$ se tiene $t_i = r_i$. Por inversión se tiene que $\vdash t_i : A$ para todo i y $\ell(A) \neq (m, n)$. Por hipótesis inductiva vale $\vdash r_i : A$ para todo i, y por la regla $+$ se tiene $\vdash \sum_i p_i r_i : A$.
- Sean $t = \mathsf{letcase}^\circ\ x = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$ y $r = \mathsf{letcase}^\circ\ x = s'\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$. Por inversión se tiene $x : n \vdash t_i : A$ para todo i, $\vdash s : (m, n)$ y $\ell(A) \neq (m', n')$. Por hipótesis inductiva $\vdash s' : (m, n)$, y por lo tanto usando la regla m_e se tiene $\vdash \mathsf{letcase}^\circ\ x = s'\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} : A$. □

4. SEMÁNTICA DENOTACIONAL EN CPM

La semántica denotacional para $\lambda_\rho^{\mu_n}$ y λ_ρ^{μ} va a ser redefinida por completo respecto a la dada para λ_ρ° en [DC17]. El objetivo es que los dominios de interpretación tengan la estructura de CPOs de matrices positivas, para poder asegurar la existencia del punto fijo como límite del punto fijo incremental dentro del dominio. Las funciones van a ser interpretadas como CPMs (Complete Positive Maps), es decir mapas completamente positivos que llevan matrices positivas de un CPO a matrices positivas de otro CPO.

Esta semántica está inspirada en la de [SV08], en la cual se usan CPMs para interpretar las funciones. Además, la construcción de los dominios como CPOs es análoga a la de [Sel04].

Los mapas en estos lenguajes son afines, es decir que pueden separarse en una suma entre una parte lineal y otra constante. Si las funciones fuesen lineales puras, el mínimo punto fijo de cualquier función sería el mínimo elemento del dominio.

Una diferencia importante respecto a λ_ρ° es que entre las matrices de densidad básicas se incluyen matrices positivas con trazas menores a 1. Esto es necesario para la construcción de la estructura de los dominios, ya que el orden en los CPOs va a estar definido en base a la positividad de las diferencias de matrices, quedando el elemento mínimo de cada uno como la matriz nula en la dimensión correspondiente. Desde un punto de vista semántico, las matrices de traza menor a 1 representan a los programas con probabilidad positiva de no detenerse nunca.

La estructura de este capítulo es la siguiente: primero se definen los dominios asociados a cada tipo. Dos de ellos (los que representan los estados de los qubits y los resultados de las mediciones) van a tener su traza acotada por 1; los tipos flecha no van a tener su traza acotada en un principio.

Luego el capítulo se divide en dos partes principales. En la primera se demuestran una serie de lemas sobre la semántica de $\lambda_\rho^{\mu_n}$ con el objetivo de demostrar el teorema (4.6.16) (adecuación). Para lograrlo fue necesario incluir dos conjeturas: la primera (4.6.1) afirma que la parte lineal de los mapas es completamente positiva y la segunda (4.6.15) afirma que la aplicación preserva positividad. Demostrar estas conjeturas se deja como trabajo futuro, por falta de tiempo.

En la segunda parte, ya teniendo el resultado de adecuación en $\lambda_\rho^{\mu_n}$, se demuestra que para cada tipo flecha existe una cota para la traza de las interpretaciones de términos bien tipados. Usando estas cotas para la traza se demuestra que los dominios tienen estructura de CPO, respecto a un orden preservado por las funciones. Esto permite demostrar la existencia del límite de la interpretación del punto fijo incremental, y definir la interpretación del punto fijo en λ_ρ^{μ} como este límite.

4.1. Dominio de interpretación

Se definen las matrices de densidad generalizadas como:

$$\mathcal{D}_n := \left\{ \rho \mid \rho \in \mathbb{C}^{2^n \times 2^n} \text{ positiva con } tr(\rho) \leq 1 \right\}$$

La interpretación de los tipos está dada por la figura (4.1).

$$(\!|n|\!) := \mathcal{D}_n$$

$$(\!|(m,n)|\!) := \left\{ p \mid p \in \bigoplus_{i=1}^{2^m} \mathcal{D}_n \text{ y } \mathsf{tr}\,(p) \leq 1 \right\}$$

$$(\!|A \multimap B|\!) := \{ f \mid f \text{ positiva en } ((\!|A|\!) \otimes (\!|B|\!)) \oplus (\!|B|\!) \}$$

Fig. 4.1: Dominios de interpretación de $\lambda_\rho^{\mu_n}$

- Los términos de tipo n se interpretan como matrices de densidad generalizadas de tamaño $2^n \times 2^n$, es decir que representan los sistemas de n qubits.
- Los términos de tipo (m,n) representan los resultados de las mediciones. Se interpretan como coproductos de las matrices de densidad que resultan de la proyección de la matriz medida mediante cada uno de los proyectores correspondientes a la medición de los primeros m qubits del sistema. Por esta razón la traza de estos elementos está acotada por 1, ya que las matrices de densidad generalizadas en el coproducto no están necesariamente normalizadas. Por ejemplo, $(\frac{1}{2}|0\rangle\langle 0| \oplus \frac{1}{2}|1\rangle\langle 1|)$ es un elemento de $(\!|(1,1)|\!)$ ya que $\frac{1}{2}|0\rangle\langle 0| \in \mathcal{D}_1, \frac{1}{2}|1\rangle\langle 1| \in \mathcal{D}_1$ y sus trazas suman 1.
- Los términos de tipo flecha $A \multimap B$ son interpretados como funciones afines en el espacio formado por el coproducto entre $(\!|A|\!) \otimes (\!|B|\!)$ y $(\!|B|\!)$. La parte lineal se representa en $(\!|A|\!) \otimes (\!|B|\!)$ mediante su forma de actuar en la base canónica de $(\!|A|\!)$, y la parte constante es una matriz en $(\!|B|\!)$.

Definición 4.1.1 (Dominios)**.** Se define el conjunto Dom de los dominios de interpretación como:

$$\mathsf{Dom} = \bigcup_{A \in \mathsf{Types}} (\!|A|\!)$$

Definición 4.1.2 (Dimensión)**.** Se define la dimensión de un tipo como la dimensión de su espacio de representación, es decir $\dim(A) := dim((\!|A|\!))$:

- $\dim(n) = 2^n$
- $\dim((m,n)) = 2^m 2^n = 2^{n+m}$
- $\dim(A \multimap B) = (\dim(A) + 1)\dim(B)$

4.2. Representación de funciones

Las funciones representadas son afines, es decir que consisten de una transformación lineal y una traslación desde el origen. La interpretación $\chi_{[f]} \in (\!|A \multimap B|\!)$ de una función f está dada por una matriz que representa la parte lineal y una matriz que representa la parte constante:

$$\chi_{[f]} := \left(\begin{array}{c|c|c} f(E_{11}^A) - f(\mathbb{0}_{\dim(A)}) & \cdots & f(E_{1n}^A) - f(\mathbb{0}_{\dim(A)}) \\ \hline \vdots & \ddots & \vdots \\ \hline f(E_{n1}^A) - f(\mathbb{0}_{\dim(A)}) & \cdots & f(E_{nn}^A) - f(\mathbb{0}_{\dim(A)}) \end{array} \right) \oplus f(\mathbb{0}_{\dim(A)})$$

donde los E_{ij}^{A} representan los elementos de la base canónica y $\mathbb{0}_{\dim(A)}$ es la matriz nula en el espacio $(\!|A|\!)$. La matriz a la izquierda del coproducto representa la transformación lineal sobre la base canónica de $(\!|A|\!)$, mientras que la matriz a la derecha representa la traslación del origen.

Ejemplos

- El término $\lambda x.\mathsf{letcase}^{\circ}\ y = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |0\rangle\langle 0|\}$ tiene tipo $1 \multimap 1$ y se denota por la función $a \overset{f}{\mapsto} \mathsf{letcase}^{\circ}\ y = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{a, |0\rangle\langle 0|\}$. Su representación se encuentra en $\mathbb{C}^{4\times 4} \oplus \mathbb{C}^{2\times 2}$:

$$\chi_{[f]} = \begin{pmatrix} \frac{1}{2}|0\rangle\langle 0| & \frac{1}{2}|0\rangle\langle 1| \\ \frac{1}{2}|1\rangle\langle 0| & \frac{1}{2}|1\rangle\langle 1| \end{pmatrix} \oplus \frac{1}{2}|0\rangle\langle 0| = \left(\begin{array}{cc|cc} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{array}\right) \oplus \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix}$$

- El término $\lambda x.\mathsf{letcase}^{\circ}\ y = x\ \mathsf{in}\ \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ tiene tipo $(1,1) \multimap 1$ y se denota por la función $a \overset{g}{\mapsto} \mathsf{letcase}^{\circ}\ y = a\ \mathsf{in}\ \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. La base canónica del espacio de salida $(\!|(1,1)|\!)$ está compuesta por:

$$\begin{array}{cccc} |0\rangle\langle 0| \oplus \mathbb{0}_2 & |1\rangle\langle 0| \oplus \mathbb{0}_2 & \mathbb{0}_2 \oplus |0\rangle\langle 0| & \mathbb{0}_2 \oplus |1\rangle\langle 0| \\ |0\rangle\langle 1| \oplus \mathbb{0}_2 & |1\rangle\langle 1| \oplus \mathbb{0}_2 & \mathbb{0}_2 \oplus |0\rangle\langle 1| & \mathbb{0}_2 \oplus |1\rangle\langle 1| \end{array}$$

  y por lo tanto la interpretación de esta función está dada por:

$$\begin{aligned} \chi_{[g]} &= \left(\begin{pmatrix} |0\rangle\langle 0| & \mathbb{0}_2 \\ \mathbb{0}_2 & |0\rangle\langle 0| \end{pmatrix} \oplus \begin{pmatrix} |1\rangle\langle 1| & \mathbb{0}_2 \\ \mathbb{0}_2 & |1\rangle\langle 1| \end{pmatrix}\right) \oplus \mathbb{0}_2 \\ &= \left(\left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \oplus \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)\right) \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

- El término $\lambda x.\pi^1 x$ tiene tipo $1 \multimap (1,1)$ y se denota por la función $a \overset{h}{\mapsto} \pi^1 a$. Su representación está dada por:

$$\begin{aligned} \chi_{[h]} &= \begin{pmatrix} |0\rangle\langle 0| \oplus \mathbb{0}_2 & \mathbb{0}_2 \oplus \mathbb{0}_2 \\ \mathbb{0}_2 \oplus \mathbb{0}_2 & \mathbb{0}_2 \oplus |1\rangle\langle 1| \end{pmatrix} \oplus (\mathbb{0}_2 \oplus \mathbb{0}_2) \\ &= \left(\begin{array}{cc} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{array}\right) \oplus \left(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right) \end{aligned}$$

4.3. Semántica de la aplicación

Las funciones son afines y su interpretación está dada por una transformación lineal y una traslación. Por lo tanto, la forma de aplicarlas es descomponer el término sobre el cual se aplican en la base canónica, aplicar la transformación lineal y luego sumar la traslación.

Definición 4.3.1 (Operador \$)**.** Sea $\{E^n_{ij}\}$ la base canónica de $\mathbb{C}^{n\times n}$. Sean $M_{ij}, M_\perp \in \mathbb{C}^{m\times m}$ para $1 \leq i,j \leq n$. Dada una matriz en $\mathbb{C}^{nm\times nm} \oplus \mathbb{C}^{m\times m}$ y un elemento de la base de $\mathbb{C}^{n\times n}$, el operador \$ selecciona la submatriz en $\mathbb{C}^{m\times m}$ correspondiente de la parte izquierda del coproducto:

$$\left(\left(\sum_{ij} E^n_{ij} \otimes M_{ij}\right) \oplus M_\perp\right) \$\ E^n_{kl} = M_{kl}$$

para todo $1 \leq k,l \leq n$. En el caso de la matriz nula $\mathbb{0}_n \in \mathbb{C}^{n\times n}$ se selecciona la parte derecha del coproducto:

$$\left(\left(\sum_{ij} E^n_{ij} \otimes M_{ij}\right) \oplus M_\perp\right) \$\ \mathbb{0}_n = M_\perp$$

Definición 4.3.2 (Operador #)**.** Sea χ un elemento de $\mathbb{C}^{nm\times nm} \oplus \mathbb{C}^{m\times m}$. El operador # define su forma de actuar sobre elementos de $\mathbb{C}^{n\times n}$ de la siguiente manera:

$$\chi \#\ \left(\sum_{ij} m_{ij} E^n_{ij}\right) = \sum_{ij} m_{ij}\left(\chi \$\ E^n_{ij}\right) + \chi \$\ \mathbb{0}_n$$

Ejemplos

Para las funciones f, g y h definidas anteriormente.

- En el caso de la función f, que denota el término $t = \lambda x.\mathsf{letcase}^\circ\ y = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |0\rangle\langle 0|\}$, se tiene:

$$\begin{aligned}\chi_{[f]} \#\ \begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix} =& \chi_{[f]} \#\ (|1\rangle\langle 1| + |0\rangle\langle 1|)\\ =& \chi_{[f]} \$\ |1\rangle\langle 1| + \chi_{[f]} \$\ |0\rangle\langle 1| + \chi_{[f]} \$\ \mathbb{0}_2\\ =& \begin{pmatrix}0 & 0\\ 0 & \frac{1}{2}\end{pmatrix} + \begin{pmatrix}0 & \frac{1}{2}\\ 0 & 0\end{pmatrix} + \begin{pmatrix}\frac{1}{2} & 0\\ 0 & 0\end{pmatrix} = \begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ 0 & \frac{1}{2}\end{pmatrix}\end{aligned}$$

- En el caso de la función g, que denota el término $t = \lambda x.\mathsf{letcase}^\circ\ y = x\ \mathsf{in}\ \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, se tiene:

$$\begin{aligned}\chi_{[g]} \#\ \left(\begin{pmatrix}0 & 0\\ 1 & \frac{1}{2}\end{pmatrix} \oplus \begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ 0 & 0\end{pmatrix}\right) &= \chi_{[g]} \#\ ((|1\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|) \oplus (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|0\rangle\langle 1|))\\ &= \chi_{[g]} \#\ (|1\rangle\langle 0| \oplus \mathbb{0}_2) + \tfrac{1}{2}\chi_{[g]} \#\ (|1\rangle\langle 1| \oplus \mathbb{0}_2)\\ +\tfrac{1}{2}\chi_{[g]} \#\ (\mathbb{0}_2 \oplus |0\rangle\langle 0|) + \frac{1}{2}\chi_{[g]} &\#\ (\mathbb{0}_2 \oplus |0\rangle\langle 1|) + \chi_{[g]} \#\ (\mathbb{0}_2 \oplus \mathbb{0}_2)\\ &= \mathbb{0}_2 + \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| + \tfrac{1}{2}\mathbb{0}_2 + \mathbb{0}_2 = \begin{pmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{pmatrix}\end{aligned}$$

- En el caso de la función h, que denota el término $t = \lambda x.\pi^1 x$, se tiene:

$$\begin{aligned}\chi_{[h]} \# \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 0 \end{pmatrix} =& \chi_{[h]} \# (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|0\rangle\langle 1|) \\ =& \tfrac{1}{2}(|0\rangle\langle 0| \oplus \mathbb{0}_2) + \tfrac{1}{2}(\mathbb{0}_2 \oplus \mathbb{0}_2) + \mathbb{0}_2 \oplus \mathbb{0}_2 \\ =& \tfrac{1}{2}|0\rangle\langle 0| \oplus \mathbb{0}_2 = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\end{aligned}$$

Lema 4.3.3. *La aplicación # es afín a derecha.*

Demostración. Sean χ en $\mathbb{C}^{nm\times nm} \oplus \mathbb{C}^{m\times m}$, α, β en $\mathbb{C}$ y M, N en $\mathbb{C}^{n\times n}$. Sea $\{E^n_{ij}\}$ la base canónica de $\mathbb{C}^{n\times n}$, descompongo M y N en esta base:

$$M = \sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}E^n_{ij} \qquad\qquad N = \sum_{i=1}^{n}\sum_{j=1}^{n} n_{ij}E^n_{ij}$$

Por lo tanto se tiene:

$$\alpha M + \beta N = \sum_{i=1}^{n}\sum_{j=1}^{n}(\alpha m_{ij} + \beta n_{ij})E^n_{ij}$$

Por lo tanto:

$$\chi \# (\alpha M + \beta N) = \sum_{i=1}^{n}\sum_{j=1}^{n}(\alpha m_{ij} + \beta n_{ij})(\chi \$ E_{ij}) + \chi \$ \mathbb{0}_n$$

El primer término del resultado de la aplicación es lineal:

$$\sum_{i=1}^{n}\sum_{j=1}^{n}(\alpha m_{ij} + \beta n_{ij})(\chi \$ E^n_{ij}) = \alpha\sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}(\chi \$ E^n_{ij}) + \beta\sum_{i=1}^{n}\sum_{j=1}^{n} n_{ij}(\chi \$ E^n_{ij})$$

Como el segundo es constante para todo argumento $(\chi \$ \mathbb{0}_n)$ la aplicación es afín a derecha. □

Lema 4.3.4. *La aplicación # es lineal a izquierda.*

Demostración. Sean $\chi_{[f]}$ y $\chi_{[g]}$ elementos de $\mathbb{C}^{nm\times nm} \oplus \mathbb{C}^{m\times m}$, y sea M una matriz en $\mathbb{C}^{n\times n}$. Sea $\{E^n_{ij}\}$ la base canónica de $\mathbb{C}^{n\times n}$, descompongo M sobre esta base como:

$$M = \sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}E^n_{ij}$$

Descompongo $\chi_{[f]}$ y $\chi_{[g]}$ en sus partes lineal y constante de la siguiente manera:

$$\chi_{[f]} = \left(\sum_{k=1}^{n}\sum_{l=1}^{n} E^n_{kl} \otimes (L_f)_{kl}\right) \oplus K_f = L_f \oplus K_f$$

$$\chi_{[g]} = \left(\sum_{k=1}^{n}\sum_{l=1}^{n} E^n_{kl} \otimes (L_g)_{kl}\right) \oplus K_g = L_g \oplus K_g$$

Sean α, β en $\mathbb{C}$. Desarrollando $(\alpha\chi_{[f]} + \beta\chi_{[g]}) \# M$:

$$\begin{aligned}
(\alpha\chi_{[f]} + \beta\chi_{[g]}) \# M &= (\alpha(L_f \oplus K_f) + \beta(L_g \oplus K_g)) \# M \\
&= ((\alpha L_f + \beta L_g) \oplus (\alpha K_f + \beta K_g)) \# \sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij} E_{ij}^n \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}(\alpha L_f + \beta L_g)_{ij} + \alpha K_f + \beta K_g \\
&= \alpha\left(\sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}(L_f)_{ij} + K_f\right) + \beta\left(\sum_{i=1}^{n}\sum_{j=1}^{n} m_{ij}(L_g)_{ij} + K_g\right) \\
&= \alpha(\chi_{[f]} \# M) + \beta(\chi_{[g]} \# M)
\end{aligned}$$

□

4.4. Semántica denotacional del cálculo con punto fijo incremental

Una valuación es una función $\theta : \mathsf{Var} \to \mathsf{Dom}$, donde Var es el conjunto de todas las variables. Dada θ una valuación y t un término de $\lambda_\rho^{\mu_n}$, se define la interpretación de t respecto a θ como $(\!|t|\!)_\theta$ en la figura (4.2). $M \#_n N$ simboliza n aplicaciones sucesivas de M sobre N, por ejemplo $M \#_3 N = M \# (M \# (M \# N))$.

$$(\!|x|\!)_\theta = \theta(x) \qquad (\!|\lambda x.t|\!)_\theta = \chi_{[a \mapsto (\!|t|\!)_{\theta, x=a}]} \qquad (\!|tr|\!)_\theta = (\!|t|\!)_\theta \# (\!|r|\!)_\theta$$

$$(\!|\mu_n x.t|\!)_\theta = (\!|\lambda x.t|\!)_\theta \#_n \mathbb{0}_{\dim(A)} \qquad (\!|\bot_A|\!)_\theta = \mathbb{0}_{\dim(A)}$$

$$(\!|\rho|\!)_\theta = \rho \qquad (\!|Ut|\!)_\theta = \overline{U}(\!|t|\!)_\theta\overline{U}^\dagger \qquad (\!|\pi^m t|\!)_\theta = \bigoplus_{i=0}^{2^m-1}\left(\overline{\pi_i}(\!|t|\!)_\theta\overline{\pi_i}^\dagger\right) \qquad (\!|t \otimes r|\!)_\theta = (\!|t|\!)_\theta \otimes (\!|r|\!)_\theta$$

$$(\!|\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}|\!)_\theta = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho_i)\,(\!|t_i|\!)_{\theta, x=\rho_i'} \text{ con}$$
$$(\!|r|\!)_\theta = \bigoplus_{i=0}^{2^m-1} \rho_i \text{ y } \rho_i' = \begin{cases} \frac{\rho_i}{\mathsf{tr}(\rho_i)} & \text{si } \mathsf{tr}\,(\rho_i) \neq 0 \\ \rho_i & \text{si } \mathsf{tr}\,(\rho_i) = 0 \end{cases}$$

$$(\!|\sum_i p_i t_i|\!)_\theta = \sum_i p_i (\!|t_i|\!)_\theta$$

Fig. 4.2: Semántica denotacional de $\lambda_\rho^{\mu_n}$

4.5. Lemas preliminares

En esta sección se demuestran cinco lemas de la semántica denotacional necesarios para demostrar el teorema de adecuación (4.6.16).

El primero de los lemas establece la linealidad de lo que fue definido como la parte lineal de la aplicación de un término de la forma $\lambda x.t$. Como las funciones del cálculo

son afines, su parte lineal está dada por la resta entre la función y su parte constante. El siguiente lema muestra que esta resta es efectivamente una función lineal. La demostración usa la linealidad a izquierda de la aplicación (lema 4.3.4) y su afinidad a derecha (lema 4.3.3).

Lema 4.5.1 (Linealidad)**.** *Sea t un término bien tipado de $\lambda_\rho^{\mu_n}$ tal que $\Gamma, x : A \vdash t : B$, entonces para a en $(\!|A|\!)$ y $n = \dim(A)$ la siguiente función es lineal.*

$$a \mapsto (\!|t|\!)_{\theta,x=a} - (\!|t|\!)_{\theta,x=\mathbb{0}_n}$$

Demostración. La función definida es lineal si cumple:

$$(\!|t|\!)_{\theta,x=\alpha A+\beta B} - (\!|t|\!)_{\theta,x=\mathbb{0}_n} = \alpha((\!|t|\!)_{\theta,x=A} - (\!|t|\!)_{\theta,x=\mathbb{0}_n}) + \beta((\!|t|\!)_{\theta,x=B} - (\!|t|\!)_{\theta,x=\mathbb{0}_n})$$

Despejando, la condición de linealidad resulta:

$$(\!|t|\!)_{\theta,x=\alpha A+\beta B} = \alpha(\!|t|\!)_{\theta,x=A} + \beta(\!|t|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|t|\!)_{\theta,x=\mathbb{0}_n} \tag{4.1}$$

Por inducción en t:

- Sea $t = x$.

$$\begin{aligned}(\!|x|\!)_{\theta,x=\alpha A+\beta B} &= \alpha A + \beta B \\ &= \alpha A + \beta B - (\alpha+\beta-1)\ \mathbb{0}_n \\ &= \alpha(\!|x|\!)_{\theta,x=A} + \beta(\!|x|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|x|\!)_{\theta,x=\mathbb{0}_n}\end{aligned}$$

- Sea $t = y \neq x$. Por un lado se tiene:

$$(\!|y|\!)_{\theta,x=\alpha A+\beta B} = (\!|y|\!)_\theta = \theta(y)$$

  Por otro lado:

$$\alpha(\!|y|\!)_{\theta,x=A} + \beta(\!|y|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|y|\!)_{\theta,x=\mathbb{0}_n} = \alpha\theta(y) + \beta\theta(y) - (\alpha+\beta-1)\theta(y) = \theta(y)$$

- Sea $t = \lambda y.r$. Quiero ver que

$$(\!|\lambda y.r|\!)_{\theta,x=\alpha A+\beta B} = \alpha(\!|\lambda y.r|\!)_{\theta,x=A} + \beta(\!|\lambda y.r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|\lambda y.r|\!)_{\theta,x=\mathbb{0}_n}$$

  Por definición de $(\!|\cdot|\!)_\theta$ esto es equivalente a ver que:

$$\chi_{[a\mapsto(\!|r|\!)_{\theta,x=\alpha A+\beta B},y=a]} = \alpha\chi_{[a\mapsto(\!|r|\!)_{\theta,x=A,y=a]}} + \beta\chi_{[a\mapsto(\!|r|\!)_{\theta,x=B,y=a]}} - (\alpha+\beta-1)\chi_{[a\mapsto(\!|r|\!)_{\theta,x=\mathbb{0}_n,y=a]}} \tag{4.2}$$

  Desarrollando el lado izquierdo de esta ecuación, por hipótesis inductiva queda:

$$\chi_{[a\mapsto(\!|r|\!)_{\theta,x=\alpha A+\beta B},y=a]} = \chi_{[a\mapsto\alpha(\!|r|\!)_{\theta,x=A,y=a}+\beta(\!|r|\!)_{\theta,x=B,y=a}-(\alpha+\beta-1)(\!|r|\!)_{\theta,x=\mathbb{0}_n,y=a]}}$$

  Esto es igual al lado derecho de (4.2), por linealidad de la suma de matrices y multiplicación de matrices por escalares.

- Sea $t = rs$. Reemplazando en (4.1), quiero ver que:

$$(\!|rs|\!)_{\theta,x=\alpha A+\beta B} = \alpha(\!|rs|\!)_{\theta,x=A} + \beta(\!|rs|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|rs|\!)_{\theta,x=\mathbb{0}_n} \tag{4.3}$$

  Como el cálculo es afín, o bien vale $x \in \mathsf{FV}(r)$ o bien vale $x \in \mathsf{FV}(s)$.

  - Si $x \in \mathsf{FV}(r)$, de (4.3) quiero ver que:

$$(\!|r|\!)_{\theta,x=\alpha A+\beta B} \# (\!|s|\!)_\theta = \alpha((\!|r|\!)_{\theta,x=A} \# (\!|s|\!)_\theta) + \beta((\!|r|\!)_{\theta,x=B} \# (\!|s|\!)_\theta) - (\alpha+\beta-1)((\!|r|\!)_{\theta,x=\mathbb{0}_n} \# (\!|s|\!)_\theta) \tag{4.4}$$

    Desarrollando el lado izquierdo se tiene:

$$\begin{aligned}(\!|r|\!)_{\theta,x=\alpha A+\beta B} \# (\!|s|\!)_\theta &\overset{HI}{=} (\alpha(\!|r|\!)_{\theta,x=A} + \beta(\!|r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|r|\!)_{\theta,x=\mathbb{0}_n}) \# (\!|s|\!)_\theta \\ &\overset{(4,3,4)}{=} \alpha((\!|r|\!)_{\theta,x=A} \# (\!|s|\!)_\theta) + \beta((\!|r|\!)_{\theta,x=B} \# (\!|s|\!)_\theta) - (\alpha+\beta-1)((\!|r|\!)_{\theta,x=\mathbb{0}_n} \# (\!|s|\!)_\theta)\end{aligned}$$

    Se obtiene el lado derecho de (4.4).

  - Si $x \in \mathsf{FV}(s)$, de (4.3) quiero ver que:

$$(\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=\alpha A+\beta B} = \alpha((\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=A}) + \beta((\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=B}) - (\alpha+\beta-1)((\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=\mathbb{0}_n}) \tag{4.5}$$

    Desarrollando el lado izquierdo se tiene:

$$\begin{aligned}(\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=\alpha A+\beta B} &\overset{HI}{=} (\!|r|\!)_\theta \# (\alpha(\!|s|\!)_{\theta,x=A} + (\beta(\!|s|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|s|\!)_{\theta,x=\mathbb{0}_n})) \\ &\overset{(4,3,3)}{=} (\!|r|\!)_\theta \# (\alpha(\!|s|\!)_{\theta,x=A}) + (\!|r|\!)_\theta \# (\beta(\!|s|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|s|\!)_{\theta,x=\mathbb{0}_n}) - ((\!|r|\!)_\theta \# \mathbb{0}_n) \\ &\overset{(4,3,3)}{=} (\!|r|\!)_\theta \# (\alpha(\!|s|\!)_{\theta,x=A}) + (\!|r|\!)_\theta \# (\beta(\!|s|\!)_{\theta,x=B}) + (\!|r|\!)_\theta \# (-(\alpha+\beta-1)(\!|s|\!)_{\theta,x=\mathbb{0}_n}) - 2((\!|r|\!)_\theta \# \mathbb{0}_n) \\ &\overset{(4,3,3)}{=} \alpha((\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=A}) + (1-\alpha)((\!|r|\!)_\theta \# \mathbb{0}_n) + \beta((\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=B}) + (1-\beta)((\!|r|\!)_\theta \# \mathbb{0}_n) \\ &\quad - (\alpha+\beta-1)((\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=\mathbb{0}_n}) + (\alpha+\beta)((\!|r|\!)_\theta \# \mathbb{0}_n) - 2((\!|r|\!)_\theta \# \mathbb{0}_n) \\ &= \alpha((\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=A}) + \beta((\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=B}) - (\alpha+\beta-1)((\!|r|\!)_\theta \# (\!|s|\!)_{\theta,x=\mathbb{0}_n})\end{aligned}$$

    Se obtiene el lado derecho de (4.5).

- Sea $t = \mu_m y.r$. En este caso quiero ver que, reemplazando en (4.1):

$$(\!|\mu_m y.r|\!)_{\theta,x=\alpha A+\beta B} = \alpha(\!|\mu_m y.r|\!)_{\theta,x=A} + \beta(\!|\mu_m y.r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|\mu_m y.r|\!)_{\theta,x=\mathbb{0}_n}$$

  Desarrollando el lado izquierdo:

$$\begin{aligned}(\!|\mu_m y.r|\!)_{\theta,x=\alpha A+\beta B} &= ((\!|\lambda y.r|\!)_{\theta,x=\alpha A+\beta B}) \ \#_m \ \mathbb{0}_n \\ &\overset{abs}{=} (\alpha(\!|\lambda y.r|\!)_{\theta,x=A} + \beta(\!|\lambda y.r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|\lambda y.r|\!)_{\theta,x=\mathbb{0}_n}) \ \#_m \ \mathbb{0}_n \\ &\overset{(4,3,4)}{=} \alpha\,((\!|\lambda y.r|\!)_{\theta,x=A}) \ \#_m \ \mathbb{0}_n + \beta\,((\!|\lambda y.r|\!)_{\theta,x=B}) \ \#_m \ \mathbb{0}_n - (\alpha+\beta-1)\,((\!|\lambda y.r|\!)_{\theta,x=\mathbb{0}_n}) \ \#_m \ \mathbb{0}_n \\ &= \alpha(\!|\mu_m y.r|\!)_{\theta,x=A} + \beta(\!|\mu_m y.r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|\mu_m y.r|\!)_{\theta,x=\mathbb{0}_n}\end{aligned}$$

- Sea $t = \bot_A$. Este caso se cumple trivialmente ya que $(\!|\bot_A|\!)_\theta = \mathbb{0}_{\dim(A)}$ para toda valuación θ.

- Sea $t = \rho^n$. Este caso es análogo al de $t = y \neq x$.
- Sea $t = Ur$. Reemplazando en (4.1) quiero ver que:

$$(\!|Ur|\!)_{\theta,x=\alpha A+\beta B} = \alpha(\!|Ur|\!)_{\theta,x=A} + \beta(\!|Ur|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|Ur|\!)_{\theta,x=\mathbb{0}_n}$$

Desarrollando el lado izquierdo:

$$\begin{aligned}(\!|Ur|\!)_{\theta,x=\alpha A+\beta B} =& \overline{U}(\!|r|\!)_{\theta,x=\alpha A+\beta B}\overline{U}^\dagger \\ \overset{HI}{=}& \overline{U}(\alpha(\!|r|\!)_{\theta,x=A} + \beta(\!|r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|r|\!)_{\theta,x=\mathbb{0}_n})\overline{U}^\dagger \\ =& \alpha(\overline{U}(\!|r|\!)_{\theta,x=A}\overline{U}^\dagger) + \beta(\overline{U}(\!|r|\!)_{\theta,x=B}\overline{U}^\dagger) - (\alpha+\beta-1)(\overline{U}(\!|r|\!)_{\theta,x=\mathbb{0}_n}\overline{U}^\dagger) \\ =& \alpha(\!|Ur|\!)_{\theta,x=A} + \beta(\!|Ur|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|Ur|\!)_{\theta,x=\mathbb{0}_n}\end{aligned}$$

- Sea $t = \pi^m r$. En este caso quiero ver que, reemplazando en (4.1):

$$(\!|\pi^m r|\!)_{\theta,x=\alpha A+\beta B} = \alpha(\!|\pi^m r|\!)_{\theta,x=A} + \beta(\!|\pi^m r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|\pi^m r|\!)_{\theta,x=\mathbb{0}_n}$$

Desarrollando el lado izquierdo:

$$\begin{aligned}(\!|\pi^m r|\!)_{\theta,x=\alpha A+\beta B} =& \bigoplus_{i=1}^{2^m}\left(\overline{\pi}_i(\!|r|\!)_{\theta,x=\alpha A+\beta B}\overline{\pi}_i^\dagger\right) \\ \overset{HI}{=}& \bigoplus_{i=1}^{2^m}\left(\overline{\pi}_i(\alpha(\!|r|\!)_{\theta,x=A} + \beta(\!|r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|r|\!)_{\theta,x=\mathbb{0}_n})\overline{\pi}_i^\dagger\right) \\ =& \bigoplus_{i=1}^{2^m}\left(\alpha\overline{\pi}_i(\!|r|\!)_{\theta,x=A}\overline{\pi}_i^\dagger + \beta\overline{\pi}_i(\!|r|\!)_{\theta,x=B}\overline{\pi}_i^\dagger - (\alpha+\beta-1)\overline{\pi}_i(\!|r|\!)_{\theta,x=\mathbb{0}_n}\overline{\pi}_i^\dagger\right) \\ =& \alpha\bigoplus_{i=1}^{2^m}\left(\overline{\pi}_i(\!|r|\!)_{\theta,x=A}\overline{\pi}_i^\dagger\right) + \beta\bigoplus_{i=1}^{2^m}\left(\overline{\pi}_i(\!|r|\!)_{\theta,x=B}\overline{\pi}_i^\dagger\right) - (\alpha+\beta-1)\bigoplus_{i=1}^{2^m}\left(\overline{\pi}_i(\!|r|\!)_{\theta,x=\mathbb{0}_n}\overline{\pi}_i^\dagger\right) \\ =& \alpha(\!|\pi^m r|\!)_{\theta,x=A} + \beta(\!|\pi^m r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|\pi^m r|\!)_{\theta,x=\mathbb{0}_n}\end{aligned}$$

- Sea $t = r \otimes s$. En este caso quiero ver que, reemplazando en (4.1):

$$(\!|r\otimes s|\!)_{\theta,x=\alpha A+\beta B} = \alpha(\!|r\otimes s|\!)_{\theta,x=A} + \beta(\!|r\otimes s|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|r\otimes s|\!)_{\theta,x=\mathbb{0}_n} \quad (4.6)$$

Como el cálculo es afín, o bien vale $x \in \mathsf{FV}(r)$ o bien vale $x \in \mathsf{FV}(s)$.

- Si $x \in \mathsf{FV}(r)$, de (4.6) quiero ver que:

$$(\!|r|\!)_{\theta,x=\alpha A+\beta B} \otimes (\!|s|\!)_\theta = \alpha(\!|r|\!)_{\theta,x=A} \otimes (\!|s|\!)_\theta + \beta(\!|r|\!)_{\theta,x=B} \otimes (\!|s|\!)_\theta - (\alpha+\beta-1)(\!|r|\!)_{\theta,x=\mathbb{0}_n} \otimes (\!|s|\!)_\theta$$

Desarrollando el lado izquierdo:

$$\begin{aligned}(\!|r|\!)_{\theta,x=\alpha A+\beta B} \otimes (\!|s|\!)_\theta \overset{HI}{=}& (\alpha(\!|r|\!)_{\theta,x=A} + \beta(\!|r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|r|\!)_{\theta,x=\mathbb{0}_n}) \otimes (\!|s|\!)_\theta \\ =& \alpha(\!|r|\!)_{\theta,x=A} \otimes (\!|s|\!)_\theta + \beta(\!|r|\!)_{\theta,x=B} \otimes (\!|s|\!)_\theta - (\alpha+\beta-1)(\!|r|\!)_{\theta,x=\mathbb{0}_n} \otimes (\!|s|\!)_\theta\end{aligned}$$

- Si $x \in \mathsf{FV}(s)$, de (4.6) quiero ver que:

  $$(\!|r|\!)_\theta \otimes (\!|s|\!)_{\theta,x=\alpha A+\beta B} = \alpha(\!|r|\!)_\theta \otimes (\!|s|\!)_{\theta,x=A} + \beta(\!|r|\!)_\theta \otimes (\!|s|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|r|\!)_\theta \otimes (\!|s|\!)_{\theta,x=\mathbb{0}_n}$$

  Desarrollando el lado izquierdo:

  $$\begin{aligned}(\!|r|\!)_\theta \otimes (\!|s|\!)_{\theta,x=\alpha A+\beta B} &\overset{HI}{=} (\!|r|\!)_\theta \otimes (\alpha(\!|s|\!)_{\theta,x=A} + \beta(\!|s|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|s|\!)_{\theta,x=\mathbb{0}_n}) \\ &= \alpha(\!|r|\!)_\theta \otimes (\!|s|\!)_{\theta,x=A} + \beta(\!|r|\!)_\theta \otimes (\!|s|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|r|\!)_\theta \otimes (\!|s|\!)_{\theta,x=\mathbb{0}_n}\end{aligned}$$

- Sea $t = \mathsf{letcase}^\circ\ y = r\ \mathsf{in}\ \{t_1, \ldots, t_m\}$. Reemplazando t en (4.1), quiero ver que:

$$\begin{aligned}(\!|\mathsf{letcase}^\circ\ y = r\ \mathsf{in}\ \{t_1, \ldots, t_m\}|\!)_{\theta,x=\alpha A+\beta B} =& \alpha(\!|\mathsf{letcase}^\circ\ y = r\ \mathsf{in}\ \{t_1, \ldots, t_m\}|\!)_{\theta,x=A} \\ &+ \beta(\!|\mathsf{letcase}^\circ\ y = r\ \mathsf{in}\ \{t_1, \ldots, t_m\}|\!)_{\theta,x=B} \\ &- (\alpha+\beta-1)(\!|\mathsf{letcase}^\circ\ y = r\ \mathsf{in}\ \{t_1, \ldots, t_m\}|\!)_{\theta,x=\mathbb{0}_n}\end{aligned} \tag{4.7}$$

  De acuerdo al sistema de tipos, o bien vale $x \in \mathsf{FV}(r)$ o bien vale $x \in \mathsf{FV}(t_i)$ para algún i (o varios).

- Si $x \in \mathsf{FV}(r)$, llamo $\rho^i_{\alpha A+\beta B}$, ρ^i_A, ρ^i_B, ρ^i_0 para $i \in \{1, \ldots, m\}$ tal que:

  $$\begin{aligned}(\!|r|\!)_{\theta,x=\alpha A+\beta B} &= \bigoplus_{i=1}^m \rho^i_{\alpha A+\beta B} \\ (\!|r|\!)_{\theta,x=A} &= \bigoplus_{i=1}^m \rho^i_A \\ (\!|r|\!)_{\theta,x=B} &= \bigoplus_{i=1}^m \rho^i_B \\ (\!|r|\!)_{\theta,x=\mathbb{0}_n} &= \bigoplus_{i=1}^m \rho^i_0\end{aligned}$$

  Por otro lado, usando la hipótesis inductiva en r, se tiene:

  $$(\!|r|\!)_{\theta,x=\alpha A+\beta B} = \alpha(\!|r|\!)_{\theta,x=A} + \beta(\!|r|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|r|\!)_{\theta,x=\mathbb{0}_n}$$

  Es decir que:

  $$\bigoplus_{i=1}^m \rho^i_{\alpha A+\beta B} = \alpha \bigoplus_{i=1}^m \rho^i_A + \beta \bigoplus_{i=1}^m \rho^i_B - (\alpha+\beta-1) \bigoplus_{i=1}^m \rho^i_0$$

  Por lo tanto para todo i vale que:

  $$\rho^i_{\alpha A+\beta B} = \alpha\rho^i_A + \beta\rho^i_B - (\alpha+\beta-1)\rho^i_0 \tag{4.8}$$

  Aplicando la traza se tiene:

  $$\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) = \alpha\mathsf{tr}\left(\rho^i_A\right) + \beta\mathsf{tr}\left(\rho^i_B\right) - (\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right) \tag{4.9}$$

En general para todo ρ vale por hipótesis inductiva en t_i (con $\alpha = \frac{1}{\mathsf{tr}(\rho)}$, $A = \rho$, $\beta = 0$, y n' la dimensión adecuada) que:

$$(\!|t_i|\!)_{\theta,y=\frac{\rho}{\mathsf{tr}(\rho)}} = \frac{1}{\mathsf{tr}\,(\rho)}(\!|t_i|\!)_{\theta,y=\rho} - (\frac{1}{\mathsf{tr}\,(\rho)} + 0 - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}$$

Es decir,

$$(\!|t_i|\!)_{\theta,y=\frac{\rho}{\mathsf{tr}(\rho)}} = \frac{1}{\mathsf{tr}\,(\rho)}(\!|t_i|\!)_{\theta,y=\rho} + (1 - \frac{1}{\mathsf{tr}\,(\rho)})(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}$$

Multiplicando a ambos lados por $\mathsf{tr}\,(\rho)$ se tiene:

$$\mathsf{tr}\,(\rho)\,(\!|t_i|\!)_{\theta,y=\frac{\rho}{\mathsf{tr}(\rho)}} = (\!|t_i|\!)_{\theta,y=\rho} + (\mathsf{tr}\,(\rho) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}} \tag{4.10}$$

Por otra parte, de (4.8) se tiene que:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} = (\!|t_i|\!)_{\theta,y=\alpha\rho^i_A+\beta\rho^i_B-(\alpha+\beta-1)\rho^i_0}$$

Por hipótesis inductiva, con $\alpha' = \alpha$, $A' = \rho^i_A$, $\beta' = 1$, $B' = \beta\rho^i_B - (\alpha+\beta-1)\rho^i_0$, se tiene que:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} = \alpha(\!|t_i|\!)_{\theta,y=\rho^i_A} + (\!|t_i|\!)_{\theta,y=\beta\rho^i_B-(\alpha+\beta-1)\rho^i_0} - \alpha(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}$$

Usando la hipótesis inductiva en el segundo término con $\alpha' = \beta$, $A' = \rho^i_B$, $\beta' = -(\alpha+\beta-1)$ y $B' = \rho^i_0$ queda:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} = \alpha(\!|t_i|\!)_{\theta,y=\rho^i_A} + \beta(\!|t_i|\!)_{\theta,y=\rho^i_B} - (\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\rho^i_0} \tag{4.11}$$

Por definición, y como $x \in \mathsf{FV}(r)$ pero $x \notin \mathsf{FV}(t_i)$ para todo i, para ver (4.7) quiero ver que:

$$\begin{aligned}\sum_{i=1}^{n} \mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)(\!|t_i|\!)_{\theta,y=\widetilde{\rho^i_{\alpha A+\beta B}}} =& \alpha\sum_{i=1}^{n} \mathsf{tr}\left(\rho^i_A\right)(\!|t_i|\!)_{\theta,y=\widetilde{\rho^i_A}} \\ &+ \beta\sum_{i=1}^{n} \mathsf{tr}\left(\rho^i_B\right)(\!|t_i|\!)_{\theta,y=\widetilde{\rho^i_B}} \\ &- (\alpha+\beta-1)\sum_{i=1}^{n} \mathsf{tr}\left(\rho^i_0\right)(\!|t_i|\!)_{\theta,y=\widetilde{\rho^i_0}}\end{aligned}$$

Donde

$$\widetilde{\phi} = \begin{cases} \mathbb{0}_{n'} & \text{si } \mathsf{tr}\,(\phi) = 0 \\ \frac{\phi}{\mathsf{tr}(\phi)} & \text{en otro caso} \end{cases} \tag{4.12}$$

Voy a ver la igualdad lugar a lugar en la sumatoria, es decir que para todo i se tiene que

$$\begin{aligned}\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)(\!|t_i|\!)_{\theta,y=\widetilde{\rho^i_{\alpha A+\beta B}}} =& \alpha\mathsf{tr}\left(\rho^i_A\right)(\!|t_i|\!)_{\theta,y=\widetilde{\rho^i_A}} \\ &+ \beta\mathsf{tr}\left(\rho^i_B\right)(\!|t_i|\!)_{\theta,y=\widetilde{\rho^i_B}} \\ &- (\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right)(\!|t_i|\!)_{\theta,y=\widetilde{\rho^i_0}}\end{aligned} \tag{4.13}$$

1. Caso $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) \neq 0$, $\mathsf{tr}\left(\rho^i_A\right) \neq 0$, $\mathsf{tr}\left(\rho^i_B\right) \neq 0$, $\mathsf{tr}\left(\rho^i_0\right) \neq 0$
   Evaluando (4.13) quiero ver que:

$$\begin{aligned}\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)(\!|t_i|\!)_{\theta,y=\frac{\rho^i_{\alpha A+\beta B}}{\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)}} =&\alpha\mathsf{tr}\left(\rho^i_A\right)(\!|t_i|\!)_{\theta,y=\frac{\rho^i_A}{\mathsf{tr}\left(\rho^i_A\right)}}\\ &+\beta\mathsf{tr}\left(\rho^i_B\right)(\!|t_i|\!)_{\theta,y=\frac{\rho^i_B}{\mathsf{tr}\left(\rho^i_B\right)}}\\ &-(\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right)(\!|t_i|\!)_{\theta,y=\frac{\rho^i_0}{\mathsf{tr}\left(\rho^i_0\right)}}\end{aligned}$$

   Usando (4.10) esto es equivalente a ver que:

$$\begin{aligned}(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}}+(\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)-1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}} =&\alpha((\!|t_i|\!)_{\theta,y=\rho^i_A}+(\mathsf{tr}\left(\rho^i_A\right)-1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}})\\ &+\beta((\!|t_i|\!)_{\theta,y=\rho^i_B}+(\mathsf{tr}\left(\rho^i_B\right)-1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}})\\ &-(\alpha+\beta-1)((\!|t_i|\!)_{\theta,y=\rho^i_0}+(\mathsf{tr}\left(\rho^i_0\right)-1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}})\end{aligned}$$

   Reordenando esto resulta equivalente a:

$$\begin{aligned}(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} =&\alpha(\!|t_i|\!)_{\theta,y=\rho^i_A}+\beta(\!|t_i|\!)_{\theta,y=\rho^i_B}-(\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\rho^i_0}+\\ &(-\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)+\alpha\mathsf{tr}\left(\rho^i_A\right)+\beta\mathsf{tr}\left(\rho^i_B\right)-(\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right))(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}\end{aligned}$$

   Usando (4.9) se anula el último término, y queda:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}}=\alpha(\!|t_i|\!)_{\theta,y=\rho^i_A}+\beta(\!|t_i|\!)_{\theta,y=\rho^i_B}-(\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\rho^i_0}$$

   Se obtiene (4.11), y por lo tanto vale.
2. Casos $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) \neq 0$, $\mathsf{tr}\left(\rho^i_A\right) = 0$, $\mathsf{tr}\left(\rho^i_B\right) \neq 0$, $\mathsf{tr}\left(\rho^i_0\right) \neq 0$ y $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) \neq 0$, $\mathsf{tr}\left(\rho^i_A\right) \neq 0$, $\mathsf{tr}\left(\rho^i_B\right) = 0$, $\mathsf{tr}\left(\rho^i_0\right) \neq 0$ (análogos)
   Pruebo el caso donde $\mathsf{tr}\left(\rho^i_B\right) = 0$. Evaluando en (4.13), quiero ver que:

$$\begin{aligned}\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)(\!|t_i|\!)_{\theta,y=\frac{\rho^i_{\alpha A+\beta B}}{\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)}} =&\alpha\mathsf{tr}\left(\rho^i_A\right)(\!|t_i|\!)_{\theta,y=\frac{\rho^i_A}{\mathsf{tr}\left(\rho^i_A\right)}}\\ &-(\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right)(\!|t_i|\!)_{\theta,y=\frac{\rho^i_0}{\mathsf{tr}\left(\rho^i_0\right)}}\end{aligned}$$

   Usando (4.10) esto es equivalente a ver que:

$$\begin{aligned}(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}}+(\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)-1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}} =&\alpha((\!|t_i|\!)_{\theta,y=\rho^i_A}+(\mathsf{tr}\left(\rho^i_A\right)-1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}})\\ &-(\alpha+\beta-1)((\!|t_i|\!)_{\theta,y=\rho^i_0}+(\mathsf{tr}\left(\rho^i_0\right)-1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}})\end{aligned}$$

   Reordenando esto resulta equivalente a:

$$\begin{aligned}(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} =&\alpha(\!|t_i|\!)_{\theta,y=\rho^i_A}-(\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\rho^i_0}+\\ &(-\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)+\alpha\mathsf{tr}\left(\rho^i_A\right)-(\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right)+\beta)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}\end{aligned}$$

   Usando (4.9) evaluada en este caso, donde $\mathsf{tr}\left(\rho^i_B\right) = 0$, queda:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}}=\alpha(\!|t_i|\!)_{\theta,y=\rho^i_A}-(\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\rho^i_0}+\beta(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}$$

   Que es equivalente a (4.11) en este caso, porque $\mathsf{tr}\left(\rho^i_B\right) = 0$ implica que $\rho^i_B = \mathbb{0}_{n'}$ por el lema (1.1.10).

3. Caso $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) \neq 0$, $\mathsf{tr}\left(\rho^i_A\right) \neq 0$, $\mathsf{tr}\left(\rho^i_B\right) \neq 0$, $\mathsf{tr}\left(\rho^i_0\right) = 0$
Evaluando en (4.13), quiero ver que:

$$\begin{aligned}\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_{\alpha A+\beta B}}{\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)}} =& \alpha \mathsf{tr}\left(\rho^i_A\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_A}{\mathsf{tr}\left(\rho^i_A\right)}} \\ &+ \beta \mathsf{tr}\left(\rho^i_B\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_B}{\mathsf{tr}\left(\rho^i_B\right)}}\end{aligned}$$

Usando (4.10) esto es equivalente a ver que:

$$\begin{aligned}(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} + (\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}} =& \alpha((\!|t_i|\!)_{\theta,y=\rho^i_A} + (\mathsf{tr}\left(\rho^i_A\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}) \\ &+ \beta((\!|t_i|\!)_{\theta,y=\rho^i_B} + (\mathsf{tr}\left(\rho^i_B\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}})\end{aligned}$$

Reordenando esto resulta equivalente a:

$$\begin{aligned}(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} =& \alpha(\!|t_i|\!)_{\theta,y=\rho^i_A} + \beta(\!|t_i|\!)_{\theta,y=\rho^i_B} + \\ &(-\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) + \alpha \mathsf{tr}\left(\rho^i_A\right) + \beta \mathsf{tr}\left(\rho^i_B\right) + 1 - \alpha - \beta)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}\end{aligned}$$

Usando (4.9) evaluada en este caso, donde $\mathsf{tr}\left(\rho^i_0\right) = 0$, queda:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} = \alpha(\!|t_i|\!)_{\theta,y=\rho^i_A} + \beta(\!|t_i|\!)_{\theta,y=\rho^i_B} - (\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}$$

Que es equivalente a (4.11) en este caso, porque $\mathsf{tr}\left(\rho^i_0\right) = 0$ implica que $\rho^i_0 = \mathbb{0}_{n'}$ por el lema (1.1.10).

4. Caso $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) \neq 0$, $\mathsf{tr}\left(\rho^i_A\right) = 0$, $\mathsf{tr}\left(\rho^i_B\right) = 0$, $\mathsf{tr}\left(\rho^i_0\right) \neq 0$
Evaluando en (4.13), quiero ver que:

$$\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_{\alpha A+\beta B}}{\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)}} = -(\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_0}{\mathsf{tr}\left(\rho^i_0\right)}}$$

Usando (4.10) esto es equivalente a ver que:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} + (\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}} = -(\alpha+\beta-1)((\!|t_i|\!)_{\theta,y=\rho^i_0} + (\mathsf{tr}\left(\rho^i_0\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}})$$

Reordenando esto resulta equivalente a:

$$\begin{aligned}(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} =& -(\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\rho^i_0} + \\ &(-\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) - (\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right) + \alpha + \beta)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}\end{aligned}$$

Usando (4.9) evaluada en este caso, donde $\mathsf{tr}\left(\rho^i_A\right) = \mathsf{tr}\left(\rho^i_B\right) = 0$, queda:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} = -(\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\rho^i_0} + (\alpha+\beta)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}$$

Que es equivalente a (4.11) en este caso, porque $\mathsf{tr}\left(\rho^i_A\right) = \mathsf{tr}\left(\rho^i_B\right) = 0$ implica que $\rho^i_A = \rho^i_B = \mathbb{0}_{n'}$ por el lema (1.1.10).

5. Casos $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) \neq 0$, $\mathsf{tr}\left(\rho^i_A\right) = 0$, $\mathsf{tr}\left(\rho^i_B\right) \neq 0$, $\mathsf{tr}\left(\rho^i_0\right) = 0$ y $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) \neq 0$, $\mathsf{tr}\left(\rho^i_A\right) \neq 0$, $\mathsf{tr}\left(\rho^i_B\right) = 0$, $\mathsf{tr}\left(\rho^i_0\right) = 0$ (análogos)
Pruebo el caso donde $\mathsf{tr}\left(\rho^i_B\right) = 0$. Evaluando en (4.13), quiero ver que:

$$\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_{\alpha A+\beta B}}{\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right)}} = \alpha\mathsf{tr}\left(\rho^i_A\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_A}{\mathsf{tr}\left(\rho^i_A\right)}}$$

Usando (4.10) esto es equivalente a ver que:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} + (\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}} = \alpha((\!|t_i|\!)_{\theta,y=\rho^i_A} + (\mathsf{tr}\left(\rho^i_A\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}})$$

Reordenando esto resulta equivalente a:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} = \alpha(\!|t_i|\!)_{\theta,y=\rho^i_A} + (-\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) + \alpha\mathsf{tr}\left(\rho^i_A\right) + 1 - \alpha)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}$$

Usando (4.9) evaluada en este caso, donde $\mathsf{tr}\left(\rho^i_B\right) = \mathsf{tr}\left(\rho^i_0\right) = 0$, queda:

$$(\!|t_i|\!)_{\theta,y=\rho^i_{\alpha A+\beta B}} = \alpha(\!|t_i|\!)_{\theta,y=\rho^i_A} + (1-\alpha)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}$$

Que es equivalente a (4.11) en este caso, porque $\mathsf{tr}\left(\rho^i_B\right) = \mathsf{tr}\left(\rho^i_0\right) = 0$ implica que $\rho^i_B = \rho^i_0 = \mathbb{0}_{n'}$ por el lema (1.1.10).

6. Caso $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) = 0$, $\mathsf{tr}\left(\rho^i_A\right) \neq 0$, $\mathsf{tr}\left(\rho^i_B\right) \neq 0$, $\mathsf{tr}\left(\rho^i_0\right) \neq 0$
Evaluando en (4.13), con n'' la dimensión adecuada, quiero ver que:

$$\mathbb{0}_{n''} = \alpha\mathsf{tr}\left(\rho^i_A\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_A}{\mathsf{tr}\left(\rho^i_A\right)}} + \beta\mathsf{tr}\left(\rho^i_B\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_B}{\mathsf{tr}\left(\rho^i_B\right)}} - (\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right) (\!|t_i|\!)_{\theta,y=\frac{\rho^i_0}{\mathsf{tr}\left(\rho^i_0\right)}}$$

Usando (4.10) esto es equivalente a ver que:

$$\begin{aligned}\mathbb{0}_{n''} =& \alpha((\!|t_i|\!)_{\theta,y=\rho^i_A} + (\mathsf{tr}\left(\rho^i_A\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}) \\ &+ \beta((\!|t_i|\!)_{\theta,y=\rho^i_B} + (\mathsf{tr}\left(\rho^i_B\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}) \\ &- (\alpha+\beta-1)((\!|t_i|\!)_{\theta,y=\rho^i_0} + (\mathsf{tr}\left(\rho^i_0\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}})\end{aligned}$$

Reordenando esto resulta equivalente a:

$$\begin{aligned}\mathbb{0}_{n''} =& \alpha(\!|t_i|\!)_{\theta,y=\rho^i_A} + \beta(\!|t_i|\!)_{\theta,y=\rho^i_B} - (\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\rho^i_0} + \\ &(\alpha\mathsf{tr}\left(\rho^i_A\right) + \beta\mathsf{tr}\left(\rho^i_B\right) - (\alpha+\beta-1)\mathsf{tr}\left(\rho^i_0\right) - 1)(\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}\end{aligned}$$

Usando (4.9) evaluada en este caso, donde $\mathsf{tr}\left(\rho_\alpha A + \beta B^i\right) = 0$, queda:

$$\mathbb{0}_{n''} = \alpha(\!|t_i|\!)_{\theta,y=\rho^i_A} + \beta(\!|t_i|\!)_{\theta,y=\rho^i_B} - (\alpha+\beta-1)(\!|t_i|\!)_{\theta,y=\rho^i_0} - (\!|t_i|\!)_{\theta,y=\mathbb{0}_{n'}}$$

Que es equivalente a (4.11) en este caso, porque $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) = 0$ implica que $\rho^i_{\alpha A+\beta B} = \mathbb{0}_{n'}$ por el lema (1.1.10).

7. Casos $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) = 0$, $\mathsf{tr}\left(\rho^i_A\right) = 0$, $\mathsf{tr}\left(\rho^i_B\right) \neq 0$, $\mathsf{tr}\left(\rho^i_0\right) \neq 0$ y $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) = 0$, $\mathsf{tr}\left(\rho^i_A\right) \neq 0$, $\mathsf{tr}\left(\rho^i_B\right) = 0$, $\mathsf{tr}\left(\rho^i_0\right) \neq 0$ (análogos)

Pruebo el caso donde $\mathsf{tr}\left(\rho_B^i\right) = 0$. Evaluando en (4.13), quiero ver que:

$$\mathbb{0}_{n''} = \alpha \mathsf{tr}\left(\rho_A^i\right) (\!|t_i|\!)_{\theta, y=\frac{\rho_A^i}{\mathsf{tr}\left(\rho_A^i\right)}} - (\alpha+\beta-1)\mathsf{tr}\left(\rho_0^i\right) (\!|t_i|\!)_{\theta, y=\frac{\rho_0^i}{\mathsf{tr}\left(\rho_0^i\right)}}$$

Usando (4.10) esto es equivalente a ver que:

$$\mathbb{0}_{n''} = \alpha((\!|t_i|\!)_{\theta, y=\rho_A^i} + (\mathsf{tr}\left(\rho_A^i\right)-1)(\!|t_i|\!)_{\theta, y=\mathbb{0}_{n'}}) - (\alpha+\beta-1)((\!|t_i|\!)_{\theta, y=\rho_0^i} + (\mathsf{tr}\left(\rho_0^i\right)-1)(\!|t_i|\!)_{\theta, y=\mathbb{0}_{n'}})$$

Reordenando esto resulta equivalente a:

$$\mathbb{0}_{n''} = \alpha(\!|t_i|\!)_{\theta, y=\rho_A^i} - (\alpha+\beta-1)(\!|t_i|\!)_{\theta, y=\rho_0^i} + (\alpha\mathsf{tr}\left(\rho_A^i\right) - (\alpha+\beta-1)\mathsf{tr}\left(\rho_0^i\right) + \beta - 1)(\!|t_i|\!)_{\theta, y=\mathbb{0}_{n'}}$$

Usando (4.9) evaluada en este caso, donde $\mathsf{tr}\left(\rho_\alpha A + \beta B^i\right) = \mathsf{tr}\left(\rho_B^i\right) = 0$, queda:

$$\mathbb{0}_{n''} = \alpha(\!|t_i|\!)_{\theta, y=\rho_A^i} - (\alpha+\beta-1)(\!|t_i|\!)_{\theta, y=\rho_0^i} + (\beta-1)(\!|t_i|\!)_{\theta, y=\mathbb{0}_{n'}}$$

Que es equivalente a (4.11) en este caso, porque $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) = \mathsf{tr}\left(\rho_B^i\right) = 0$ implica que $\rho^i_{\alpha A+\beta B} = \rho_B^i = \mathbb{0}_{n'}$ por el lema (1.1.10).

8. Caso $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) = 0$, $\mathsf{tr}\left(\rho_A^i\right) \neq 0$, $\mathsf{tr}\left(\rho_B^i\right) \neq 0$, $\mathsf{tr}\left(\rho_0^i\right) = 0$
Evaluando en (4.13), quiero ver que:

$$\mathbb{0}_{n''} = \alpha \mathsf{tr}\left(\rho_A^i\right) (\!|t_i|\!)_{\theta, y=\frac{\rho_A^i}{\mathsf{tr}\left(\rho_A^i\right)}} + \beta\mathsf{tr}\left(\rho_B^i\right) (\!|t_i|\!)_{\theta, y=\frac{\rho_B^i}{\mathsf{tr}\left(\rho_B^i\right)}}$$

Usando (4.10) esto es equivalente a ver que:

$$\mathbb{0}_{n''} = \alpha((\!|t_i|\!)_{\theta, y=\rho_A^i} + (\mathsf{tr}\left(\rho_A^i\right)-1)(\!|t_i|\!)_{\theta, y=\mathbb{0}_{n'}}) + \beta((\!|t_i|\!)_{\theta, y=\rho_B^i} + (\mathsf{tr}\left(\rho_B^i\right)-1)(\!|t_i|\!)_{\theta, y=\mathbb{0}_{n'}})$$

Reordenando esto resulta equivalente a:

$$\mathbb{0}_{n''} = \alpha(\!|t_i|\!)_{\theta, y=\rho_A^i} + \beta(\!|t_i|\!)_{\theta, y=\rho_B^i} + (\alpha\mathsf{tr}\left(\rho_A^i\right) + \beta\mathsf{tr}\left(\rho_B^i\right) - \alpha - \beta)(\!|t_i|\!)_{\theta, y=\mathbb{0}_{n'}}$$

Usando (4.9) evaluada en este caso, donde $\mathsf{tr}\left(\rho_\alpha A + \beta B^i\right) = \mathsf{tr}\left(\rho_0^i\right) = 0$, queda:

$$\mathbb{0}_{n''} = \alpha(\!|t_i|\!)_{\theta, y=\rho_A^i} + \beta(\!|t_i|\!)_{\theta, y=\rho_B^i} - (\alpha+\beta)(\!|t_i|\!)_{\theta, y=\mathbb{0}_{n'}}$$

Que es equivalente a (4.11) en este caso, porque $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) = \mathsf{tr}\left(\rho_0^i\right) = 0$ implica que $\rho^i_{\alpha A+\beta B} = \rho_0^i = \mathbb{0}_{n'}$ por el lema (1.1.10).

9. Casos triviales:
El caso donde $\mathsf{tr}\left(\rho^i_{\alpha A+\beta B}\right) = \mathsf{tr}\left(\rho_A^i\right) = \mathsf{tr}\left(\rho_B^i\right) = \mathsf{tr}\left(\rho_0^i\right) = 0$ se cumple trivialmente.
Los demás casos que faltan serían aquellos tales que $\mathsf{tr}\left(\rho_M^i\right) \neq 0$ para algún $M \in \{\alpha A + \beta B, A, B, 0\}$ y las demás trazas valen 0. Pero por (4.9), se tiene que:
   - (Caso $M = \alpha A + \beta B$) $\mathsf{tr}\left(\rho_{\alpha A+\beta B}\right) = 0$ y por lo tanto se cumple (4.13).
   - (Caso $M = A$) Vale $\alpha\mathsf{tr}\left(\rho_A^i\right) = 0$ y o bien $\alpha = 0$ o bien $\mathsf{tr}\left(\rho_A^i\right) = 0$ y en ambos casos se cumple (4.13).
   - (Caso $M = B$) Vale $\beta\mathsf{tr}\left(\rho_B^i\right) = 0$ y o bien $\beta = 0$ o bien $\mathsf{tr}\left(\rho_B^i\right) = 0$ y en ambos casos se cumple (4.13).

- (Caso $M = 0$) Vale $(\alpha + \beta - 1)\mathsf{tr}\left(\rho_0^i\right) = 0$ y o bien $(\alpha + \beta - 1) = 0$ o bien $\mathsf{tr}\left(\rho_0^i\right) = 0$ y en ambos casos se cumple (4.13).

- Si $x \in \mathsf{FV}(t_i)$ para uno o varios i, sean ρ^i tal que:

$$(\!|r|\!)_\theta = \bigoplus_{i=1}^{n} \rho^i$$

De (4.7), en este caso quiero ver que:

$$\begin{aligned}\sum_{i=1}^{n} \mathsf{tr}\left(\rho^i\right) (\!|t_i|\!)_{\theta, x=\alpha A+\beta B, y=\widetilde{\rho^i}} =& \alpha \sum_{i=1}^{n} \mathsf{tr}\left(\rho^i\right) (\!|t_i|\!)_{\theta, x=A, y=\widetilde{\rho^i}} \\ &+ \beta \sum_{i=1}^{n} \mathsf{tr}\left(\rho^i\right) (\!|t_i|\!)_{\theta, x=B, y=\widetilde{\rho^i}} \\ &- (\alpha + \beta - 1) \sum_{i=1}^{n} \mathsf{tr}\left(\rho^i\right) (\!|t_i|\!)_{\theta, x=\mathbb{0}_n, y=\widetilde{\rho^i}}\end{aligned}$$

Con $\widetilde{\cdot}$ definida en (4.12). Voy a ver la igualdad lugar a lugar en la sumatoria, es decir que para todo i vale:

$$\begin{aligned}\mathsf{tr}\left(\rho^i\right) (\!|t_i|\!)_{\theta, x=\alpha A+\beta B, y=\widetilde{\rho^i}} =& \alpha \mathsf{tr}\left(\rho^i\right) (\!|t_i|\!)_{\theta, x=A, y=\widetilde{\rho^i}} + \beta \mathsf{tr}\left(\rho^i\right) (\!|t_i|\!)_{\theta, x=B, y=\widetilde{\rho^i}} \\ &- (\alpha + \beta - 1) \mathsf{tr}\left(\rho^i\right) (\!|t_i|\!)_{\theta, x=\mathbb{0}_n, y=\widetilde{\rho^i}}\end{aligned}$$

Si $\mathsf{tr}\left(\rho^i\right)$, vale. Si no, quiero ver que para todo i:

$$\begin{aligned}(\!|t_i|\!)_{\theta, x=\alpha A+\beta B, y=\frac{\rho^i}{\mathsf{tr}(\rho^i)}} =& \alpha (\!|t_i|\!)_{\theta, x=A, y=\frac{\rho^i}{\mathsf{tr}(\rho^i)}} + \beta (\!|t_i|\!)_{\theta, x=B, y=\frac{\rho^i}{\mathsf{tr}(\rho^i)}} \\ &- (\alpha + \beta - 1) (\!|t_i|\!)_{\theta, x=\mathbb{0}_n, y=\frac{\rho^i}{\mathsf{tr}(\rho^i)}}\end{aligned}$$

Llamo $\theta' = \theta \cup \{y = \frac{\rho^i}{\mathsf{tr}(\rho^i)}\}$. Entonces esto es equivalente a ver que para todo i tal que $\mathsf{tr}\left(\rho^i\right) \neq 0$ vale:

$$(\!|t_i|\!)_{\theta', x=\alpha A+\beta B} = \alpha (\!|t_i|\!)_{\theta', x=A} + \beta (\!|t_i|\!)_{\theta', x=B} - (\alpha + \beta - 1) (\!|t_i|\!)_{\theta', x=\mathbb{0}_n}$$

Que vale por hipótesis inductiva en t_i.

- Sea $t = \sum_i p_i t_i$, con $\sum_i p_i \leq 1$ y $0 < p_i \leq 1$ para todo i. En este caso quiero ver que, reemplazando en (4.1):

$$(\!|\sum_i p_i t_i|\!)_{\theta, x=\alpha A+\beta B} = \alpha (\!|\sum_i p_i t_i|\!)_{\theta, x=A} + \beta (\!|\sum_i p_i t_i|\!)_{\theta, x=B} - (\alpha + \beta - 1) (\!|\sum_i p_i t_i|\!)_{\theta, x=\mathbb{0}_n}$$

Desarrollando el lado izquierdo:

$$\begin{aligned}(\!|\sum_i p_i t_i|\!)_{\theta,x=\alpha A+\beta B} &= \sum_i p_i (\!|t_i|\!)_{\theta,x=\alpha A+\beta B} \\ &\overset{HI}{=} \sum_i p_i(\alpha(\!|t_i|\!)_{\theta,x=A} + \beta(\!|t_i|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|t_i|\!)_{\theta,x=\mathbb{0}_n}) \\ &= \alpha \sum_i p_i (\!|t_i|\!)_{\theta,x=A} + \beta \sum_i p_i (\!|t_i|\!)_{\theta,x=B} - (\alpha+\beta-1)\sum_i p_i (\!|t_i|\!)_{\theta,x=\mathbb{0}_n} \\ &= \alpha (\!|\sum_i p_i t_i|\!)_{\theta,x=A} + \beta (\!|\sum_i p_i t_i|\!)_{\theta,x=B} - (\alpha+\beta-1)(\!|\sum_i p_i t_i|\!)_{\theta,x=\mathbb{0}_n} \quad \square\end{aligned}$$

El siguiente lema establece que las interpretaciones de los términos son matrices de dimensión correspondiente a la de su tipo.

Definición 4.5.2. Sea θ una valuación y $\Gamma \subseteq \mathsf{Var} \times \mathsf{Types}$ un contexto de tipado. $\theta \vDash_{\dim} \Gamma$ si y sólo si para todo par $(x, A) \in \Gamma$ se tiene $\dim(\theta(x)) = \dim(A)$.

Lema 4.5.3. *Sea t un término tal que $\Gamma \vdash t : A$ y $\theta \vDash_{\dim} \Gamma$. Entonces* $\dim((\!|t|\!)_\theta) = \dim(A)$.

Demostración. Por inducción en t.

- Sea $t = x$. Entonces $(x, A) \in \Gamma$ y como $\theta \vDash_{\dim} \Gamma$ se tiene que $\dim((\!|x|\!)_\theta) = \dim(\theta(x)) = \dim(A)$.
- Sea $t = \lambda x.u$. En este caso $A = B \multimap C$. Por definición se tiene $(\!|\lambda x.u|\!)_\theta = \chi_{[a \mapsto (\!|u|\!)_{\theta,x=a}]}$. Sea $\{E_{ij}^B\}$ la base canónica de $\mathbb{C}^{\dim(B)\times\dim(B)}$. Por inversión vale $\Gamma, x : B \vdash u : C$, y como $\theta \vDash_{\dim} \Gamma$, $\dim(E_{ij}^B) = \dim(B)$ y $\dim(\mathbb{0}_{\dim(B)}) = \dim(B)$ se tiene

$$\theta \cup \{x := E_{ij}^B\} \vDash_{\dim} \Gamma, x : B$$
$$\theta \cup \{x := \mathbb{0}_{\dim(B)}\} \vDash_{\dim} \Gamma, x : B$$

  Entonces por hipótesis inductiva

$$\dim((\!|u|\!)_{\theta,x=E_{ij}^B}) = \dim(C)$$
$$\dim((\!|u|\!)_{\theta,x=\mathbb{0}_{\dim(B)}}) = \dim(C)$$

  Finalmente, por definición de $\chi_{[a \mapsto (\!|u|\!)_{\theta,x=a}]}$, $\dim((\!|\lambda x.u|\!)_\theta) = \dim(B)\dim(C)+\dim(C) = \dim(B \multimap C)$.

- Sea $t = uv$. Sean $\Gamma_1, \Gamma_2 = \Gamma$ tales que $\Gamma_1 \vdash u : B \multimap A$ y $\Gamma_2 \vdash v : B$, se tiene $\theta \vDash_{\dim} \Gamma_1$ y $\theta \vDash_{\dim} \Gamma_2$. Por hipótesis inductiva $\dim((\!|u|\!)_\theta) = \dim(B \multimap A)$ y $\dim((\!|v|\!)_\theta) = \dim(B)$. Como $\dim(B \multimap A) = (\dim(B) + 1)\dim(A)$, por definición de $\#$ se tiene $\dim((\!|uv|\!)_\theta) = \dim((\!|u|\!)_\theta \# (\!|v|\!)_\theta) = \dim(A)$.
- Sea $t = \mu_n x.u$. Por inversión se tiene $\Gamma, x : A \vdash u : A$, y por la regla $\multimap_i$ vale $\Gamma \vdash \lambda x.u : A \multimap A$. Por definición se tiene $(\!|\mu_n x.u|\!)_\theta = (\!|\lambda x.u|\!)_\theta \#_n \mathbb{0}_{\dim(A)}$, y usando el caso de la abstracción de más arriba se tiene $\dim((\!|\lambda x.u|\!)_\theta) = \dim(A \multimap A)$. Por lo tanto como $\dim(A \multimap A) = (\dim(A) + 1)\dim(A)$ y cada aplicación de $\#$ devuelve una matriz en $\mathbb{C}^{\dim(A)\times\dim(A)}$ se tiene que $\dim((\!|\mu_n x.u|\!)_\theta) = \dim(A)$.

- Sea $t = \bot_A$. Por definición vale $\dim(\llparenthesis \bot_A \rrparenthesis_\theta) = \dim(\mathbb{0}_{\dim(A)}) = \dim(A)$.
- Sea $t = \rho^n$. En este caso $A = n$ y $\dim(\rho^n) = 2^n$.
- Sea $t = U^m v$. En este caso $A = n$. Por inversión vale $\Gamma \vdash v : n$ y por hipótesis inductiva se tiene $\dim(\llparenthesis v \rrparenthesis_\theta) = 2^n$. Por lo tanto $\dim(\llparenthesis U^m v \rrparenthesis_\theta) = \dim(\overline{U^m} \llparenthesis v \rrparenthesis_\theta \overline{U^m}^\dagger) = 2^n$.
- Sea $t = \pi^m u$. En este caso $A = (m, n)$. Por inversión vale $\Gamma \vdash u : n$ y por hipótesis inductiva se tiene $\dim(\llparenthesis u \rrparenthesis_\theta) = 2^n$. Por lo tanto $\dim(\llparenthesis \pi^m u \rrparenthesis_\theta) = \dim(\bigoplus_{i=0}^{2^m-1} \overline{\pi_i} \llparenthesis u \rrparenthesis_\theta \overline{\pi^m}^\dagger) = 2^m 2^n$, ya que $\dim(\overline{\pi_i} \llparenthesis u \rrparenthesis_\theta \overline{\pi^m}^\dagger) = 2^n$ para todo i.
- Sea $t = u \otimes v$. En este caso $A = n + m$. Sean $\Gamma_1, \Gamma_2 = \Gamma$ tales que $\Gamma_1 \vdash u : n$ y $\Gamma_2 \vdash v : m$, por hipótesis inductiva como $\theta \vDash_{\dim} \Gamma_1$ y $\theta \vDash_{\dim} \Gamma_2$ se tiene $\dim(\llparenthesis u \rrparenthesis_\theta) = 2^n$ y $\dim(\llparenthesis v \rrparenthesis_\theta) = 2^m$. Por lo tanto $\dim(\llparenthesis u \otimes v \rrparenthesis_\theta) = \dim(\llparenthesis u \rrparenthesis_\theta \otimes \llparenthesis v \rrparenthesis_\theta) = 2^{n+m}$.
- Sea $t = \sum_{i=1}^n p_i t_i$. Por inversión se tiene $\Gamma \vdash t_i : A$ para todo i, y por hipótesis inductiva $\dim(\llparenthesis t_i \rrparenthesis_\theta) = \dim(A)$. Por lo tanto $\dim(\llparenthesis \sum_{i=1}^n p_i t_i \rrparenthesis_\theta) = \dim(\sum_{i=1}^n p_i \llparenthesis t_i \rrparenthesis_\theta) = \dim(A)$.
- Sea $t = \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$. Sean $\Gamma_0, \ldots, \Gamma_{2^m-1}, \Gamma' = \Gamma$ tales que $\Gamma_i, x : n \vdash t_i : A$ para todo i y $\Gamma' \vdash r : (m, n)$. Entonces $\theta \vDash_{\dim} \Gamma'$ y por hipótesis inductiva $\dim(\llparenthesis r \rrparenthesis_\theta) = \dim((m, n)) = 2^{n+m}$. Sea ρ_i con $0 \leq i \leq 2^m - 1$ cada una de las submatrices de $2^n \times 2^n$ en la diagonal de $\llparenthesis r \rrparenthesis_\theta$, defino ρ_i' como ρ_i si $\mathsf{tr}(\rho_i) = 0$ y como $\frac{\rho_i}{\mathsf{tr}(\rho_i)}$ sino. Como $\dim(\rho_i') = 2^n$ se tiene $\theta \cup \{x := \rho_i'\} \vDash_{\dim} \Gamma_i, x : n$ para todo i y por hipótesis inductiva $\dim(t_i) = \dim(A)$. Por lo tanto $\dim(\llparenthesis \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \rrparenthesis_\theta) = \dim(\sum_{i=0}^{2^m-1} \mathsf{tr}(\rho_i)\, \llparenthesis t_i \rrparenthesis_{\theta, x=\rho_i'}) = \dim(A)$.

□

Definición 4.5.4. Sea θ una valuación y $\Gamma \subseteq \mathsf{Var} \times \mathsf{Types}$ un contexto de tipado. Decimos que θ satisface a Γ, notado como $\theta \vDash \Gamma$, si y sólo si para todo par $(x, A) \in \Gamma$ se tiene $\theta(x) \in \llparenthesis A \rrparenthesis$.

El siguiente lema establece que la aplicación se comporta de la forma esperada respecto a la valuación usada en la interpretación. Su demostración se basa en el lema anterior de linealidad.

Lema 4.5.5 (Aplicación)**.** *Si $\Gamma, x : A \vdash t : B$ y $\theta \vDash \Gamma$, entonces para todo $a \in \mathbb{C}^{\dim(A) \times \dim(A)}$ vale*

$$\llparenthesis \lambda x.t \rrparenthesis_\theta \,\#\, a = \llparenthesis t \rrparenthesis_{\theta, x=a}$$

Demostración. Por definición se tiene:

$$\begin{aligned}
\llparenthesis \lambda x.t \rrparenthesis_\theta &= \chi_{[a \mapsto \llparenthesis t \rrparenthesis_{\theta, x=a}]} \\
&= \begin{pmatrix} \llparenthesis t \rrparenthesis_{\theta, x=E_{11}^A} - \llparenthesis t \rrparenthesis_{\theta, x=\mathbb{0}_{\dim(A)}} & \cdots & \llparenthesis t \rrparenthesis_{\theta, x=E_{1n}^A} - \llparenthesis t \rrparenthesis_{\theta, x=\mathbb{0}_{\dim(A)}} \\ \vdots & \ddots & \vdots \\ \llparenthesis t \rrparenthesis_{\theta, x=E_{n1}^A} - \llparenthesis t \rrparenthesis_{\theta, x=\mathbb{0}_{\dim(A)}} & \cdots & \llparenthesis t \rrparenthesis_{\theta, x=E_{nn}^A} - \llparenthesis t \rrparenthesis_{\theta, x=\mathbb{0}_{\dim(A)}} \end{pmatrix} \oplus \llparenthesis t \rrparenthesis_{\theta, x=\mathbb{0}_{\dim(A)}}
\end{aligned}$$

Sea $\{E_{ij}^A\}$ la base canónica de $\mathbb{C}^{\dim(A)\times\dim(A)}$, descomponiendo a en la base y aplicando $(\!|\lambda x.t|\!)_\theta$ mediante $\#$:

$$\begin{aligned}(\!|\lambda x.t|\!)_\theta \# a =& (\!|\lambda x.t|\!)_\theta \# \left(\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{ij}^A\right)\\ =& \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\left((\!|t|\!)_{\theta,x=E_{ij}^A} - (\!|t|\!)_{\theta,x=\mathbb{0}_{\dim(A)}}\right) + (\!|t|\!)_{\theta,x=\mathbb{0}_{\dim(A)}}\end{aligned}$$

Por el lema (4.5.1), $(\!|t|\!)_{\theta,x=E_{ij}^A} - (\!|t|\!)_{\theta,x=\mathbb{0}_{\dim(A)}}$ es lineal en E_{ij}^A, entonces se tiene:

$$(\!|\lambda x.t|\!)_\theta \# a = (\!|t|\!)_{\theta,x=\sum\limits_{ij} a_{ij}E_{ij}^A} - (\!|t|\!)_{\theta,x=\mathbb{0}_{\dim(A)}} + (\!|t|\!)_{\theta,x=\mathbb{0}_{\dim(A)}} = (\!|t|\!)_{\theta,x=a} \qquad \square$$

El siguiente es un lema de sustitución habitual, para ver que la interpretación de los términos está bien definida respecto a la sustitución de variables.

Lema 4.5.6 (Sustitución)**.** $(\!|t[x := r]|\!)_\theta = (\!|t|\!)_{\theta,x=(\!|r|\!)_\theta}$

Demostración. Por inducción en t.

- Sea $t = x$, en este caso quiero ver que $(\!|x[x := r]|\!)_\theta = (\!|x|\!)_{\theta,x=(\!|r|\!)_\theta}$. Por un lado se tiene que $(\!|x[x := r]|\!)_\theta = (\!|r|\!)_\theta$ y por otro $(\!|x|\!)_{\theta,x=(\!|r|\!)_\theta} = \theta'(x) = (\!|r|\!)_\theta$, donde $\theta' = \theta \cup \{x = (\!|r|\!)_\theta\}$.
- Sea $t = y \neq x$, quiero ver que $(\!|y[x := r]|\!)_\theta = (\!|y|\!)_{\theta,x=(\!|r|\!)_\theta}$. Como $x \neq y$, se tiene que ambos lados son iguales a $(\!|y|\!)_\theta$.
- Sea $t = \lambda y.s$, en este caso quiero ver que $(\!|(\lambda y.s)[x := r]|\!)_\theta = (\!|\lambda y.s|\!)_{\theta,x=(\!|r|\!)_\theta}$.

  Desarrollando el lado izquierdo se tiene:

  $$(\!|(\lambda y.s)[x := r]|\!)_\theta = (\!|\lambda y.(s[x := r])|\!)_\theta = \chi_{[a\mapsto (\!|s[x:=r]|\!)_{\theta,y=a}]}$$

  Por hipótesis inductiva esto es igual a $\chi_{[a\mapsto (\!|s|\!)_{\theta,y=a,x=(\!|r|\!)_{\theta,y=a}}]}$, y como y no pertenece a las variables libres de r, se tiene que $(\!|r|\!)_{\theta,y=a} = (\!|r|\!)_\theta$. Entonces esto es igual a $\chi_{[a\mapsto (\!|s|\!)_{\theta,y=a,x=(\!|r|\!)_\theta}]}$, que es lo mismo que $(\!|\lambda y.s|\!)_{\theta,x=(\!|r|\!)_\theta}$.
- Sea $t = s_1 s_2$, en este caso quiero ver que $(\!|(s_1 s_2)[x := r]|\!)_\theta = (\!|s_1 s_2|\!)_{\theta,x=(\!|r|\!)_\theta}$. Como el cálculo es afín hay dos casos disjuntos: o bien $x \in \mathsf{FV}(s_1)$ y $x \notin \mathsf{FV}(s_2)$, o bien $x \notin \mathsf{FV}(s_1)$ y $x \in \mathsf{FV}(s_2)$.
  - Para el primer caso se tiene desarrollando el lado izquierdo:

    $$(\!|(s_1 s_2)[x := r]|\!)_\theta = (\!|(s_1[x := r])s_2|\!)_\theta = (\!|s_1[x := r]|\!)_\theta \# (\!|s_2|\!)_\theta$$

    Por hipótesis inductiva esto es igual a $(\!|s_1|\!)_{\theta,x=(\!|r|\!)_\theta} \# (\!|s_2|\!)_\theta$. Como $x \notin \mathsf{FV}(s_2)$, esto resulta igual a $(\!|s_1|\!)_{\theta,x=(\!|r|\!)_\theta} \# (\!|s_2|\!)_{\theta,x=(\!|r|\!)_\theta} = (\!|s_1 s_2|\!)_{\theta,x=(\!|r|\!)_\theta}$.
  - Para el segundo caso, desarrollando el lado izquierdo se tiene:

    $$(\!|(s_1 s_2)[x := r]|\!)_\theta = (\!|s_1(s_2[x := r])|\!)_\theta = (\!|s_1|\!)_\theta \# (\!|s_2[x := r]|\!)_\theta$$

    Por hipótesis inductiva, esto es igual a $(\!|s_1|\!)_\theta \# (\!|s_2|\!)_{\theta,x=(\!|r|\!)_\theta}$. Como $x \notin \mathsf{FV}(s_1)$, resulta igual a $(\!|s_1|\!)_{\theta,x=(\!|r|\!)_\theta} \# (\!|s_2|\!)_{\theta,x=(\!|r|\!)_\theta} = (\!|s_1 s_2|\!)_{\theta,x=(\!|r|\!)_\theta}$.

- Sea $t = \mu_n y.s$. En este caso quiero ver que $(\!|(\mu_n y.s)[x := r]|\!)_\theta = (\!|\mu_n y.s|\!)_{\theta, x=(\!|r|\!)_\theta}$. Desarrollando el lado izquierdo se tiene:

$$(\!|(\mu_n y.s)[x := r]|\!)_\theta = (\!|\mu_n y.(s[x := r])|\!)_\theta = (\!|\lambda y.(s[x := r])|\!)_\theta \#_n \mathbb{0}_A$$

  De acuerdo a la demostración para el caso $t = \lambda y.s$ visto más arriba, esto es igual a:

$$(\!|\lambda y.s|\!)_{\theta, x=(\!|r|\!)_\theta} \#_n \mathbb{0}_A = (\!|\mu_n y.s|\!)_{\theta, x=(\!|r|\!)_\theta}$$

- Sea $t = \bot_A$, este caso es análogo al de $t = y \neq x$.
- Sea $t = \rho^n$, este caso es análogo al de $t = y \neq x$.
- Sea $t = U^m s$, en este caso quiero ver que $(\!|(U^m s)[x := r]|\!)_\theta = (\!|U^m s|\!)_{\theta, x=(\!|r|\!)_\theta}$. Desarrollando el lado izquierdo se tiene:

$$(\!|(U^m s)[x := r]|\!)_\theta = (\!|U^m (s[x := r])|\!)_\theta = \overline{U^m} (\!|s[x := r]|\!)_\theta \overline{U^m}^\dagger$$

  Por hipótesis inductiva esto resulta igual a $\overline{U^m} (\!|s|\!)_{\theta, x=(\!|r|\!)_\theta} \overline{U^m}^\dagger = (\!|U^m s|\!)_{\theta, x=(\!|r|\!)_\theta}$.

- Sea $t = \pi^m s$, en este caso quiero ver que $(\!|(\pi^m s)[x := r]|\!)_\theta = (\!|\pi^m s|\!)_{\theta, x=(\!|r|\!)_\theta}$. Desarrollando el lado izquierdo se tiene:

$$(\!|(\pi^m s)[x := r]|\!)_\theta = (\!|\pi^m (s[x := r])|\!)_\theta = \bigoplus_{i=0}^{2^m - 1} (\overline{\pi_i} (\!|s[x := r]|\!)_\theta \overline{\pi_i}^\dagger)$$

  Por hipótesis inductiva, esto es igual a $\bigoplus_{i=0}^{2^m - 1} (\overline{\pi_i} (\!|s|\!)_{\theta, x=(\!|r|\!)_\theta} \overline{\pi_i}^\dagger) = (\!|\pi^m s|\!)_{\theta, x=(\!|r|\!)_\theta}$.

- Sea $t = s_1 \otimes s_2$, en este caso quiero ver que $(\!|(s_1 \otimes s_2)[x := r]|\!)_\theta = (\!|s_1 s_2|\!)_{\theta, x=(\!|r|\!)_\theta}$. Como el cálculo es afín, hay dos casos: o bien $x \in \mathsf{FV}(s_1)$ y $x \notin \mathsf{FV}(s_2)$, o bien $x \notin \mathsf{FV}(s_1)$ y $x \in \mathsf{FV}(s_2)$.

  - En el primer caso, desarrollando el lado izquierdo se tiene:

$$(\!|(s_1 \otimes s_2)[x := r]|\!)_\theta = (\!|(s_1[x := r]) \otimes s_2|\!)_\theta = (\!|s_1[x := r]|\!)_\theta \otimes (\!|s_2|\!)_\theta$$

    Por hipótesis inductiva esto es igual a $(\!|s_1|\!)_{\theta, x=(\!|r|\!)_\theta} \otimes (\!|s_2|\!)_\theta$. Como $x \notin \mathsf{FV}(s_2)$ vale $(\!|s_2|\!)_\theta = (\!|s_2|\!)_{\theta, x=(\!|r|\!)_\theta}$, entonces:

$$(\!|(s_1 \otimes s_2)[x := r]|\!)_\theta = (\!|s_1|\!)_{\theta, x=(\!|r|\!)_\theta} \otimes (\!|s_2|\!)_{\theta, x=(\!|r|\!)_\theta} = (\!|s_1 \otimes s_2|\!)_{\theta, x=(\!|r|\!)_\theta}$$

  - En el segundo caso, desarrollando el lado izquierdo se tiene:

$$(\!|(s_1 \otimes s_2)[x := r]|\!)_\theta = (\!|s_1 \otimes (s_2[x := r])|\!)_\theta = (\!|s_1|\!)_\theta \otimes (\!|s_2[x := r]|\!)_\theta$$

    Por hipótesis inductiva esto es igual a $(\!|s_1|\!)_\theta \otimes (\!|s_2|\!)_{\theta, x=(\!|r|\!)_\theta}$. Como $x \notin \mathsf{FV}(s_1)$ vale $(\!|s_1|\!)_\theta = (\!|s_1|\!)_{\theta, x=(\!|r|\!)_\theta}$, entonces:

$$(\!|(s_1 \otimes s_2)[x := r]|\!)_\theta = (\!|s_1|\!)_{\theta, x=(\!|r|\!)_\theta} \otimes (\!|s_2|\!)_{\theta, x=(\!|r|\!)_\theta} = (\!|s_1 \otimes s_2|\!)_{\theta, x=(\!|r|\!)_\theta}$$

- Sea $t = \mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$. En este caso quiero ver que $(\!|(\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\})[x := r]|\!)_\theta = (\!|\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}|\!)_{\theta, x=(\!|r|\!)_\theta}$.

  Desarrollando el lado derecho se tiene que:

$$(\!|\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}|\!)_{\theta, x=(\!|r|\!)_\theta} = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho_i)\ (\!|t_i|\!)_{\theta, x=(\!|r|\!)_\theta, y=\frac{\rho_i}{\mathsf{tr}(\rho_i)}} \tag{4.14}$$

  donde

$$(\!|s|\!)_{\theta, x=(\!|r|\!)_\theta} = \bigoplus_{i=0}^{2^m-1} \rho_i \tag{4.15}$$

  Por afinidad o bien $x \in \mathsf{FV}(s)$ y $x \notin \mathsf{FV}(t_i)$ para todo i, o bien $x \notin \mathsf{FV}(s)$ y existe a lo sumo un j tal que $x \in \mathsf{FV}(t_j)$.

  - En el primer caso, desarrollando el lado izquierdo se tiene:

$$(\!|(\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\})[x := r]|\!)_\theta =$$
$$(\!|\mathsf{letcase}^\circ\ y = s[x := r]\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}|\!)_\theta = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho'_i)\ (\!|t_i|\!)_{\theta, y=\frac{\rho'_i}{\mathsf{tr}(\rho'_i)}}$$

    donde $(\!|s[x := r]|\!)_\theta = \bigoplus_{i=0}^{2^m-1} \rho'_i$. Por hipótesis inductiva, se tiene que $(\!|s[x := r]|\!)_\theta = (\!|s|\!)_{\theta, x=(\!|r|\!)_\theta}$. Por (4.15), esto implica que $\rho'_i = \rho_i$ para todo i.
    Por lo tanto, y como $x \notin \mathsf{FV}(t_i)$ para todo i:

$$\sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho'_i)\ (\!|t_i|\!)_{\theta, y=\frac{\rho'_i}{\mathsf{tr}(\rho'_i)}} = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho_i)\ (\!|t_i|\!)_{\theta, y=\frac{\rho_i}{\mathsf{tr}(\rho_i)}}$$
$$= \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho_i)\ (\!|t_i|\!)_{\theta, x=(\!|r|\!)_\theta, y=\frac{\rho_i}{\mathsf{tr}(\rho_i)}}$$

    y se obtiene la igualdad con el lado derecho de (4.14).

  - En el segundo caso se tiene, desarrollando el lado izquierdo:

$$(\!|(\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\})[x := r]|\!)_\theta =$$
$$(\!|\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0[x := r], \ldots, t_{2^m-1}[x := r]\}|\!)_\theta = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho''_i)\ (\!|t_i[x := r]|\!)_{\theta, y=\frac{\rho''_i}{\mathsf{tr}(\rho''_i)}}$$

    donde $(\!|s|\!)_\theta = \bigoplus_{i=0}^{2^m-1} \rho''_i$. Como $x \notin \mathsf{FV}(s)$, vale que $(\!|s|\!)_\theta = (\!|s|\!)_{\theta, x=(\!|r|\!)_\theta}$. Por (4.15) esto implica que $\rho''_i = \rho_i$ para todo i.
    Por lo tanto se tiene que:

$$(\!|(\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\})[x := r]|\!)_\theta = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho_i)\ (\!|t_i[x := r]|\!)_{\theta, y=\frac{\rho_i}{\mathsf{tr}(\rho_i)}}$$

Usando la hipótesis inductiva sobre los t_i:

$$(\!|(\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\})[x := r]|\!)_\theta = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho_i)\,(\!|t_i|\!)_{\theta, x=(\!|r|\!)_\theta, y=\frac{\rho_i}{\mathsf{tr}(\rho_i)}, y=\frac{\rho_i}{\mathsf{tr}(\rho_i)}}$$

Y como $y \notin \mathsf{FV}(r)$, se obtiene la igualdad con el lado derecho de (4.14).

- Sea $t = \sum_i p_i t_i$, quiero ver que $(\!|(\sum_i p_i t_i)[x := r]|\!)_\theta = (\!|\sum_i p_i t_i|\!)_{\theta, x=(\!|r|\!)_\theta}$:

  Desarrollando el lado izquierdo se tiene:

  $$(\!|(\sum_i p_i t_i)[x := r]|\!)_\theta = (\!|\sum_i p_i (t_i[x := r])|\!)_\theta = \sum_i p_i (\!|t_i[x := r]|\!)_\theta$$

  Por hipótesis inductiva, esto es igual a $\sum_i p_i (\!|t_i|\!)_{\theta, x=(\!|r|\!)_\theta} = (\!|\sum_i p_i t_i|\!)_{\theta, x=(\!|r|\!)_\theta}$. □

El siguiente lema demuestra que la interpretación es estable con respecto a la reducción. Usa los lemas de aplicación y de sustitución anteriores, y la linealidad a izquierda de la aplicación.

Lema 4.5.7 (Correctitud de la reducción)**.** *Si* $\Gamma \vdash t : A$, $\theta \vDash \Gamma$ *y* $t \rightsquigarrow r$ *entonces* $(\!|t|\!)_\theta = (\!|r|\!)_\theta$

Demostración. Por inducción en $\rightsquigarrow$.

- $(\lambda x.t)r \rightsquigarrow t[x := r]$

  En este caso quiero ver que $(\!|(\lambda x.t)r|\!)_\theta = (\!|t[x := r]|\!)_\theta$. Por definición se tiene que $(\!|(\lambda x.t)r|\!)_\theta = (\!|\lambda x.t|\!)_\theta \,\#\, (\!|r|\!)_\theta$. Por el lema (4.5.5) esto es igual a $(\!|t|\!)_{\theta, x=(\!|r|\!)_\theta}$. Por el lema (4.5.6) vale $(\!|t|\!)_{\theta, x=(\!|r|\!)_\theta} = (\!|t[x := r]|\!)_\theta$ y se tiene la igualdad.

- $\mathsf{letcase}^\circ\ x = \pi^m \rho\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \rightsquigarrow \sum_{i=0}^{2^m-1} p_i t_i[x := \rho_i]$ donde:

$$p_i = \mathsf{tr}\left(\overline{\pi_i} \rho \overline{\pi_i}^\dagger\right)$$

$$\rho_i = \begin{cases} \frac{\overline{\pi_i} \rho \overline{\pi_i}^\dagger}{p_i} & \text{si } p_i \neq 0 \\ \overline{\pi_i} \rho \overline{\pi_i}^\dagger & \text{si } p_i = 0 \end{cases}$$

  En este caso quiero ver que vale:

  $$(\!|\mathsf{letcase}^\circ\ x = \pi^m \rho\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}|\!)_\theta = (\!|\sum_{i=0}^{2^m-1} p_i t_i[x := \rho_i]|\!)_\theta$$

  Por un lado vale $(\!|\mathsf{letcase}^\circ\ x = \pi^m \rho\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}|\!)_\theta = \sum_{i=0}^{2^m-1} p_i (\!|t_i|\!)_{\theta, x=\rho_i}$ usando las definiciones de más arriba para p_i y ρ_i, porque $(\!|\pi^m \rho|\!)_\theta = \bigoplus_{i=0}^{2^m-1} \overline{\pi_i} \rho \overline{\pi_i}^\dagger$.

  Por otro lado se tiene que vale $(\!|\sum_{i=1}^{2^m} p_i t_i[x := \rho_i]|\!)_\theta = \sum_{i=1}^{2^m} p_i (\!|t_i[x := \rho_i]|\!)_\theta$ por definición. Usando el lema de sustitución esto es igual a $\sum_{i=1}^{2^m} p_i (\!|t_i|\!)_{\theta, x=(\!|\rho_i|\!)_\theta}$. Como $(\!|\rho_i|\!)_\theta = \rho_i$ para toda θ, esto resulta igual a $\sum_{i=1}^{2^m} p_i (\!|t_i|\!)_{\theta, x=\rho_i}$ y se tiene la igualdad.

- $\mu_0 x.t \rightsquigarrow \bot_A$

  En este caso quiero ver que $(\!|\mu_0 x.t|\!)_\theta = (\!|\bot_A|\!)_\theta$. Por definición se tiene que $(\!|\mu_0 x.t|\!)_\theta = (\!|\lambda x.t|\!)_\theta \,\#_0\, \mathbb{0}_{\dim(A)}$. Esto es igual a $\mathbb{0}_{\dim(A)}$, que a su vez es igual a $(\!|\bot_A|\!)_\theta$.

- $\mu_{n+1} x.t \rightsquigarrow t[x := \mu_n x.t]$

  En este caso quiero ver que $(\!|\mu_{n+1} x.t|\!)_\theta = (\!|t[x := \mu_n x.t]|\!)_\theta$. Por definición se tiene que $(\!|\mu_{n+1} x.t|\!)_\theta = (\!|\lambda x.t|\!)_\theta \,\#_{n+1}\, \mathbb{0}_{\dim(A)}$. Descomponiendo las aplicaciones, esto resulta igual a

  $$(\!|\lambda x.t|\!)_\theta \,\#\, ((\!|\lambda x.t|\!)_\theta \,\#_n\, \mathbb{0}_{\dim(A)})$$

  Por hipótesis inductiva, esto es lo mismo que $(\!|\lambda x.t|\!)_\theta \,\#\, (\!|\mu_n x.t|\!)_\theta$. Como $\Gamma \vdash \mu_{n+1} x.t : A$ entonces por inversión $\Gamma, x : A \vdash t : A$, y por la regla μ se tiene $\Gamma \vdash \mu_n x.t : A$. Como $\theta \vDash \Gamma$ también se tiene $\theta \vDash_{\dim} \Gamma$ y usando el lema (4.5.3) resulta $\dim((\!|\mu_n x.t|\!)_\theta) = \dim(A)$. Usando el lema (4.5.5), se tiene $(\!|\lambda x.t|\!)_\theta \,\#\, (\!|\mu_n x.t|\!)_\theta = (\!|t|\!)_{\theta, x=(\!|\mu_n x.t|\!)_\theta}$. Usando el lema (4.5.6) se obtiene $(\!|t[x := \mu_n x.t]|\!)_\theta$.

- $\bot_n \rightsquigarrow \mathbb{0}_{2^n}$

  Por definición se tiene que $(\!|\bot_n|\!)_\theta = \mathbb{0}_{\dim(n)} = \mathbb{0}_{2^n}$.

- $\bot_{(m,n)} \rightsquigarrow \pi^m \mathbb{0}_{2^n}$

  Por un lado se tiene que $(\!|\bot_{(m,n)}|\!)_\theta = \mathbb{0}_{\dim((m,n))} = \mathbb{0}_{2^{n+m}}$. Por el otro se tiene $(\!|\pi^m \mathbb{0}_{2^n}|\!)_\theta = \bigoplus_{i=0}^{2^m-1} \mathbb{0}_{2^n}$, que es equivalente a $\mathbb{0}_{2^{n+m}}$ cuando represento $\oplus$ mediante la inclusión de las matrices en la diagonal.

- $\bot_{A \multimap B}\ t \rightsquigarrow \bot_B$

  Desarrollando $(\!|\bot_{A \multimap B}\ t|\!)_\theta$ se tiene:

  $$(\!|\bot_{A \multimap B}\ t|\!)_\theta = (\!|\bot_{A \multimap B}|\!)_\theta \,\#\, (\!|t|\!)_\theta = \mathbb{0}_{\dim(A \multimap B)} \,\#\, (\!|t|\!)_\theta = \mathbb{0}_{\dim(B)} = (\!|\bot_B|\!)_\theta$$

- $pt + q\bot_A \rightsquigarrow pt$

  Desarrollando, se tiene $(\!|pt + q\bot_A|\!)_\theta = p(\!|t|\!)_\theta + q(\!|\bot_A|\!)_\theta = p(\!|t|\!)_\theta + q\mathbb{0}_{\dim(A)} = p(\!|t|\!)_\theta = (\!|pt|\!)_\theta$.

- $U^m \rho^n \rightsquigarrow \rho'^n$ con $\rho'^n = \overline{U^m} \rho^n \overline{U^m}^\dagger$

  En este caso quiero ver que vale $(\!|U^m \rho^n|\!)_\theta = (\!|\rho'^n|\!)_\theta$.

  Por definición se tiene que $(\!|U^m \rho^n|\!)_\theta = \overline{U^m} (\!|\rho^n|\!)_\theta \overline{U^m}^\dagger = \overline{U^m} \rho^n \overline{U^m}^\dagger$. Esto es igual a la definición de ρ'^n. Vale $\rho'^n = (\!|\rho'^n|\!)_\theta$ y se obtiene la igualdad.

- $\rho \otimes \rho' \rightsquigarrow \rho''$ con $\rho'' = \rho \otimes \rho'$

  En este caso quiero ver que vale $(\!|\rho \otimes \rho'|\!)_\theta = (\!|\rho''|\!)_\theta$.

  Por definición vale que $(\!|\rho \otimes \rho'|\!)_\theta = (\!|\rho|\!)_\theta \otimes (\!|\rho'|\!)_\theta = \rho \otimes \rho'$. Esto es igual a la definición de ρ''. Vale $\rho'' = (\!|\rho''|\!)_\theta$ y se tiene la igualdad.

- $\sum_i p_i \rho_i^n \rightsquigarrow \rho'^n$ con $\rho'^n = \sum_i p_i \rho_i^n$

  En este caso quiero ver que vale $(\!|\sum_i p_i \rho_i^n|\!)_\theta = (\!|\rho'^n|\!)_\theta$.

  Por definición se tiene que $(\!|\sum_i p_i \rho_i^n|\!)_\theta = \sum_i p_i (\!|\rho_i^n|\!)_\theta = \sum_i p_i \rho_i^n$. Esto es igual a la definición de ρ'^n. Vale $\rho'^n = (\!|\rho'^n|\!)_\theta$ y se tiene la igualdad.

- $\sum_i (p_i t) \rightsquigarrow (\sum_i p_i) t$

  En este caso quiero ver que $(\!|\sum_i (p_i t)|\!)_\theta = (\!|(\sum_i p_i) t|\!)_\theta$. Ambos son iguales a $\sum_i p_i (\!|t|\!)_\theta$, considerando $\sum_i p_i$ como el único número de la sumatoria en el segundo término.

- $(\sum_i p_i t_i) r \rightsquigarrow \sum_i p_i (t_i r)$

  En este caso quiero ver que $(\!|(\sum_i p_i t_i) r|\!)_\theta = (\!|\sum_i p_i (t_i r)|\!)_\theta$. Desarrollando desde $(\!|(\sum_i p_i t_i) r|\!)_\theta$, y usando el lema (4.3.4):

$$(\!|(\sum_i p_i t_i) r|\!)_\theta = (\!|\sum_i p_i t_i|\!)_\theta \# (\!|r|\!)_\theta = (\sum_i p_i (\!|t_i|\!)_\theta) \# (\!|r|\!)_\theta$$
$$\overset{(4,3,4)}{=} \sum_i p_i \, ((\!|t_i|\!)_\theta \# (\!|r|\!)_\theta) = \sum_i p_i (\!|t_i r|\!)_\theta = (\!|\sum_i p_i (t_i r)|\!)_\theta$$

Casos contextuales:

- $t \rightsquigarrow r \implies ts \rightsquigarrow rs$

  En este caso quiero ver que $(\!|ts|\!)_\theta = (\!|rs|\!)_\theta$ cuando $t \rightsquigarrow r$.

  Por definición se tiene que $(\!|ts|\!)_\theta = (\!|t|\!)_\theta \# (\!|s|\!)_\theta$. Por hipótesis inductiva, como $t \rightsquigarrow r$ vale $(\!|t|\!)_\theta = (\!|r|\!)_\theta$ y por lo tanto $(\!|t|\!)_\theta \# (\!|s|\!)_\theta = (\!|r|\!)_\theta \# (\!|s|\!)_\theta$ que por definición es igual a $(\!|rs|\!)_\theta$ y se tiene la igualdad.

- $t \rightsquigarrow r \implies st \rightsquigarrow sr$

  En este caso quiero ver que $(\!|st|\!)_\theta = (\!|sr|\!)_\theta$ cuando $t \rightsquigarrow r$.

  Por definición se tiene que $(\!|st|\!)_\theta = (\!|s|\!)_\theta \# (\!|t|\!)_\theta$. Por hipótesis inductiva, como $t \rightsquigarrow r$ vale $(\!|t|\!)_\theta = (\!|r|\!)_\theta$ y por lo tanto $(\!|s|\!)_\theta \# (\!|t|\!)_\theta = (\!|s|\!)_\theta \# (\!|r|\!)_\theta$ que por definición es igual a $(\!|sr|\!)_\theta$.

- $t \rightsquigarrow r \implies U^m t \rightsquigarrow U^m r$

  En este caso quiero ver que $(\!|U^m t|\!)_\theta = (\!|U^m r|\!)_\theta$ cuando $t \rightsquigarrow r$.

  Por definición se tiene que $(\!|U^m t|\!)_\theta = \overline{U^m} (\!|t|\!)_\theta \overline{U^m}^\dagger$. Por hipótesis inductiva, como $t \rightsquigarrow r$ vale $(\!|t|\!)_\theta = (\!|r|\!)_\theta$. Reemplazando se obtiene $\overline{U^m} (\!|r|\!)_\theta \overline{U^m}^\dagger$, y esto resulta igual a $(\!|U^m r|\!)_\theta$ por definición.

- $t \rightsquigarrow r \implies \pi^m t \rightsquigarrow \pi^m r$

  En este caso quiero ver que $(\!|\pi^m t|\!)_\theta = (\!|\pi^m r|\!)_\theta$ cuando $t \rightsquigarrow r$.

  Por definición vale $(\!|\pi^m t|\!)_\theta = \bigoplus_{i=0}^{2^m-1} (\overline{\pi_i} (\!|t|\!)_\theta \overline{\pi_i}^\dagger)$. Usando la hipótesis inductiva según la cual $(\!|t|\!)_\theta = (\!|r|\!)_\theta$, esto resulta igual a $\bigoplus_{i=0}^{2^m-1} (\overline{\pi_i} (\!|r|\!)_\theta \overline{\pi_i}^\dagger)$. Por definición esto es igual a $(\!|\pi^n r|\!)_\theta$ y se obtiene la igualdad buscada.

- $t \rightsquigarrow r \implies t \otimes s \rightsquigarrow r \otimes s$

  En este caso quiero ver que vale $(\!|t \otimes s|\!)_\theta = (\!|r \otimes s|\!)_\theta$ cuando $t \rightsquigarrow r$.

  Por definición vale que $(\!|t \otimes s|\!)_\theta = (\!|t|\!)_\theta \otimes (\!|s|\!)_\theta$. Esto es igual a $(\!|r|\!)_\theta \otimes (\!|s|\!)_\theta$ por hipótesis inductiva, y nuevamente por definición se tiene la igualdad con $(\!|r \otimes s|\!)_\theta$.

- $t \rightsquigarrow r \implies s \otimes t \rightsquigarrow s \otimes r$

  En este caso quiero ver que vale $(\!|s \otimes t|\!)_\theta = (\!|s \otimes r|\!)_\theta$ cuando $t \rightsquigarrow r$.

  Por definición vale que $(\!|s \otimes t|\!)_\theta = (\!|s|\!)_\theta \otimes (\!|t|\!)_\theta$. Esto es igual a $(\!|s|\!)_\theta \otimes (\!|r|\!)_\theta$ por hipótesis inductiva, y nuevamente por definición se tiene la igualdad con $(\!|s \otimes r|\!)_\theta$.

- $t_j \rightsquigarrow r_j$ para algún j en $\{1, \ldots, n\} \implies$
  $$\sum_{i=1}^{n} p_i t_i \rightsquigarrow \sum_{i=1}^{n} p_i r_i \text{ con } t_i = r_i \text{ para todo } i \neq j \text{ en } \{1, \ldots, n\}$$

  En este caso quiero ver que vale $(\!|\sum_{i=1}^n p_i t_i|\!)_\theta = (\!|\sum_{i=1}^n p_i r_i|\!)_\theta$ con $t_i = r_i$ para todo $i \neq j$ en $\{1, \ldots, n\}$ cuando $t_j \rightsquigarrow r_j$ para un j en $\{1, \ldots, n\}$.

  Por definición se tiene que $(\!|\sum_{i=1}^n p_i t_i|\!)_\theta = \sum_{i=1}^n p_i (\!|t_i|\!)_\theta$. Separando el término con j de la sumatoria esto es lo mismo que $\sum_{\substack{i=1 \\ i \neq j}}^n p_i (\!|t_i|\!)_\theta + p_j (\!|t_j|\!)_\theta$. Como $t_j \rightsquigarrow r_j$, por hipótesis inductiva vale que $(\!|t_j|\!)_\theta = (\!|r_j|\!)_\theta$. Al definir $r_i = t_i$ para todo $i \neq j$, la sumatoria queda igual a $\sum_{\substack{i=1 \\ i \neq j}}^n p_i (\!|r_i|\!)_\theta + p_j (\!|r_j|\!)_\theta = \sum_{i=1}^n p_i (\!|r_i|\!)_\theta$ que por definición es igual a $(\!|\sum_{i=1}^n p_i r_i|\!)_\theta$.

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

  Quiero ver que $(\!|\mathsf{letcase}^\circ\ x = t\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}|\!)_\theta = (\!|\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}|\!)_\theta$ cuando $t \rightsquigarrow r$.

  Por definición se tiene que $(\!|\mathsf{letcase}^\circ\ x = t\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}|\!)_\theta = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho_i)\,(\!|s_i|\!)_{\theta, x=\frac{\rho_i}{\mathsf{tr}(\rho_i)}}$ con $(\!|t|\!)_\theta = \bigoplus_{i=0}^{2^m-1} \rho_i$; y $(\!|\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}|\!)_\theta = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\sigma_i)\,(\!|s_i|\!)_{\theta, x=\frac{\sigma_i}{\mathsf{tr}(\sigma_i)}}$ con $(\!|r|\!)_\theta = \bigoplus_{i=0}^{2^m-1} \sigma_i$.

  Como por hipótesis inductiva se tiene que $(\!|t|\!)_\theta = (\!|r|\!)_\theta$, entonces se tiene que $\rho_i = \sigma_i$ para todo i, y se tiene que $\sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho_i)\,(\!|s_i|\!)_{\theta, x=\frac{\rho_i}{\mathsf{tr}(\rho_i)}} = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\sigma_i)\,(\!|s_i|\!)_{\theta, x=\frac{\sigma_i}{\mathsf{tr}(\sigma_i)}}$ que es la igualdad buscada. □

4.6. Adecuación

El teorema de adecuación (4.6.16) dice que para todos los términos bien tipados del cálculo su interpretación se encuentra dentro de la interpretación de su tipo.

La parte más complicada de su demostración está en los términos de tipo flecha. La estructura de la demostración es la siguiente: primero se demuestra adecuación en el caso de los términos de la forma $\lambda x.t$. Luego se demuestra un lema de progreso (4.6.10), por el que todos los términos de tipo flecha reducen a alguno que tiene esta forma. Usando la correctitud de la reducción (4.5.7), se obtiene adecuación para todos los términos de tipo flecha.

Para la demostración de la adecuación de las funciones explícitas fue necesario agregar la conjetura (4.6.1). Además se agregó la conjetura (4.6.15) para la demostración de los casos de aplicación y punto fijo en el teorema de adecuación (4.6.16). La demostración de ambas conjeturas se deja para trabajo futuro.

4.6.1. Adecuación para funciones explícitas

La siguiente conjetura dice que la parte lineal de la interpretación de las funciones, visto en el lema (4.5.1), es completamente positiva. Esto significa que la aplicación de estas funciones sobre matrices positivas devuelve matrices positivas, es decir que no salen fuera del dominio. Es necesaria para ver que la matriz característica de la parte lineal de las interpretaciones de funciones es una matriz positiva, en el lema (4.6.4).

Conjetura 4.6.1. *Sea t un término tal que $\Gamma \vdash t : A \multimap B$, con $\theta \vDash \Gamma$ y sea $n = \dim(A)$, entonces la siguiente función es completamente positiva:*

$$a \mapsto (\!|t|\!)_{\theta,x=a} - (\!|t|\!)_{\theta,x=\mathbb{0}_n}$$

El siguiente lema es auxiliar a la demostración de lema (4.6.4).

Lema 4.6.2. *Sean $M \in \mathcal{P}_m, N \in \mathcal{P}_n$. Entonces $M \oplus N \in \mathcal{P}_{n+m}$.*

Demostración.

- $M \oplus N$ es hermítica porque M y N lo son.

$$(M \oplus N)^\dagger = M^\dagger \oplus N^\dagger = M \oplus N$$

- $M \oplus N$ es semidefinida positiva porque M y N lo son. Sea $u = (v, w)$, con $v \in \mathbb{C}^m$ y $w \in \mathbb{C}^n$.

$$u^\dagger (M \oplus N) u = (v,w)^\dagger (M \oplus N)(v,w) = (v^\dagger M v) + (w^\dagger N w) \geq 0$$ □

El siguiente teorema se utiliza en la demostración de adecuación.

Teorema 4.6.3. [Sel04, Teorema 6.5] *Sea $F : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$ un operador lineal, y sea $\chi_F \in \mathbb{C}^{nm\times nm}$ su matriz característica.*

(a) F es de la forma $F(A) = UAU^\dagger$, para algún $U \in \mathbb{C}^{m\times n}$, si y sólo si χ_F es pura.

(b) Las siguiente proposiciones son equivalentes:

(i) F es completamente positiva.

(ii) χ_F es positiva.

(iii) F es de la forma $F(A) = \sum_i U_i A U_i^\dagger$, para alguna secuencia finita de matrices $U_1, \ldots, U_k \in \mathbb{C}^{m\times n}$. □

Finalmente se demuestra adecuación para funciones explícitas.

Lema 4.6.4 (Adecuación para funciones explícitas)**.** *Sean A y B dos tipos. Sea t un término tal que $\Gamma, x : A \vdash t : B$, y θ una valuación tal que $\theta \vDash \Gamma$. Además, asumo que tanto $(\!|t|\!)_{\theta,x=a}$ como $(\!|t|\!)_{\theta,x=\perp}$ están en $(\!|B|\!)$. Entonces $\chi_{[a\mapsto(\!|t|\!)_{\theta,x=a}]} \in (\!|A \multimap B|\!)$.*

Demostración. Por el lema (4.5.1) se tiene que dado un término t, la función $a \mapsto (\!|t|\!)_{\theta,x=a} - (\!|t|\!)_{\theta,x=\perp}$ es lineal. Además, es completamente positiva por la conjetura (4.6.1), por lo tanto su matriz característica es positiva por el teorema (4.6.3).

Su matriz característica está dada por:

$$M_t = \begin{pmatrix} (\!|t|\!)_{\theta,x=E_{11}} - (\!|t|\!)_{\theta,x=\perp} & \cdots & (\!|t|\!)_{\theta,x=E_{1n}} - (\!|t|\!)_{\theta,x=\perp} \\ \vdots & \ddots & \vdots \\ (\!|t|\!)_{\theta,x=E_{n1}} - (\!|t|\!)_{\theta,x=\perp} & \cdots & (\!|t|\!)_{\theta,x=E_{nn}} - (\!|t|\!)_{\theta,x=\perp} \end{pmatrix}$$

De acuerdo a la definición en (4.2), se tiene que

$$\chi_{[a\mapsto(\!|t|\!)_{\theta,x=a}]} = M_t \oplus (\!|t|\!)_{\theta,x=\perp}$$

Como $M_t \in (\!|A|\!) \otimes (\!|B|\!)$, se tiene que $\chi_{[a\mapsto(\!|t|\!)_{\theta,x=a}]} \in ((\!|A|\!) \otimes (\!|B|\!)) \oplus (\!|B|\!)$. Por otra parte, como $(\!|t|\!)_{\theta,x=\perp}$ pertenece a $(\!|B|\!)$, es una matriz positiva. Entonces por el lema (4.6.2) $\chi_{[a\mapsto(\!|t|\!)_{\theta,x=a}]}$ es una matriz positiva, y como está en $((\!|A|\!) \otimes (\!|B|\!)) \oplus (\!|B|\!)$, pertenece a $(\!|A \multimap B|\!)$. □

4.6.2. Adecuación para funciones implícitas

Llamo funciones implícitas a los términos t del lenguaje tales que $(\!|t|\!)_\theta \in (\!|A \multimap B|\!)$ para ciertos tipos A y B y valuación θ, pero tales que t no es de la forma $\sum_{i=1}^{n} \lambda x.s_i$.

Por el lema (4.6.4) ya sé que las funciones explícitas cumplen adecuación. Para demostrarlo en el caso de las funciones implícitas se definen valores y se demuestra un lema de progreso para términos abiertos (4.6.10). Se definen las funciones de cierre, que son sustituciones que cierran los términos para poder reducirlos de acuerdo a la valuación respecto a la cual se los busca interpretar. Al cerrar los términos de forma coherente con su contexto de tipado, se los puede reducir y llegar a alguno de los valores posibles para los términos de tipo flecha. Estos son o bien la función nula o bien una combinación lineal de términos de la forma $\lambda x.t$, que por el lema (4.6.4) cumplen con adecuación.

Finalmente usando estos resultados se demuestra el lema (4.6.13).

Definición 4.6.5 (Valores)**.** Llamo Val al conjunto de valores del cálculo, definido por los siguientes términos cerrados:

$$\mathsf{Val} := \rho^n \mid \pi^m \rho^n \mid \sum_{i=1}^{n} p_i(\lambda x.t_i)$$

donde $0 < p_i \leq 1$ y t_i es un término cualquiera para todo $i \in \{1, \ldots, n\}$, y vale $\sum_{i=1}^{n} p_i \leq 1$.

El caso particular de los términos de la forma $\lambda x.t$ está contemplado dentro de la sumatoria, con $n = 1$ y $p_1 = 1$. Además, las funciones que forman parte de los valores pueden reducir a otras funciones que también sean valores.

Definición 4.6.6 (Función de cierre)**.** Sea $\tau : \mathsf{Var} \to \mathsf{Val} \cup \{\perp_A\}$, denoto $\tau(t)$ a la sustitución que reemplaza las variables libres en t por valores de acuerdo al mapeo dado por τ. Llamo a τ función de cierre.

Las funciones de cierre van a usarse sobre términos tipados, por lo que tienen que ser coherentes con los contextos de tipado, es decir asignar valores con el mismo tipo que la variable que se está reemplazando.

Definición 4.6.7. Sea τ una función de cierre, sea Γ un contexto de tipado. τ satisface Γ (notado como $\tau \vDash \Gamma$) si y sólo si para todo $x : A$ en Γ vale $\vdash \tau(x) : A$.

A continuación se demuestra que las funciones de cierre que satisfacen el contexto de tipado de un término, al ser aplicadas devuelven términos cerrados del mismo tipo. Para demostrar esto primero se prueba un lema donde la satisfacción es parcial, y luego en el corolario (4.6.9) se muestra el caso particular en que se satisface todo el contexto. Se decidió hacer la demostración de esta manera a causa del caso de las abstracciones en la inducción.

Lema 4.6.8. *Sea t un término tal que $\Gamma, \Delta \vdash t : A$. Sea τ una función de cierre tal que $\tau \vDash \Gamma$. Entonces $\Delta \vdash \tau(t) : A$.*

Demostración. Por inducción en t.

- Sea $t = x$. En este caso se tiene $\Gamma, \Delta \vdash x : A$.
  - Si $x : A \in \Gamma$ entonces como $\tau \vDash \Gamma$ se tiene que $\vdash \tau(x) : A$, por lo tanto $\Delta \vdash \tau(x) : A$.
  - Si $x : A \in \Delta$, τ no sustituye a x por lo tanto $\tau(x) = x$ y $x : A \vdash x : A$, es decir $\Delta \vdash \tau(x) : A$.
- Sea $t = \lambda x.u$. Entonces se tiene $\Gamma, \Delta \vdash \lambda x.u : B \multimap C$, y vale $\Gamma, \Delta, x : B \vdash u : C$. Por hipótesis inductiva se tiene entonces que $\Delta, x : B \vdash \tau(u) : C$, y por lo tanto $\Delta \vdash \lambda x.\tau(u) : C$.
- Sea $t = uv$. Se tiene que $\Gamma, \Delta \vdash uv : A$. Sean $\Gamma = \Gamma_1, \Gamma_2$ y $\Delta = \Delta_1, \Delta_2$ tales que $\Gamma_1, \Delta_1 \vdash u : B \multimap A$ y $\Gamma_2, \Delta_2 \vdash v : B$. Como $\tau \vDash \Gamma$ se tienen $\tau \vDash \Gamma_1$ y $\tau \vDash \Gamma_2$. Por hipótesis inductiva vale que $\Delta_1 \vdash \tau(u) : B \multimap A$ y $\Delta_2 \vdash \tau(v) : B$, y por lo tanto $\Delta \vdash \tau(u)\tau(v) : A$.
- Sea $t = \mu_n x.u$. Se tiene $\Gamma, \Delta \vdash \mu_n x.u : A$, por lo tanto vale $\Gamma, \Delta, x : A \vdash u : A$. Por hipótesis inductiva se tiene que $\Delta, x : A \vdash \tau(u) : A$, y por lo tanto $\Delta \vdash \mu_n x.\tau(u) : A$.
- Sea $t = \bot_A$. En este caso no hay variables libres.
- Sea $t = \rho^n$. En este caso no hay variables libres.
- Sea $t = U^m v$. Se tiene $\Gamma, \Delta \vdash U^m v : n$, por lo tanto $\Gamma, \Delta \vdash v : n$. Por hipótesis inductiva vale que $\Delta \vdash \tau(v) : n$ y entonces se tiene $\Delta \vdash U^m \tau(v) : n$.
- Sea $t = \pi^m u$. Se tiene $\Gamma, \Delta \vdash \pi^m u : (m, n)$. Por lo tanto $\Gamma, \Delta \vdash u : n$. Por hipótesis inductiva se tiene que $\Delta \vdash \tau(u) : n$, y por lo tanto $\Delta \vdash \pi^m \tau(u) : (m, n)$.
- Sea $t = u \otimes v$. En este caso se tiene $\Gamma, \Delta \vdash u \otimes v : n + m$. Sean $\Gamma = \Gamma_1, \Gamma_2$ y $\Delta = \Delta_1, \Delta_2$ tales que $\Gamma_1, \Delta_1 \vdash u : n$ y $\Gamma_2, \Delta_2 \vdash v : m$. Como $\tau \vDash \Gamma$ se tienen $\tau \vDash \Gamma_1$ y $\tau \vDash \Gamma_2$. Por hipótesis inductiva vale que $\Delta_1 \vdash \tau(u) : n$ y $\Delta_2 \vdash \tau(v) : m$. Por lo tanto $\Delta \vdash \tau(u) \otimes \tau(v) : n + m$.
- Sea $t = \sum_{i=1}^{n} p_i t_i$. Se tiene $\Gamma, \Delta \vdash \sum_{i=1}^{n} p_i t_i : A$. Por lo tanto, vale que $\Gamma, \Delta \vdash t_i : A$ para todo i en $\{1, \ldots, n\}$. Por hipótesis inductiva se tiene que $\Delta \vdash \tau(t_i) : A$ para todo i, por lo tanto $\Delta \vdash \sum_{i=1}^{n} p_i \tau(t_i) : A$.
- Sea $t = \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$. En este caso se tiene $\Gamma, \Delta \vdash \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} : A$. Sean $\Gamma = \Gamma_1, \Gamma_2$ y $\Delta = \Delta_1, \Delta_2$ tales que $\Gamma_1, \Delta_1, x : n \vdash t_i : A$ para todo i en $\{0, \ldots, 2^m - 1\}$ y $\Gamma_2, \Delta_2 \vdash r : (m, n)$. Como $\tau \vDash \Gamma$ se tienen $\tau \vDash \Gamma_1$ y $\tau \vDash \Gamma_2$. Por hipótesis inductiva se tiene que $\Delta_1, x : n \vdash \tau(t_i) : A$ para todo i y $\Delta_2 \vdash \tau(r) : (m, n)$. Por lo tanto $\Delta \vdash \mathsf{letcase}^\circ\ x = \tau(r)\ \mathsf{in}\ \{\tau(t_0), \ldots, \tau(t_{2^m-1})\} : A$. □

El siguiente corolario es el caso particular del lema cuando Δ es vacío.

Corolario 4.6.9 (Sustitución)**.** *Sea t un término tal que $\Gamma \vdash t : A$. Sea τ una función de cierre tal que $\tau \vDash \Gamma$. Entonces $\vdash \tau(t) : A$.* □

A continuación se demuestra el lema de progreso para términos abiertos, cerrándolos mediante funciones de cierre.

Lema 4.6.10 (Progreso)**.** *Sea t un término tal que $\Gamma \vdash t : A$. Sea τ una función de cierre tal que $\tau \vDash \Gamma$. Entonces $\tau(t)$ o bien está en $\mathsf{Val} \cup \{\bot_A\}$ o bien reduce.*

Demostración. Por inducción en t.

- Sea $t = x$. En este caso se tiene $\Gamma = \{x : A\} \vdash x : A$. Como $\tau \vDash \Gamma$, entonces $\tau(t) = \tau(x) \in \mathsf{Val} \cup \{\bot_A\}$.
- Sea $t = \lambda x.u$. Vale $\tau(t) = \lambda x.\tau(u)$, donde τ no reemplaza las apariciones libres de x en u. Entonces $\tau(t) \in \mathsf{Val}$ ya que es un caso particular de la sumatoria.
- Sea $t = uv$, vale $\tau(t) = \tau(u)\tau(v)$. Se tiene que $\Gamma \vdash uv : A$. Sean $\Gamma = \Gamma_1, \Gamma_2$ tales que $\Gamma_1 \vdash u : B \multimap A$ y $\Gamma_2 \vdash v : B$. Como $\tau \vDash \Gamma$ se tienen $\tau \vDash \Gamma_1$ y $\tau \vdash \Gamma_2$. Por hipótesis inductiva vale que tanto $\tau(u)$ como $\tau(v)$ o bien están en $\mathsf{Val} \cup \{\bot_A\}$, o bien reducen.
  - Por el lema (4.6.8) se tiene que $\vdash \tau(u) : B \multimap A$. Entonces, si $\tau(u)$ está en $\mathsf{Val} \cup \{\bot_A\}$, por su tipo o bien $\tau(u) = \sum_{i=1}^{n} p_i(\lambda x.t_i)$ para x una variable y términos t_i (con $0 < p_i \leq 1$ y $\sum_{i=1}^{n} p_i \leq 1$), o bien $\tau(t) = \bot_{A \multimap B}$.
    En el primer caso, si $n = 1$ y $p_1 = 1$:
    $$\tau(t) = (\lambda x.t_1)\ \tau(v) \rightsquigarrow t_1[x := \tau(v)]$$
    Para las demás distribuciones posibles de p_i:
    $$\tau(t) = \left(\sum_{i=1}^{n} p_i(\lambda x.t_i)\right) \tau(v) \rightsquigarrow \sum_{i=1}^{n} p_i\,((\lambda x.t_i)\ \tau(v))$$
    En el segundo caso:
    $$\tau(t) = \bot_{A \multimap B}\ \tau(v) \rightsquigarrow \bot_B$$
  - Si $\tau(u) \rightsquigarrow r$ entonces $\tau(t) \rightsquigarrow r\ \tau(v)$.
- Sea $t = \mu_n x.u$. En este caso $\tau(t) = \mu_n x.\tau(u)$, donde τ no reemplaza las apariciones libres de x en u. Por inducción en n:
  - Si $n = 0$ se tiene $\tau(t) \rightsquigarrow \bot_A$.
  - Si $n > 0$, entonces $\tau(t) \rightsquigarrow \tau(u)[x := \mu_{(n-1)} x.\tau(u)]$.
- Sea $t = \bot_A$. En este caso $\tau(\bot_A) = \bot_A$.
- Sea $t = \rho^n$. En este caso $\tau(\rho^n) = \rho^n \in \mathsf{Val}$.
- Sea $t = U^m u$. En este caso $\tau(t) = U^m \tau(u)$. Por hipótesis, se tiene $\Gamma \vdash U^m u : n$. Por lo tanto $\Gamma \vdash u : n$, entonces por hipótesis inductiva $\tau(u)$ o bien está en $\mathsf{Val} \cup \{\bot_A\}$, o bien reduce.
  - Por el lema (4.6.8) se tiene que $\vdash \tau(u) : n$. Si $\tau(u)$ está en $\mathsf{Val} \cup \{\bot_A\}$, por su tipo vale $\tau(u) = \rho^n$ y se tiene $\tau(t) = U^m \rho^n \rightsquigarrow \overline{U^m} \rho^n \overline{U^\dagger}$.

  - Si $\tau(u) \rightsquigarrow r$, entonces $\tau(t) \rightsquigarrow U^m r$.

- Sea $t = \pi^m u$. En este caso $\tau(t) = \pi^m \tau(u)$. Por hipótesis se tiene que $\Gamma \vdash \pi^m u : (m, n)$, por lo tanto $\Gamma \vdash u : n$. Por hipótesis inductiva entonces $\tau(u)$ o bien está en $\mathsf{Val} \cup \{\bot_A\}$, o bien reduce.

  - Por el lema (4.6.8), vale que $\vdash \tau(u) : n$. Si $\tau(u)$ está en $\mathsf{Val} \cup \{\bot_A\}$ se tiene que $\tau(u) = \rho^n$. Por lo tanto $\tau(t) = \pi^m \rho^n$ es un valor.
  - Si $\tau(u) \rightsquigarrow r$, se tiene que $\tau(t) \rightsquigarrow \pi^m r$.

- Sea $t = u \otimes v$. En este caso $\tau(t) = \tau(u) \otimes \tau(v)$. Por hipótesis se tiene que $\Gamma \vdash u \otimes v : n + m$. Sean $\Gamma = \Gamma_1, \Gamma_2$ tales que $\Gamma_1 \vdash u : n$ y $\Gamma_2 \vdash v : m$. Como $\tau \vDash \Gamma$, se tiene que $\tau \vDash \Gamma_1$ y $\tau \vDash \Gamma_2$. Por hipótesis inductiva, tanto $\tau(u)$ como $\tau(v)$ o bien están en $\mathsf{Val} \cup \{\bot_A\}$, o bien reducen.

  - Por el lema (4.6.8) se tiene que $\vdash \tau(u) : n$ y $\vdash \tau(v) : m$. Si tanto $\tau(u)$ como $\tau(v)$ están en $\mathsf{Val} \cup \{\bot_A\}$, entonces $\tau(u) = \rho^n$ y $\tau(v) = \rho^m$. Por lo tanto $\tau(t) = \rho^n \otimes \rho^m \rightsquigarrow \rho^{n+m}$, con $\rho^{n+m} = \rho^n \otimes \rho^m$.
  - Si $\tau(u) \rightsquigarrow u'$, se tiene $\tau(t) \rightsquigarrow u' \otimes \tau(v)$.
  - Si $\tau(v) \rightsquigarrow v'$, se tiene $\tau(t) \rightsquigarrow \tau(u) \otimes v'$.

- Sea $t = \sum_{i=1}^n p_i t_i$. En este caso se tiene $\tau(t) = \sum_{i=1}^n p_i \tau(t_i)$. Por hipótesis vale que $\Gamma \vdash \sum_{i=1}^n p_i t_i : A$, por lo tanto $\Gamma \vdash t_i : A$ para todo i en $\{1, \ldots, n\}$. Entonces por hipótesis inductiva vale que $\tau(t_i)$ o bien está en $\mathsf{Val} \cup \{\bot_A\}$, o bien reduce. Además por el lema (4.6.8) se tiene que $\vdash \tau(t_i) : A$ para todo i.

  - Si $\tau(t_i)$ está en $\mathsf{Val} \cup \{\bot_A\}$ para todo i y $A = m$, por su tipo vale que $\tau(t_i) = \rho_i^m$ para todo i. Si $n = 1$ y $p_1 = 1$ se tiene $\tau(t) = \rho^m \in \mathsf{Val}$. En otro caso se tiene $\tau(t) = \sum_{i=1}^n p_i \rho_i^m \rightsquigarrow \rho^m$, con $\rho^m = \sum_{i=1}^n p_i \rho_i^m$.
  - Si $\tau(t_i)$ está en $\mathsf{Val} \cup \{\bot_A\}$ para todo i y $A = B \multimap C$, $n > 1$ y existe $j \in \{1, \ldots, n\}$ tal que $\tau(t_j) = \bot_{B \multimap C}$, entonces $\tau(t) = \sum_{i=1}^n p_i \tau(t_i) \rightsquigarrow \sum_{\substack{i=1 \\ i \neq j}}^n p_i \tau(t_i)$.
  - Si $\tau(t_i)$ está en $\mathsf{Val} \cup \{\bot_A\}$ para todo i y $A = B \multimap C$, pero $\tau(t_i) \neq \bot_{B \multimap C}$ para todo i, se tiene que para todo i existe un término u_i tal que $\tau(t_i) = \lambda x.u_i$, por su tipo y porque considero que todas las posibles sumatorias están aplanadas. Entonces $\tau(t) = \sum_{i=1}^n p_i \tau(t_i)$ es un valor.
  - Si $\tau(t_j) \rightsquigarrow t'_j$ para algún j en $\{1, \ldots, n\}$, entonces se tiene

$$\tau(t) = \sum_{i=1}^{n} p_i \tau(t_i) \rightsquigarrow \sum_{\substack{i=1 \\ i \neq j}}^{n} p_i \tau(t_i) + p_j t'_j$$

- Sea $t = \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m - 1}\}$. En este caso se tiene $\tau(t) = \mathsf{letcase}^\circ\ x = \tau(r)\ \mathsf{in}\ \{\tau(t_0), \ldots, \tau(t_{2^m - 1})\}$. Por hipótesis, $\Gamma \vdash \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m - 1}\} : A$. Sean $\Gamma = \Gamma_1, \Gamma_2$ tal que $\Gamma_1, x : n \vdash t_i : A$ para todo i y $\Gamma_2 \vdash r : (m, n)$. Como $\tau \vDash \Gamma$, valen $\tau \vDash \Gamma_1$ y $\tau \vDash \Gamma_2$. Por hipótesis inductiva $\tau(r)$ o bien reduce, o bien está en $\mathsf{Val} \cup \{\bot_A\}$.

- Por el lema (4.6.8) se tiene que $\vdash \tau(r) : (m, n)$. Si $\tau(r)$ está en $\mathsf{Val} \cup \{\bot_A\}$, por su tipo vale $\tau(r) = \pi^m \rho^n$. Entonces se tiene que:

$$\tau(t) \rightsquigarrow \sum_{i=0}^{2^m-1} p_i \tau(t_i)[x := \rho_i^n]$$

  donde $p_i = \mathsf{tr}\left(\overline{\pi_i} \rho^n \overline{\pi_i^\dagger}\right)$ y $\rho_i^n = \frac{\overline{\pi_i} \rho^n \overline{\pi_i^\dagger}}{p_i}$.
- Si $\tau(r) \rightsquigarrow s$ entonces $\tau(t) \rightsquigarrow \mathsf{letcase}^\circ\ x = s\ \mathsf{in}\ \{\tau(t_0), \ldots, \tau(t_{2^m-1})\}$. □

La siguiente definición de coherencia entre una valuación θ y una función de cierre τ es necesaria ya que la demostración de la equivalencia entre funciones explícitas e implícitas se hace por separado del teorema de adecuación, donde esta equivalencia está garantizada.

Definición 4.6.11. Sea τ una función de cierre y θ una valuación, τ y θ son coherentes (notado $\tau \leftrightarrow \theta$) si y sólo si

$$\tau(x) = v \iff \theta(x) = (\!|v|\!)_\emptyset$$

El siguiente corolario es una consecuencia directa del lema de sustitución (4.5.6).

Corolario 4.6.12. *Sea t un término tal que $\Gamma \vdash t : A$, θ una valuación tal que $\theta \vDash \Gamma$ y τ una función de cierre tal que $\tau \vDash \Gamma$ y $\tau \leftrightarrow \theta$. Entonces vale $(\!|t|\!)_\theta = (\!|\tau(t)|\!)_\emptyset$.*

Demostración. Sean $x_1, x_2, \ldots, x_n$ las variables libres de t. Sea $\theta = \{x_1 := v_1, x_2 := v_2, \ldots, x_n := v_n\}$. Entonces, usando el lema (4.5.6) n veces:

$$\begin{aligned}
(\!|t|\!)_\theta &= (\!|t[x_1 := v_1]|\!)_{\theta \setminus x_1} \\
&= (\!|t[x_1 := v_1, x_2 := v_2]|\!)_{(\theta \setminus x_1) \setminus x_2} \\
&\vdots \\
&= (\!|t[x_1 := v_1, x_2 := v_2, \ldots, x_n := v_n]|\!)_\emptyset \\
&= (\!|\tau(t)|\!)_\emptyset
\end{aligned}$$

□

Finalmente, usando los lemas anteriores, a continuación se demuestra el lema de adecuación para funciones implícitas.

Lema 4.6.13 (Adecuación para funciones implícitas)**.** *Sea t un término tal que $\Gamma \vdash t : A \multimap B$, y θ una valuación tal que $\theta \vDash \Gamma$. Hay dos posibilidades:*

- *Existen n términos $t_1, \ldots, t_n$ y n reales $p_1, \ldots, p_n$ tales que $x : A \vdash t_i : B$, $0 < p_i \leq 1$, $\sum_{i=1}^n p_i \leq 1$ y $(\!|t|\!)_\theta = \sum_{i=1}^n p_i (\!|\lambda x.t_i|\!)_\emptyset$.*
- $(\!|t|\!)_\theta = \mathbb{0}_{\dim(A \multimap B)}$

Demostración. Sea τ una función de cierre tal que $\tau \vDash \Gamma$ y $\tau \leftrightarrow \theta$. Por el lema (4.6.10) se tiene que $\tau(t)$ o bien está en $\mathsf{Val} \cup \{\bot_A\}$ o bien reduce, y por el lema (4.6.12) se tiene que $(\!|t|\!)_\theta = (\!|\tau(t)|\!)_\emptyset$. Además por el corolario 4.6.9) se tiene que $\vdash \tau(t) : A \multimap B$.

- Si $\tau(t)$ está en $\mathsf{Val} \cup \{\bot_A\}$, por su tipo se tiene que o bien $\tau(t) = \sum_{i=1}^{n} p_i(\lambda x.t_i)$ para una variable x y términos t_i (tales que $x : A \vdash t_i : B$, $0 < p_i \leq 1$ y $\sum_{i=1}^{n} p_i \leq 1$), o bien $\tau(t) = \bot_{A \multimap B}$.

  En el primer caso se tiene:

$$(\!|t|\!)_\theta = (\!|\tau(t)|\!)_\emptyset = (\!|\sum_i p_i(\lambda x.t_i)|\!)_\emptyset = \sum_i p_i (\!|\lambda x.t_i|\!)_\emptyset$$

  En el segundo caso se tiene:

$$(\!|t|\!)_\theta = (\!|\tau(t)|\!)_\emptyset = (\!|\bot_{A \multimap B}|\!)_\emptyset = \mathbb{0}_{\dim(A \multimap B)}$$

- Si $\tau(t) \rightsquigarrow r$, como $\vdash \tau(t) : A \multimap B$, usando el teorema (3.2.3) se tiene que $\vdash r : A \multimap B$. Como $\tau(r) = r$ al ser r un término cerrado, usando el lema (4.6.10) sucesivamente se tiene que existen $r_1, \ldots, r_{n-1}$ términos cerrados y r_n en $\mathsf{Val} \cup \{\bot_A\}$, con $\vdash r_i : A \multimap B$, tales que

$$\tau(t) \rightsquigarrow r \rightsquigarrow r_1 \rightsquigarrow \cdots \rightsquigarrow r_n$$

  Esto es así ya que no hay reducciones infinitas debido al teorema de normalización fuerte (3.2.1). Por el teorema (4.5.7) se tiene entonces que:

$$(\!|t|\!)_\theta = (\!|\tau(t)|\!)_\emptyset = (\!|r|\!)_\emptyset = (\!|r_1|\!)_\emptyset = \cdots = (\!|r_n|\!)_\emptyset$$

  Como en particular $\vdash r_n : A \multimap B$ y r_n está en $\mathsf{Val} \cup \{\bot_A\}$, se tienen los mismos resultados que en el ítem anterior. □

4.6.3. Teorema de adecuación

Habiendo demostrado los lemas de adecuación para funciones (4.6.4) y (4.6.13), en esta sección se demuestra el teorema de adecuación (4.6.16) usando principalmente estos dos lemas, un lema auxiliar (4.6.14) y la segunda conjetura (4.6.15).

El siguiente lema establece que las combinaciones lineales pesadas por probabilidades de términos de un dominio pertenecen al mismo dominio, cuando la suma de las probabilidades es menor o igual a 1.

Lema 4.6.14. *Sea A un tipo. Para i en $\{1, \ldots, n\}$, sean $a_i \in (\!|A|\!)$ y $0 < p_i \leq 1$ con $\sum_{i=1}^{n} p_i \leq 1$. Entonces $\sum_{i=1}^{n} p_i a_i \in (\!|A|\!)$.*

Demostración. - Si $A = n$, se tiene $(\!|A|\!) = \mathcal{D}_n$.

  Como $p_i \leq 1$ para todo i, por el teorema (1.1.9) $\sum_{i=1}^{n} p_i a_i \in \mathcal{P}_n$.

  Por linealidad de la traza, se tiene que $\mathsf{tr}\left(\sum_{i=1}^{n} p_i a_i\right) = \sum_{i=1}^{n} p_i \mathsf{tr}\left(a_i\right)$. Esto está acotado por $\sum_{i=1}^{n} p_i \leq 1$ porque por hipótesis $a_i \in (\!|n|\!) = \mathcal{D}_n$.

- Si $A = (m, n)$, se tiene $(\!|A|\!) = \{p \mid p \in \bigoplus_{i=1}^{2^m-1} \mathcal{D}_n \text{ y } \mathsf{tr}\,(p) \leq 1\}$.

  Como por hipótesis $a_i \in (\!|(m, n)|\!)$, puedo descomponer los a_i como $a_i = \bigoplus_{j=0}^{2^m-1} a_{ij}$, donde $a_{ij} \in \mathcal{D}_n$. Entonces se tiene:

$$\sum_{i=1}^{n} p_i a_i = \sum_{i=1}^{n} p_i \left(\bigoplus_{j=0}^{2^m-1} a_{ij} \right) = \bigoplus_{j=0}^{2^m-1} \left(\sum_{i=1}^{n} p_i a_{ij} \right)$$

  Por el caso $A = n$ se tiene que $\sum_{i=1}^{n} p_i a_{ij} \in \mathcal{D}_n$ para todo $j \in \{0, \ldots, 2^m - 1\}$, por lo tanto $\sum_{i=1}^{n} p_i a_i \in \bigoplus_{i=0}^{2^m-1} \mathcal{D}_n$.

  Por linealidad de la traza, se tiene que $\mathsf{tr}\,(\sum_{i=1}^{n} p_i a_i) = \sum_{i=1}^{n} p_i \mathsf{tr}\,(a_i)$. Como por hipótesis $a_i \in (\!|(m, n)|\!)$, entonces esto está acotado por $\sum_{i=1}^{n} p_i \leq 1$.

- Si $A = B \multimap C$, se tiene $(\!|A|\!) = \{f \mid f \text{ positiva en } ((\!|B|\!) \otimes (\!|C|\!)) \oplus (\!|C|\!)\}$.

  Como $\sum_{i=1}^{n} p_i a_i$ es una combinación lineal positiva de elementos de $(\!|B \multimap C|\!)$, por el teorema (1.1.9) está en $(\!|B \multimap C|\!)$. □

La siguiente conjetura dice que la aplicación de las funciones preserva positividad. Es necesario ya que la conjetura (4.6.1) sólo establecía este hecho para la parte lineal de las interpretaciones. Esto es equivalente a pedir que la parte constante (es decir, la función evaluada en $\mathbb{0}$) es siempre positiva.

Conjetura 4.6.15 (# preserva positividad)**.** *Sean t un término y θ una valuación tales que $(\!|\lambda x.t|\!)_\theta \in (\!|A \multimap B|\!)$, entonces para todo a en $(\!|A|\!)$ se tiene que $(\!|t|\!)_{\theta, x=a} \in (\!|B|\!)$.*

Finalmente se demuestra el teorema de adecuación.

Teorema 4.6.16 (Adecuación)**.** *Si $\Gamma \vdash t : A$ y $\theta \vDash \Gamma$, entonces $(\!|t|\!)_\theta \in (\!|A|\!)$.*

Demostración. Por inducción en las reglas de tipado:

1. $\dfrac{}{\Gamma, x : A \vdash x : A}\ \mathsf{ax}$

   En este caso se tiene $(\!|x|\!)_\theta = \theta(x)$ por definición. Además por hipótesis se tiene que $\theta \vDash \Gamma, x : A$, por lo tanto $\theta(x) = (\!|x|\!)_\theta \in (\!|A|\!)$.

2. $\dfrac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \multimap B}\ \multimap_i$

   Por hipótesis inductiva vale que para todo θ' tal que $\theta' \vDash \Gamma, x : A$ se tiene que $(\!|t|\!)_{\theta'} \in (\!|B|\!)$. Sea $a \in (\!|A|\!)$, entonces $\theta' = \theta \cup \{x = a\} \vDash \Gamma, x : A$, por lo tanto $(\!|t|\!)_{\theta, x=a} \in (\!|B|\!)$. Además, $\mathbb{0}_{\dim(A)} \in (\!|A|\!)$, por lo tanto $(\!|t|\!)_{\theta, x=\bot} \in (\!|B|\!)$ también. Por definición se tiene que $(\!|\lambda x.t|\!)_\theta = \chi_{[a \mapsto (\!|t|\!)_{\theta, x=a}]}$ y por el lema (4.6.4) esto pertenece a $(\!|A \multimap B|\!)$.

3. $\dfrac{\Gamma \vdash t : A \multimap B \quad \Delta \vdash r : A}{\Gamma, \Delta \vdash tr : B}\ \multimap_e$

   Como se tiene $\theta \vDash \Gamma, \Delta$, vale que $\theta \vDash \Gamma$ y $\theta \vDash \Delta$. Por hipótesis inductiva vale entonces que $(\!|t|\!)_\theta \in (\!|A \multimap B|\!)$ y $(\!|r|\!)_\theta \in (\!|A|\!)$. Por el lema (4.6.13) se tiene entonces que o bien dado $n \in \mathbb{N}$ existen n términos $t_1, \ldots, t_n$ y n reales $p_1, \ldots, p_n$ tales que $(\!|t|\!)_\theta = \sum_{i=1}^{n} p_i (\!|\lambda x.t_i|\!)_\emptyset$ (con $x : A \vdash t_i : B$, $0 < p_i \leq 1$ y $\sum_{i=1}^{n} p_i \leq 1$), o bien $(\!|t|\!)_\theta = \mathbb{0}_{\dim(A \multimap B)}$.

   Por definición se tiene $(\!|tr|\!)_\theta = (\!|t|\!)_\theta \,\#\, (\!|r|\!)_\theta$.

- En el primer caso se tiene:

$$(\!|tr|\!)_\theta = \left(\sum_{i=1}^{n} p_i (\!|\lambda x.t_i|\!)_\emptyset\right) \# (\!|r|\!)_\theta = \sum_{i=1}^{n} p_i ((\!|\lambda x.t_i|\!)_\emptyset \# (\!|r|\!)_\theta)$$

  Por el lema (4.5.5) se tiene que esto es igual a $\sum_{i=1}^{n} p_i (\!|t_i|\!)_{x=(\!|r|\!)_\theta}$. Por la conjetura (4.6.15), $(\!|t_i|\!)_{x=(\!|r|\!)_\theta} \in (\!|B|\!)$ para todo i. Por el lema (4.6.14) esta combinación lineal está en $(\!|B|\!)$.

- En el segundo caso se tiene:

$$(\!|tr|\!)_\theta = \mathbb{0}_{\dim(A \multimap B)} \# (\!|r|\!)_\theta = \mathbb{0}_{\dim(B)} \in (\!|B|\!)$$

  Esto es así porque de acuerdo a la definición de $\#$, $\mathbb{0}_{\dim(A \multimap B)}$ es la función constante $a \mapsto \mathbb{0}_{\dim(B)}$.

4. $\dfrac{\Gamma, f : A \vdash t : A}{\Gamma \vdash \mu_n f.t : A}\ \mu$

   Asumo que tengo Γ y θ tal que $\Gamma \vdash \mu_n f.t : A$ y $\theta \vDash \Gamma$. Entonces por μ_n se tiene que $\Gamma, f : A \vdash t : A$. Usando $\multimap_i$ vale que entonces $\Gamma \vdash \lambda f.t : A \multimap A$. Usando el caso de adecuación para las abstracciones de más arriba, tengo que $(\!|\lambda f.t|\!)_\theta \in (\!|A \multimap A|\!)$.

   Quiero ver que $(\!|\mu_n f.t|\!)_\theta = (\!|\lambda f.t|\!)_\theta \#_n \mathbb{0}_{\dim(A)}$ está en $(\!|A|\!)$. Por inducción en n:

   - Caso base: $(\!|\lambda f.t|\!)_\theta \#_0 \mathbb{0}_{\dim(A)} = \mathbb{0}_{\dim(A)} \in (\!|A|\!)$ por definición.
   - $(\!|\lambda f.t|\!)_\theta \#_{n+1} \mathbb{0}_{\dim(A)} = (\!|\lambda f.t|\!)_\theta \# ((\!|\lambda f.t|\!)_\theta \#_n \mathbb{0}_{\dim(A)})$. Por hipótesis inductiva se tiene que $(\!|\lambda f.t|\!)_\theta \#_n \mathbb{0}_{\dim(A)} \in (\!|A|\!)$. Como $(\!|\lambda f.t|\!)_\theta$ pertenece a $(\!|A \multimap A|\!)$ se tiene que $(\!|\lambda f.t|\!)_\theta \#_{n+1} \mathbb{0}_{\dim(A)}$ está en $(\!|A|\!)$ por la conjetura (4.6.15).

5. $\dfrac{}{\Gamma \vdash \bot_A : A}\ \bot$

   Por definición se tiene que $(\!|\bot_A|\!)_\theta = \mathbb{0}_{\dim(A)}$. La matriz nula es hermítica, semidefinida positiva y de traza acotada por 1, por lo tanto $\mathbb{0}_{\dim(A)}$ pertenece a $(\!|A|\!)$ para todo tipo A.

6. $\dfrac{}{\Gamma \vdash \rho^n : n}\ \mathsf{ax}_\rho$

   Para todo θ, en particular tal que $\theta \vDash \Gamma$, vale que $(\!|\rho^n|\!)_\theta = \rho^n \in \mathcal{D}_n = (\!|n|\!)$.

7. $\dfrac{\Gamma \vdash t : n}{\Gamma \vdash U^m t : n}\ \mathsf{u}_i$

   Por hipótesis inductiva vale que para todo θ' tal que $\theta' \vDash \Gamma$ se tiene que $(\!|t|\!)_{\theta'} \in (\!|n|\!) = \mathcal{D}_n$.

   Como $\theta \vDash \Gamma$ entonces $(\!|t|\!)_\theta \in \mathcal{D}_n$. Por definición se tiene que $(\!|U^m t|\!)_\theta = \overline{U^m} (\!|t|\!)_\theta \overline{U^m}^\dagger$. Por el lema (1.1.13) se tiene que $\overline{U^m}$ es unitaria, y por el teorema (1.1.14) esto está en $\mathcal{D}_n$.

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

   Por hipótesis inductiva vale que para todo θ' tal que $\theta' \vDash \Gamma$ se tiene $(\!|t|\!)_{\theta'} \in (\!|n|\!) = \mathcal{D}_n$.

Como $\theta \vDash \Gamma$, entonces $(\!|t|\!)_\theta \in \mathcal{D}_n$. Por definición se tiene que $(\!|\pi^m t|\!)_\theta = \bigoplus_{i=0}^{2^m-1}(\overline{\pi_i}(\!|t|\!)_\theta\overline{\pi_i}^\dagger)$.

Como $(\!|t|\!)_\theta$ está en $\mathcal{D}_n$, por el lema (1.2.4), $\overline{\pi_i}(\!|t|\!)_\theta\overline{\pi_i}^\dagger$ también está en $\mathcal{D}_n$. Falta ver que se cumple la restricción de que $\mathsf{tr}\,((\!|\pi^m t|\!)_\theta) \leq 1$. Usando el lema (1.2.2), se tiene que $\mathsf{tr}\,((\!|\pi^m t|\!)_\theta) = \mathsf{tr}\left(\bigoplus_{i=0}^{2^m-1}\overline{\pi_i}(\!|t|\!)_\theta\overline{\pi_i}^\dagger\right) = \mathsf{tr}\,((\!|t|\!)_\theta)$, que está acotada por 1 por definición de $\mathcal{D}_n$.

Por lo tanto, $(\!|\pi^m r|\!)_\theta \in \bigoplus_{i=0}^{2^m-1}\mathcal{D}_n = (\!|(m,n)|\!)$.

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

Por hipótesis inductiva vale que para todo θ' tal que $\theta' \vDash \Gamma$ vale que $(\!|t|\!)_{\theta'} \in (\!|n|\!) = \mathcal{D}_n$; y que para todo θ'' tal que $\theta'' \vDash \Delta$ vale que $(\!|t|\!)_{\theta''} \in (\!|m|\!) = \mathcal{D}_m$.

Como por hipótesis se tiene que $\theta \vDash \Gamma, \Delta$, vale que $\theta \vDash \Gamma$ y $\theta \vDash \Delta$. Por lo tanto, $(\!|t|\!)_\theta \in \mathcal{D}_n$ y $(\!|r|\!)_\theta \in \mathcal{D}_m$.

Entonces se tiene que $(\!|r \otimes s|\!)_\theta = (\!|r|\!)_\theta \otimes (\!|s|\!)_\theta \in \mathcal{D}_{n+m} = (\!|n+m|\!)$ porque la aridad del producto tensorial está dada por $\otimes\colon \mathcal{D}_n \times \mathcal{D}_m \to \mathcal{D}_{n+m}$.

10. $\dfrac{\Delta_0, x : n \vdash t_0 : A \quad \ldots \quad \Delta_{2^m-1}, x : n \vdash t_{2^m-1} : A \quad \Gamma \vdash r : (m,n) \quad \ell(A) \neq (m',n')}{\Delta_0, \ldots, \Delta_{2^m-1}, \Gamma \vdash \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} : A}\ \mathsf{m}_e$

Por hipótesis inductiva vale que para todo θ' tal que $\theta' \vDash \Gamma$ se tiene que $(\!|r|\!)_{\theta'} \in (\!|(m,n)|\!)$. Como $\theta \vDash \Delta_0, \ldots, \Delta_{2^m-1}, \Gamma$, vale que $\theta \vDash \Gamma$ y entonces $(\!|r|\!)_\theta \in (\!|(m,n)|\!)$.

También por hipótesis inductiva vale que para todo i en $\{0, \ldots, 2^m-1\}$, para todo θ' tal que $\theta' \vDash \Delta_i, x : n$ se tiene que $(\!|t_i|\!)_{\theta'} \in (\!|A|\!)$. Como $\theta \vDash \Delta_0, \ldots, \Delta_{2^m-1}, \Gamma$, en particular $\theta \vDash \Delta_i$ para todo i y $\theta \cup \{x := \rho\} \vDash \Delta_i, x : n$ para todo $\rho \in \mathcal{D}_n$. Por lo tanto $(\!|t_i|\!)_{\theta, x=\rho} \in (\!|A|\!)$ para todo $\rho \in \mathcal{D}_n$ y todo $i \in \{0, \ldots, 2^m-1\}$.

Por definición se tiene que:

$$(\!|\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}|\!)_\theta = \sum_{i=0}^{2^m-1} \mathsf{tr}\,(\rho_i)\,(\!|t_i|\!)_{\theta, x=\widetilde{\rho_i}}$$

donde $(\!|r|\!)_\theta = \bigoplus_{i=0}^{2^m-1}\rho_i \in (\!|(m,n)|\!)$ y

$$\widetilde{\rho_i} = \begin{cases} \dfrac{\rho_i}{\mathsf{tr}\,(\rho_i)} & \text{si } \mathsf{tr}\,(\rho_i) \neq 0 \\ \rho_i & \text{si } \mathsf{tr}\,(\rho_i) = 0 \end{cases}$$

$\widetilde{\rho_i} \in \mathcal{D}_n$ porque $\rho_i \in \mathcal{D}_n$ y $\mathsf{tr}\left(\frac{\rho}{\mathsf{tr}(\rho)}\right) = 1$, por lo tanto $(\!|t_i|\!)_{\theta, x=\widetilde{\rho_i}} \in (\!|A|\!)$ para todo i en $\{0, \ldots, 2^m-1\}$.

Como $\rho_i \in \mathcal{D}_n$ para todo i, se tiene $0 \leq \mathsf{tr}\,(\rho_i) \leq 1$. Además, como $(\!|r|\!)_\theta \in (\!|(m,n)|\!)$, se tiene $\mathsf{tr}\,((\!|r|\!)_\theta) \leq 1$. Por lo tanto,

$$\mathsf{tr}\,((\!|r|\!)_\theta) = \mathsf{tr}\left(\bigoplus_{i=0}^{2^m-1}\rho_i\right) = \sum_{i=0}^{2^m-1}\mathsf{tr}\,(\rho_i) \leq 1$$

Entonces por el lema (4.6.14), $\sum_{i=0}^{2^m-1}\mathsf{tr}\,(\rho_i)\,(\!|t_i|\!)_{\theta, x=\widetilde{\rho_i}} \in (\!|A|\!)$.

11. $$\frac{\Gamma \vdash t_1 : A \quad \dots \quad \Gamma \vdash t_n : A \quad \sum_{i=1}^{n} p_i \leq 1 \quad \ell(A) \neq (m,n)}{\Gamma \vdash \sum_{i=1}^{n} p_i t_i : A} +$$

Por hipótesis inductiva se tiene que para todo θ' tal que $\theta' \vDash \Gamma$ vale $(\!|t_i|\!)_{\theta'} \in (\!|A|\!)$ para todo i en $\{1, \dots, n\}$.

Como por hipótesis $\theta \vdash \Gamma$, vale $(\!|t_i|\!)_\theta \in (\!|A|\!)$ para todo i en $\{1, \dots, n\}$.

Por definición se tiene que $(\!|\sum_{i=1}^{n} p_i t_i|\!)_\theta = \sum_{i=1}^{n} p_i (\!|t_i|\!)_\theta$, y por el lema (4.6.14) esto está en $(\!|A|\!)$. □

4.7. Dominios acotados

Para ver que el límite del punto fijo existe en el cálculo vamos a demostrar que todos los términos posibles tienen su traza acotada. La parte del dominio que representa a los tipos n y (m, n) tiene su traza trivialmente acotada por 1, por definición. La parte que no tiene una cota definida para la traza es la de las funciones, y se puede ver que al interpretar la parte lineal de estos términos en el espacio generado por el producto tensorial de la interpretación de los espacios de salida y llegada, esto introduce términos con traza potencialmente mayor a 1. Un ejemplo de esto es la función identidad en $1 \multimap 1$, cuya interpretación tiene traza igual a 2:

$$(\!|\lambda x.x|\!)_\emptyset = \chi_{[a \mapsto (\!|x|\!)_{x=a}]} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Se define el tamaño de los tipos como el valor de la cota para la traza que van a tener los términos bien tipados correspondientes. A continuación se demuestra que esta cota es correcta.

Definición 4.7.1 (Tamaño de tipos)**.**

- $N_n = 1$
- $N_{(m,n)} = 1$
- $N_{A \multimap B} = (\dim(A) + 1) N_B$

Teorema 4.7.2. *Para todo término cerrado t tal que $\vdash t \colon A$ vale que* $\mathsf{tr}\,((\!|t|\!)_\emptyset) \leq N_A$.

Demostración. Por inducción en los tipos.

Por el teorema (4.6.16) se tiene que $(\!|t|\!)_\emptyset \in (\!|A|\!)$ para todo tipo A.

- Si $A = n$ ó $A = (m, n)$, vale que $\mathsf{tr}\,((\!|t|\!)_\emptyset) \leq 1$ por definición de $(\!|n|\!)$ y $(\!|(m,n)|\!)$.
- Si $A = B \multimap C$, por el lema (4.6.13) hay dos posibilidades:
  - Para $n \in \mathbb{N}$, existen n términos $t_1, \dots, t_n$ y n reales $p_1, \dots, p_n$ tales que $x : B \vdash t_i : C$, $0 < p_i \leq 1$, $\sum_{i=1}^{n} p_i \leq 1$ y $(\!|t|\!)_\emptyset = \sum_{i=1}^{n} p_i (\!|\lambda x.t_i|\!)_\emptyset$. Por linealidad de la

traza:

$$\begin{aligned}
\mathsf{tr}\left(\llparenthesis t \rrparenthesis_{\emptyset}\right) &= \mathsf{tr}\left(\sum_{i=1}^{n} p_i \llparenthesis \lambda x.t_i \rrparenthesis_{\emptyset}\right) \\
&= \sum_{i=1}^{n} p_i \mathsf{tr}\left(\llparenthesis \lambda x.t_i \rrparenthesis_{\emptyset}\right) \\
&= \sum_{i=1}^{n} p_i \left(\sum_{j=1}^{\dim(B)} \mathsf{tr}\left(\llparenthesis t_i \rrparenthesis_{x=E_{ii}^B} - \llparenthesis t_i \rrparenthesis_{x=\mathbb{0}_{\dim(B)}}\right) + \mathsf{tr}\left(\llparenthesis t_i \rrparenthesis_{x=\mathbb{0}_{\dim(B)}}\right)\right) \\
&= \sum_{i=1}^{n} p_i \left(\sum_{j=1}^{\dim(B)} \mathsf{tr}\left(\llparenthesis t_i \rrparenthesis_{x=E_{ii}^B}\right) - \sum_{j=1}^{\dim(B)} \mathsf{tr}\left(\llparenthesis t_i \rrparenthesis_{x=\mathbb{0}_{\dim(B)}}\right) + \mathsf{tr}\left(\llparenthesis t_i \rrparenthesis_{x=\mathbb{0}_{\dim(B)}}\right)\right)
\end{aligned}$$

Por la conjetura (4.6.15), tanto $\llparenthesis t_i \rrparenthesis_{x=E_{ii}^B}$ como $\llparenthesis t_i \rrparenthesis_{x=\mathbb{0}_{\dim(B)}}$ están en $\llparenthesis C \rrparenthesis$, para todo i. Por lo tanto, y por hipótesis inductiva, todos esos términos son positivos y están acotados por N_C. Entonces se tiene:

$$\mathsf{tr}\left(\llparenthesis t \rrparenthesis_{\emptyset}\right) \leq \sum_{i=1}^{n} p_i \left(\sum_{j=1}^{\dim(B)} N_C + N_C\right) = \sum_{i=1}^{n} p_i (N_{B \multimap C}) \leq N_{B \multimap C}$$

La última desigualdad se obtiene por la cota a la sumatoria de p_i.

- $\llparenthesis t \rrparenthesis_{\emptyset} = \mathbb{0}_{\dim(B \multimap C)}$
  Este caso es trivial ya que:

$$\mathsf{tr}\left(\llparenthesis t \rrparenthesis_{\emptyset}\right) = \mathsf{tr}\left(\mathbb{0}_{\dim(B \multimap C)}\right) = 0 \leq N_{B \multimap C}$$ □

4.8. Existencia de punto fijo

Habiendo visto que todos los términos de $\lambda_{\rho}^{\mu_n}$ se interpretan en dominios de matrices positivas y con trazas acotadas según su tipo, falta ver que estos dominios cumplen con la definición de CPO para cierto orden definido en ellos. Además es necesario ver algunas propiedades que las interpretaciones de funciones cumplen, con el objetivo de probar la existencia del límite del punto fijo incremental. Con esa existencia probada, se reemplaza el punto fijo incremental de $\lambda_{\rho}^{\mu_n}$ por el punto fijo a secas definiendo así el cálculo λ_{ρ}^{μ}. Su interpretación va a ser el límite de la interpretación del punto fijo incremental.

En el caso de las matrices cuadradas complejas, las cuales contienen a los dominios, los supremos de las sucesiones son iguales a sus límites por [Sel04, Observación 3.8]. Por lo tanto la definición de continuidad (1.1.17) y el teorema de punto fijo (1.1.18) serán usados en este contexto, reemplazando los supremos de las cadenas por su límite.

Se define el siguiente orden sobre las matrices positivas. Este define un CPO sobre los dominios, como se demostrará en el lema (4.8.5).

Definición 4.8.1 (Orden de Löwner)**.** Sean $A, B \in \mathcal{P}_n$. Entonces $A \sqsubseteq_L B$ si y sólo si $B - A \in \mathcal{P}_n$.

Lema 4.8.2. *Las funciones explícitas de $\lambda_\rho^{\mu_n}$ preservan el orden de Löwner.*

Demostración. Sea t tal que $\Gamma, x : A \vdash t : A$, con $\theta \vDash \Gamma$. Quiero ver que para todo $a, b \in (\!|A|\!)$, si $a \sqsubseteq_L b$ entonces $(\!|\lambda x.t|\!)_\theta \# a \sqsubseteq_L (\!|\lambda x.t|\!)_\theta \# b$.

Por la conjetura (4.6.1) y el lema (4.5.1), se tiene que la siguiente función es lineal y completamente positiva, donde $n = \dim(A)$.

$$f(c) = (\!|t|\!)_{\theta, x=c} - (\!|t|\!)_{\theta, x=\mathbb{0}_n}$$

Como $a \sqsubseteq_L b$ por hipótesis, $b - a$ es una matriz positiva y como f es completamente positiva, $f(b-a)$ es una matriz positiva. Pero además f es lineal, entonces $f(b-a) = f(b) - f(a)$ es positiva.

$$\begin{aligned} f(b-a) =& (\!|t|\!)_{\theta, x=b} - (\!|t|\!)_{\theta, x=\mathbb{0}_n} - ((\!|t|\!)_{\theta, x=a} - (\!|t|\!)_{\theta, x=\mathbb{0}_n}) \\ =& (\!|t|\!)_{\theta, x=b} - (\!|t|\!)_{\theta, x=a} \end{aligned}$$

Por el lema (4.5.5) se tiene que $(\!|t|\!)_{\theta, x=a} = (\!|\lambda x.t|\!)_\theta \# a$ y $(\!|t|\!)_{\theta, x=b} = (\!|\lambda x.t|\!)_\theta \# b$. Reemplazando vale:

$$f(b-a) = (\!|\lambda x.t|\!)_\theta \# b - (\!|\lambda x.t|\!)_\theta \# a$$

Por lo tanto $(\!|\lambda x.t|\!)_\theta \# b - (\!|\lambda x.t|\!)_\theta \# a$ es una matriz positiva, lo que implica que

$$(\!|\lambda x.t|\!)_\theta \# a \sqsubseteq_L (\!|\lambda x.t|\!)_\theta \# b$$

□

El siguiente lema muestra que las funciones del cálculo sobre las que se puede calcular punto fijo son continuas según la definición (1.1.17), usando el límite.

Lema 4.8.3. *Las funciones explícitas de $\lambda_\rho^{\mu_n}$ son continuas.*

Demostración. Por el lema (4.8.2) se tiene que las funciones explícitas de $\lambda_\rho^{\mu_n}$ son monótonas respecto al orden de Löwner.

Sea (P_n) una sucesión creciente de elementos de $\mathcal{P}_n$ tal que $\lim_{n\to\infty} P_n = P$. Esto significa que para todo $1 \leq i, j \leq n, \lim_{n\to\infty}(P_n)_{ij} = P_{ij}$, donde $(P_n)_{ij}$ es una sucesión en $\mathbb{C}$. Sean L_{ij}, K en $\mathbb{C}^{m\times m}$ y $\{E_{ij}^n\}$ la base canónica de $\mathbb{C}^{n\times n}$ tal que:

$$\chi = \left(\sum_{i=1}^{n} \sum_{j=1}^{n} E_{ij}^n \otimes L_{ij} \right) \oplus K$$

Como el primer término de la aplicación es lineal en el argumento por el lema (4.3.3), es lineal en cada elemento de la matriz. Por lo tanto la aplicación es continua en cada elemento de la matriz sobre la cual actúa:

$$\lim_{n\to\infty} \chi \# P_n = \lim_{n\to\infty} \sum_{i=1}^{n}\sum_{j=1}^{n} (P_n)_{ij} L_{ij} + K = \sum_{i=1}^{n}\sum_{j=1}^{n} P_{ij} L_{ij} + K = \chi \# P = \chi \# \left(\lim_{n\to\infty} P_n \right)$$

□

El siguiente lema es necesario para demostrar la existencia del límite en todas las cadenas crecientes de acuerdo al orden de Löwner en los dominios.

Lema 4.8.4. *Para toda M en $\mathcal{P}_n$ y u en $\mathbb{C}^n$ se tiene que $u^\dagger M u \leq \mathsf{tr}\,(M)\,\|u\|^2$.*

Demostración. Como M es positiva, es diagonalizable y se la puede descomponer como $P^{-1}DP$ donde $D \in \mathbb{C}^{n\times n}$ es diagonal y $P \in \mathbb{C}^{n\times n}$ es unitaria.

Por lo tanto se tiene que

$$u^\dagger M u = u^\dagger (P^{-1}DP)u = (u^\dagger P^{-1})D(Pu) = v^\dagger D v$$

definiendo $v = Pu \in \mathbb{C}^n$. Llamando $v_i \in \mathbb{C}$ a las componentes de v:

$$u^\dagger M u = \sum_i v_i^2 d_{ii} \leq \left(\sum_i v_i^2\right)\left(\sum_i d_{ii}\right) = \mathsf{tr}\,(D)\,\|v\|^2 = \mathsf{tr}\,(M)\,\|u\|^2$$

La desigualdad vale porque $d_{ii} \geq 0$ para todo i ya que son los autovalores de M, que es una matriz positiva. □

El siguiente lema acerca de la estructura de los dominios de λ_ρ^μ está demostrado en forma análoga a la proposición (3.6) en [Sel04].

Lema 4.8.5. *Para todo A tipo de $\lambda_\rho^{\mu_n}$ $(\!|A|\!), \sqsubseteq_L)$ es un orden parcial completo.*

Demostración. Quiero ver que para todo dominio de λ_ρ^μ las sucesiones crecientes respecto al orden de Löwner tienen supremo. Los dominios están compuestos de matrices positivas, restringidas con una cota para la traza que depende del tipo asociado a cada dominio.

Sea A un tipo cualquiera de λ_ρ^μ. Su dominio asociado es $(\!|A|\!) \subseteq \mathcal{P}_{2^n}$. Sean M_1 y M_2 matrices en $(\!|A|\!)$.

Por definición $M_1 \sqsubseteq_L M_2$ si y sólo si $M_2 - M_1$ es una matriz positiva, y esto sucede si y sólo si $u^\dagger(M_2 - M_1)u \geq 0$ para todo u en $\mathbb{C}^{2^n}$. Por lo tanto $M_1 \sqsubseteq_L M_2$ si y sólo si $u^\dagger M_1 u \leq u^\dagger M_2 u$ para todo u en $\mathbb{C}^{2^n}$.

De esta forma cualquier sucesión creciente en $(\!|A|\!)$:

$$M_1 \sqsubseteq_L M_2 \sqsubseteq_L \ldots \sqsubseteq_L M_n \sqsubseteq_L \ldots$$

tiene una sucesión creciente correspondiente en $\mathbb{R}_{\geq 0}$ para cada u en $\mathbb{C}^{2^n}$:

$$u^\dagger M_1 u \leq u^\dagger M_2 u \leq \cdots \leq u^\dagger M_n u \leq \ldots$$

Usando el lema (4.8.4) y el corolario (4.7.2) se tiene que los elementos de la sucesión creciente $\{u^\dagger M_n u\}_n$ están acotados por $N_A \|u\|^2$, ya que las matrices M_n están en $(\!|A|\!)$. Cualquier sucesión creciente y acotada en $\mathbb{R}$ tiene supremo. Por lo tanto la sucesión correspondiente $\{M_n\}$ en $(\!|A|\!)$ también tiene supremo, y éste cumple con la cota de la traza por continuidad de la traza, por lo tanto está en $(\!|A|\!)$. □

Como corolario de los lemas de esta sección y usando el teorema de punto fijo del capítulo de Preliminares (1.1.18), se demuestra su existencia en los dominios del cálculo.

Corolario 4.8.6. *El mínimo punto fijo existe en λ_ρ^μ y se interpreta como el límite infinito del punto fijo incremental.*

Demostración. Por los lemas (4.8.3) y (4.8.5), usando el teorema (1.1.18). □

4.9. Semántica denotacional del cálculo con punto fijo

Se define la semántica de λ_ρ^μ igual a la de $\lambda_\rho^{\mu_n}$, excepto en la interpretación del punto fijo. Usando el corolario (4.8.6) esta se define como el límite de la interpretación del punto fijo incremental en $\lambda_\rho^{\mu_n}$, es decir:

$$(\!|\mu x.t|\!)_\theta = \lim_{n\to\infty} \left((\!|\lambda x.t|\!)_\theta \#_n \mathbb{0}_{\dim(A)}\right)$$

Ejemplos

- El término del ejemplo (3.1.1) tiene la siguiente interpretación:

$$\begin{aligned}(\!|\mu x.\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\}|\!)_\emptyset &= \lim_{n\to\infty} (\!|\lambda x.\mathsf{letcase}^\circ\ z = \pi^1|+\rangle\langle+|\ \mathsf{in}\ \{x, |+\rangle\langle+|\}|\!)_\emptyset \#_n \mathbb{0}_2 \\ &= \lim_{n\to\infty} \left(\tfrac{1}{2}x + \tfrac{1}{2}|+\rangle\langle+|\right) \#_n \mathbb{0}_2 \\ &= \lim_{n\to\infty} \tfrac{1}{2^n}\mathbb{0}_2 + \sum_{i=1}^{n} \tfrac{1}{2^i}|+\rangle\langle+| \\ &= \lim_{n\to\infty} \left(\frac{1-\frac{1}{2^{n+1}}}{1-\frac{1}{2}} - 1\right)|+\rangle\langle+| = |+\rangle\langle+|\end{aligned}$$

- La función identidad tiene como puntos fijos a todos los elementos de su dominio. La interpretación de su punto fijo es entonces el mínimo del dominio, es decir la matriz nula:

$$(\!|\mu x.x|\!)_\emptyset = \lim_{n\to\infty} (\!|\lambda x.x|\!)_\emptyset \#_n \mathbb{0}_2 = \mathbb{0}_2$$

5. CONCLUSIONES Y TRABAJO FUTURO

En esta tesis se definieron los cálculos $\lambda_\rho^{\mu_n}$ y λ_ρ^{μ}, que agregan punto fijo al cálculo λ_ρ° definido en [DC17]. Para hacerlo se redefinió por completo la semántica respecto a la original, en dominios de matrices positivas. El resultado conseguido asume la validez de las conjeturas (4.6.1) y (4.6.15). Esto representa un puntapié inicial hacia la definición de punto fijo en este cálculo, y aunque creemos que la conjeturas son ciertas es necesario demostrarlas. Esto queda como trabajo futuro.

Trabajo futuro

Un camino posible para demostrar las conjeturas es el siguiente. En [Cho75, Teorema 1], Choi da la siguiente forma de descomposición para los mapas completamente positivos:

Teorema. *Sea* $\Phi : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$. *Entonces* Φ *es completamente positivo si y sólo si* Φ *es de la forma* $\Phi(A) = \sum_i V_i^\dagger A V_i$ *para todo* A *en* $\mathbb{C}^{n\times n}$ *donde* V_i *son matrices de* $n \times m$.

Si pudiéramos redefinir la semántica de las funciones en términos de estas V_i, podríamos tener asegurado que preservan la positividad, lo cual resolvería la segunda conjetura. La primera conjetura, donde se afirma que la parte lineal de las funciones es completamente positiva para tener adecuación de las abstracciones, tendría que revisarse ya que una nueva semántica en función de las V_i tendría que estar definida de forma tal de cumplir adecuación.

Queda pendiente también demostrar confluencia para esta extensión. Romero demuestra en [Rom20] que λ_ρ° es confluente, por lo que se espera que $\lambda_\rho^{\mu_n}$ y λ_ρ^{μ} también lo sean.

Bibliografía

[AD17] Arrighi, Pablo y Gilles Dowek: *Lineal: A linear-algebraic Lambda-calculus*. Log. Methods Comput. Sci., 13(1), 2017.

[ADC12] Arrighi, Pablo y Alejandro Díaz-Caro: *A System F accounting for scalars*. Logical Methods in Computer Science, 8(1:11), 2012.

[ADCP+14] Assaf, Ali, Alejandro Díaz-Caro, Simon Perdrix, Christine Tasson y Benoît Valiron: *Call-by-value, call-by-name and the vectorial behaviour of the algebraic λ-calculus*. Logical Methods in Computer Science, 10(4:8), 2014.

[ADCV17] Arrighi, Pablo, Alejandro Díaz-Caro y Benoît Valiron: *The Vectorial Lambda-Calculus*. Information and Computation, 254(1):105–139, 2017.

[AG05] Altenkirch, T. y J. Grattage: *A Functional Quantum Programming Language*. 20th Annual IEEE Symposium on Logic in Computer Science (LICS' 05), 2005.

[Bor19] Borgna, Agustín: *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.

[BP15] Bădescu, Costin y Prakash Panangaden: *Quantum Alternation: Prospects and Problems*. Electronic Proceedings in Theoretical Computer Science, 195:33–42, Noviembre 2015, ISSN 2075-2180. http://dx.doi.org/10.4204/EPTCS.195.3.

[Cho75] Choi, Man Duen: *Completely positive linear maps on complex matrices*. Linear Algebra and its Applications, 10(3):285–290, 1975.

[DC17] Díaz-Caro, Alejandro: *A lambda calculus for density matrices with classical and probabilistic controls*. En Chang, Bor Yuh Evan (editor): *Programming Languages and Systems (APLAS 2017)*, volumen 10695 de *Lecture Notes in Computer Science*, páginas 448–467. Springer, Cham, 2017.

[DCD17] Díaz-Caro, Alejandro y Gilles Dowek: *Typing quantum superpositions and measurement*. En Martín-Vide, Carlos, Roman Neruda y Miguel A. Vega-Rodríguez (editores): *Theory and Practice of Natural Computing (TPNC 2017)*, volumen 10687 de *Lecture Notes in Computer Science*, páginas 281–293. Springer, Cham, 2017.

[DCGMV19] Díaz-Caro, Alejandro, Mauricio Guillermo, Alexandre Miquel y Benoît Valiron: *Realizability in the Unitary Sphere*. En *Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2019)*, páginas 1–13, 2019.

[DCP12] Díaz-Caro, Alejandro y Barbara Petit: *Linearity in the non-deterministic call-by-value setting*. En Ong, Luke y Ruy de Queiroz (editores): *Logic,*

Language, Information and Computation, volumen 7456 de *Lecture Notes in Computer Science*, páginas 216–231. Springer, Berlin, Heidelberg, 2012.

[DP06] D'HONDT, ELLIE y PRAKASH PANANGADEN: *Quantum weakest preconditions.* Mathematical Structures in Computer Science, 16(3):429–451, Junio 2006, ISSN 1469-8072.

[FDY11] Feng, Yuan, Runyao Duan y Mingsheng Ying: *Bisimulation for quantum processes.* Proceedings of the 38th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages - POPL '11, 2011.

[FYY13] Feng, Yuan, Nengkun Yu y Mingsheng Ying: *Model checking quantum Markov chains.* Journal of Computer and System Sciences, 79(7):1181–1198, Noviembre 2013, ISSN 0022-0000.

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

[Mar17] Martínez, Guido: *Confluencia en sistemas de reescritura probabilista.* Tesis de Licenciatura, Universidad Nacional de Rosario, 2017.

[NC11] Nielsen, Michael A. y Isaac L. Chuang: *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2011, ISBN 1107002176.

[PSV14] Pagani, Michele, Peter Selinger y Benoît Valiron: *Applying Quantitative Semantics to Higher-Order Quantum Computing.* En *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2014, San Diego*, volumen 49(1) de *ACM SIGPLAN Notices*, Enero 2014.

[Rom20] Romero, Lucas Rafael: *Una extensión polimórfica para los λ-cálculos cuánticos λ_ρ y λ°_ρ.* Tesis de Licenciatura, Universidad de Buenos Aires, 2020.

[Sel04] Selinger, Peter: *Towards a Quantum Programming Language.* Mathematical Structures in Computer Science, 14(4):527–586, 2004.

[SV05] Selinger, Peter y Benoît Valiron: *A Lambda Calculus for Quantum Computation with Classical Control.* En *Proceedings of the 7th International Conference on Typed Lambda Calculi and Applications, TLCA 2005, Nara, Japan*, volumen 3461 de *Lecture Notes in Computer Science*, páginas 354–368. Springer, 2005.

[SV08] Selinger, Peter y Benoît Valiron: *On a Fully Abstract Model for a Quantum Linear Functional Language.* En *Proceedings of the 4th International Workshop on Quantum Programming Languages, QPL 2006, Oxford*, volumen 210 de *Electronic Notes in Theoretical Computer Science*, páginas 123–137. Elsevier, 2008.

[Ter03] Terese: *Term Rewriting Systems*, volumen 55 de *Cambridge Tracts in Theoretical Computer Science.* Cambridge University Press, 2003.

[vT04] Tonder, André van: *A Lambda Calculus for Quantum Computation.* SIAM Journal on Computing, 33(5):1109–1135, Enero 2004, ISSN 1095-7111.

[Win93] Winskel, Glynn: *The Formal Semantics of Programming Languages: An Introduction.* Foundation of Computing series. MIT Press, 1993, ISBN 978-0-262-23169-5.

[Yin12] Ying, Mingsheng: *Floyd–Hoare Logic for Quantum Programs.* ACM Trans. Program. Lang. Syst., 33(6), Enero 2012, ISSN 0164-0925.

[Yin16] Ying, Mingsheng: *Foundations of Quantum Programming.* Elsevier, 2016.

[YYF12] Ying, Mingsheng, Nengkun Yu y Yuan Feng: *Defining Quantum Control Flow*, 2012.

[YYF14] Ying, Mingsheng, Nengkun Yu y Yuan Feng: *Alternation in Quantum Programming: From Superposition of Data to Superposition of Programs*, 2014.

[YYW17] Ying, Mingsheng, Shenggang Ying y Xiaodi Wu: *Invariants of Quantum Programs: Characterisations and Generation.* SIGPLAN Not., 52(1):818–832, Enero 2017, ISSN 0362-1340.

[Zor16] Zorzi, Margherita: *On quantum lambda calculi: a foundational perspective.* Mathematical Structures in Computer Science, 26(7):1107–1195, 2016.