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

A Compositional Extension of λ°_{ρ} via Pauli Decomposition

Tesis de Licenciatura en Ciencias de la Computación

Tomás Miguez

Director: Alejandro Díaz-Caro

Buenos Aires, 2026

UNA EXTENSIÓN COMPOSICIONAL DE λ_ρ° MEDIANTE LA DESCOMPOSICIÓN DE PAULI

Extendemos el cálculo lambda cuántico λ_ρ°, un cálculo que manipula matrices de densidad con control probabilístico, con un operador let. El cálculo original, propuesto por Díaz-Caro, permite expresar algoritmos cuánticos donde los datos se representan mediante matrices de densidad en lugar de vectores de estado, sin necesidad de mantener un registro separado de dichos datos. Sin embargo, carece de un mecanismo para descomponer un estado cuántico de múltiples qubits en sus componentes individuales. Nuestra extensión introduce un constructor let $x^{\otimes n} = \rho^n$ in t que, mediante la descomposición de Pauli y la descomposición espectral de las matrices de Pauli, expresa cualquier estado de n qubits como combinación lineal de productos tensoriales de estados de un único qubit. Esto permite que los programas operen sobre qubits individuales de un sistema compuesto de manera algebraicamente coherente. Además, presentamos una interpretación semántica simplificada de λ_ρ° que elimina el seguimiento innecesario de los resultados de medición. Presentamos la gramática extendida, el sistema de reescritura, el sistema de tipos y la interpretación semántica del cálculo resultante, y demostramos las propiedades fundamentales de Subject Reduction, Progress, Strong Normalisation, Soundness y Adequacy. Mostramos además que cuando una variable ligada por let no aparece libre en el cuerpo, el constructor computa correctamente la traza parcial sobre los qubits descartados, respetando así el teorema cuántico de no-borrado.

Palabras clave: cálculo lambda, computación cuántica, matrices de densidad, descomposición de Pauli, composicionalidad, control clásico.

A COMPOSITIONAL EXTENSION OF λ_ρ° VIA PAULI DECOMPOSITION

We extend the quantum lambda calculus λ_ρ°, a calculus that manipulates density matrices with probabilistic control, with a let operator. The original calculus, proposed by Díaz-Caro, allows the expression of quantum algorithms where data is represented by density matrices instead of state vectors, without keeping track of said data in separate registries. However, it lacks a mechanism for decomposing a multi-qubit quantum state into its individual components. Our extension introduces a construct let $x^{\otimes n} = \rho^n$ in t that, via the Pauli decomposition and the spectral decomposition of the Pauli matrices, expresses any n-qubit state as a linear combination of tensor products of single-qubit states. This allows programs to operate on individual qubits of a composite system in an algebraically coherent way. Additionally, we present a simplified semantic interpretation of λ_ρ° that removes the unnecessary tracking of measurement outcomes. We present the extended grammar, rewrite system, type system, and semantic interpretation of the resulting calculus, and prove the fundamental properties of Subject Reduction, Progress, Strong Normalisation, Soundness, and Adequacy. We further show that when a variable bound by let does not appear free in the body, the construct correctly computes the partial trace over the discarded qubits, thus respecting the quantum no-deleting theorem.

Keywords: lambda calculus, quantum computing, density matrices, Pauli decomposition, compositionality, classical control.

AGRADECIMIENTOS

Me parece importante reconocer a toda la gente que fue parte de este proyecto, directamente debido a haber participado activamente, o indirectamente producto de acompañarme durante todo el proceso.

Gracias a mi familia; Sandra, Sofía, Gustavo y Bichi por siempre estar ahí. A Fran que es como un hermano desde hace más de media vida. Lo mismo para mis amigos de todos los días que hacen todo más llevadero; Gonza, Fer, Ian, Guido, Seba y Lucas. A mis compañeros de secundaria con los que pasé grandes momentos; Oli, Manu, Dante y Ale. Y ya más cercano a este trabajo, la gente de la facu con la que hice incontables TPs y cursé muchas materias; Mauro, Martín y Nacho. Quiero mencionar también a la gente del laburo, que fomentan un ambiente en el que seguir con una carrera es algo más que posible, incluso buscado; Juan, Clau, Hashi, Caro, Emi, Seba, Her y tantos más.

Quiero también agradecerle a los docentes y no docentes de la facultad, proveyendo una educación de calidad en todo contexto.

Por último me gustaría agradecerle a Jano, por su tutela y por hacer de esta tesis algo sumamente disfrutable, teniendome paciencia incluso cuando me borraba un par de meses. Y a los jurados, Romain y Rafael por la buena onda y el trabajo de revisión y evaluación que realizaron.

¡Gracias a todos!

CONTENTS

0. PRELIMINARIES

This chapter provides the theoretical background necessary for the rest of the thesis. We begin with a summary of the notation used throughout, then introduce quantum computing in the density matrix formalism, present the quantum lambda calculus λ_ρ° from [2], recall the Pauli decomposition of density matrices, and finally review the spectral decomposition theorem that will be needed later.

0.1 Notation

Quantum states and operators. We write $|\psi\rangle$ for a state vector (Dirac ket notation) and $\langle\psi|$ for its transpose. For a matrix A, we write $A^\dagger$ for the conjugate transpose and $\mathsf{tr}(A)$ for the trace.

Density matrices. We write ρ^n for a density matrix of n qubits, i.e. a positive semidefinite matrix $\rho \in \mathbb{C}^{2^n \times 2^n}$ with $\mathsf{tr}(\rho) = 1$. We write $\mathcal{D}_n$ for the set of all density matrices of n-qubit systems. We use $\rho, \sigma, \tau, \gamma$ to denote density matrices in general.

Terms and variables. We use t, r, s, u for terms of the calculus. Variables are denoted x, y, z. We write $t[r/x]$ for the substitution of r for x in t, and $FV(t)$ for the set of free variables of t.

Natural Numbers. For natural numbers, we use n, m, i, j, k, l.

Types. Types are abstractly denoted with capital letters up to E, A, B, C, D. Possible specific types are n, (m, n), $A \multimap B$.

Typing contexts. Contexts are denoted with greek capital letters, Γ, Δ. We write $\Gamma \vdash t : A$ for the typing judgment that t has type A under context Γ.

Probabilities and coefficients. For general coefficients, we use c, λ, α. We use p for probabilities.

Unitary operators. We write U^m for a unitary operator of dimension $2^m \times 2^m$. When m is not needed, we write U, V, M, X, Y, Z, I.

Semantic notation. We write $[\![A]\!]$ for the semantic interpretation of a type A, and $[\![t]\!]_\theta$ for the interpretation of a term t under a valuation θ. A *valuation* θ is a map from variables to semantic values (density matrices or completely positive maps); we write $\theta \vDash \Gamma$ to mean that $\theta(x)$ belongs to the semantic domain of type A for every $x : A \in \Gamma$.

0.2 Quantum Computing

0.2.1 Density Matrices

In the standard formulation of quantum mechanics, the state of a quantum system is described by a unit vector in a Hilbert space. While this description is sufficient for pure states, it cannot describe situations where our knowledge of the system is incomplete; for example, when a measurement has been performed but we do not know its outcome. The density matrix formalism provides a more general description that encompasses both pure and mixed states. We refer to [6, Ch. 2] for a comprehensive introduction.

Definition 0.2.1 (Density matrix)**.** A *density matrix* (or density operator) is a positive semidefinite matrix ρ with $\mathsf{tr}(\rho) = 1$, where tr denotes the trace. For an n-qubit system, ρ is a $2^n \times 2^n$ matrix. We write $\mathcal{D}_n$ for the set of density matrices of n-qubit systems.

A pure state $|\psi\rangle$ corresponds to the density matrix $\rho = |\psi\rangle\langle\psi|$. A mixed state, representing a statistical ensemble where the system is in state ρ_i with probability p_i (with $\sum_i p_i = 1$), is described by $\rho = \sum_i p_i \rho_i$.

Example 0.2.2. The qubit $|0\rangle$ is represented by the density matrix $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. The balanced superposition $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is represented by $|+\rangle\langle +| = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. A fair coin toss between $|0\rangle$ and $|1\rangle$ gives the mixed state $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}I$.

The four postulates of quantum mechanics can be stated entirely in terms of density matrices [6, Ch. 2, §2.4.2].

Postulate 1 (State Space). A quantum system is completely described by a density matrix ρ, which is a positive operator with $\mathsf{tr}(\rho) = 1$, acting on the Hilbert space associated with the system. If the system is in state ρ_i with probability p_i (with $p_i \geq 0$ and $\sum_i p_i = 1$), the density matrix of the system is $\rho = \sum_i p_i \rho_i$.

Postulate 2 (Evolution). The evolution of a closed quantum system is described by a unitary operator U. If the system is in state ρ, after the evolution it will be in state

$$\rho' = U \rho U^\dagger.$$

Example 0.2.3. Some standard unitary operators on a single qubit include:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathsf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Applying the Hadamard gate H to $|0\rangle\langle 0|$ gives $\mathsf{H}|0\rangle\langle 0|\mathsf{H}^\dagger = |+\rangle\langle +|$.

Postulate 3 (Measurement). A quantum measurement is described by a collection of measurement operators $\{\pi_i\}_i$ satisfying $\sum_i \pi_i^\dagger \pi_i = I$ [6, Ch. 2, §2.2.3]. If the system is in state ρ, the probability of obtaining outcome i is

$$p_i = \mathsf{tr}(\pi_i^\dagger \pi_i \, \rho),$$

and the post-measurement state, conditioned on outcome i (defined only when $p_i > 0$), is

$$\rho_i = \frac{\pi_i \, \rho \, \pi_i^\dagger}{p_i}.$$

Example 0.2.4. Consider measuring the state $\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{\sqrt{3}}{4}|0\rangle\langle 1| + \frac{\sqrt{3}}{4}|1\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$ in the computational basis, with $\pi_0 = |0\rangle\langle 0|$ and $\pi_1 = |1\rangle\langle 1|$. The outcome probabilities are $p_0 = \mathsf{tr}(|0\rangle\langle 0| \, \rho) = \frac{3}{4}$ and $p_1 = \frac{1}{4}$, and the post-measurement states are $\rho_0 = |0\rangle\langle 0|$ and $\rho_1 = |1\rangle\langle 1|$.

Postulate 4 (Composite Systems). The state space of a composite quantum system is the tensor product of the state spaces of the component systems. If system A is in state ρ^A and system B is in state ρ^B, the joint state is $\rho^{AB} = \rho^A \otimes \rho^B$. Note that not every density matrix of a pure composite system can be written as a tensor product of its parts such states are called *entangled*.

Example 0.2.5. The Bell state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ has density matrix $\beta_{00} = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$, which cannot be written as $\rho^A \otimes \rho^B$ for any single-qubit density matrices ρ^A and ρ^B.

0.2.2 Partial Trace

When dealing with composite systems, it is often necessary to describe the state of a subsystem without reference to the rest. The *partial trace* provides this operation.

Definition 0.2.6 (Partial trace [6, Ch. 2, §2.4.3])**.** Let A and B be quantum systems. The *partial trace over* A is the unique linear map tr_A defined on product operators by

$$\mathsf{tr}_A(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |b_1\rangle\langle b_2| \, \mathsf{tr}(|a_1\rangle\langle a_2|) = \langle a_2|a_1\rangle \; |b_1\rangle\langle b_2|, \tag{0.1}$$

where $|a_i\rangle$ are vectors in the state space of A, and the same for $|b_i\rangle$. The *reduced density matrix* of subsystem B is $\rho^B = \mathsf{tr}_A(\rho^{AB})$.

On product states the partial trace acts simply as $\mathsf{tr}_A(\rho^A \otimes \rho^B) = \mathsf{tr}(\rho^A) \, \rho^B = \rho^B$. For entangled states, however, the partial trace produces a mixed state even when the global state is pure.

More generally, for a tripartite system $A \otimes B \otimes C$, the partial trace over the middle subsystem B is defined on product operators by:

$$\mathsf{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2| \otimes |c_1\rangle\langle c_2|) = \langle b_2|b_1\rangle \; |a_1\rangle\langle a_2| \otimes |c_1\rangle\langle c_2|,$$

The same principle applies to tracing out any subset of subsystems in an n-partite system: the partial trace over subsystem k acts as tr on the k-th tensor factor and as the identity on all others.

Example 0.2.7. Consider the Bell state β_{00} from the previous example. Its matrix expansion is:

$$\beta_{00} = \tfrac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|).$$

Applying Definition 0.2.6 term by term to trace out the first qubit:

$$\begin{aligned}\mathsf{tr}_1(\beta_{00}) &= \tfrac{1}{2}\big(\,\langle 0|0\rangle\ |0\rangle\langle 0| + \langle 1|0\rangle\ |0\rangle\langle 1| + \langle 0|1\rangle\ |1\rangle\langle 0| + \langle 1|1\rangle\ |1\rangle\langle 1|\big)\\ &= \tfrac{1}{2}(|0\rangle\langle 0| + 0 + 0 + |1\rangle\langle 1|) = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \tfrac{I}{2}.\end{aligned}$$

The reduced state of the second qubit is the maximally mixed state $\frac{I}{2}$, reflecting the fact that no information about the second qubit can be obtained without access to the first.

0.2.3 The No-Cloning Theorem

A fundamental consequence of the linearity of quantum mechanics is that it is impossible to create an identical copy of an arbitrary unknown quantum state.

Theorem 0.2.8 (No-cloning [6, Ch. 12, Box 12.1])**.** *There is no unitary operator U acting on two qubits such that $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$ for every state $|\psi\rangle$.*

The no-cloning theorem has profound implications for quantum computing. It means that quantum information cannot be broadcast or backed up like classical information. However, it also enables useful protocols: quantum key distribution relies on the impossibility of eavesdropping without disturbing the state, and quantum teleportation (below) provides a way to transfer quantum states without cloning them. From a programming language perspective, the no-cloning theorem motivates the use of linear or affine type systems for quantum data, as we will see in Section 0.3, as they properly codify this property.

0.2.4 The No-Deleting Theorem

A companion result to the no-cloning theorem concerns deletion. Just as quantum information cannot be duplicated, it also cannot be erased.

Theorem 0.2.9 (No-deleting [7])**.** *There is no linear map A acting on two copies of an arbitrary quantum state such that $A(|\psi\rangle \otimes |\psi\rangle) = |\psi\rangle \otimes |0\rangle$ for every state $|\psi\rangle$.*

The no-deleting theorem states that quantum information cannot be truly erased: any operation that appears to delete a qubit must, in reality, hide the information somewhere else in the universe (e.g., in the environment). The physical operation that corresponds to *ignoring* a subsystem, rather than annihilating it, is the **partial trace**, which marginalises over the discarded system while moving its information to the environment.

This distinction has direct consequences for programming languages. A language construct that "discards" a qubit must, for physical faithfulness, have a denotation in terms of partial trace, not literal deletion. In Chapter 2 we introduce a let construct whose reduction semantics provably computes the partial trace when a variable is left unused (Proposition 3.1.2), making the extended calculus faithful to the no-deleting principle.

0.2.5 Quantum Teleportation

Quantum teleportation [6, Ch. 1, §1.3.7] is a protocol that transfers a quantum state from one party (Alice) to another (Bob) using a shared entangled pair and two bits of classical communication. Crucially, the original state is destroyed in the process, consistent with the no-cloning theorem. The circuit is shown in Figure 0.1.

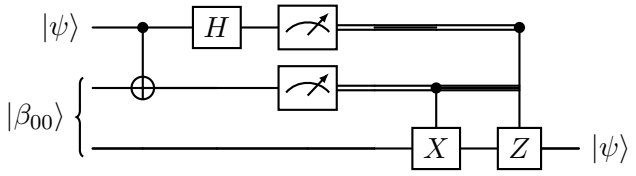

Fig. 0.1: Quantum teleportation circuit. The double lines denote classical bits transmitted from Alice to Bob, which condition the corrective X and Z gates.

Suppose Alice holds a qubit in an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and that Alice and Bob share a Bell pair $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where Alice holds the first qubit and Bob the second. The initial three-qubit state is:

$$\begin{aligned}|\psi\rangle \otimes |\beta_{00}\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \tfrac{1}{\sqrt{2}}\big(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\big).\end{aligned}$$

Step 1: CNOT. Alice applies a Cnot gate with her qubit (qubit 1) as control and her half of the Bell pair (qubit 2) as target. This flips qubit 2 when qubit 1 is $|1\rangle$:

$$\xrightarrow{\mathsf{Cnot}_{12}} \tfrac{1}{\sqrt{2}}\big(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\big).$$

Step 2: Hadamard. Alice applies a Hadamard gate on qubit 1. Since $\mathsf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $\mathsf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, each term expands as follows:

$$\begin{aligned}\alpha|000\rangle &\xrightarrow{\mathsf{H}_1} \tfrac{\alpha}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle = \tfrac{\alpha}{\sqrt{2}}(|000\rangle + |100\rangle), \\ \alpha|011\rangle &\xrightarrow{\mathsf{H}_1} \tfrac{\alpha}{\sqrt{2}}(|0\rangle + |1\rangle)|11\rangle = \tfrac{\alpha}{\sqrt{2}}(|011\rangle + |111\rangle), \\ \beta|110\rangle &\xrightarrow{\mathsf{H}_1} \tfrac{\beta}{\sqrt{2}}(|0\rangle - |1\rangle)|10\rangle = \tfrac{\beta}{\sqrt{2}}(|010\rangle - |110\rangle), \\ \beta|101\rangle &\xrightarrow{\mathsf{H}_1} \tfrac{\beta}{\sqrt{2}}(|0\rangle - |1\rangle)|01\rangle = \tfrac{\beta}{\sqrt{2}}(|001\rangle - |101\rangle).\end{aligned}$$

Including the overall $\frac{1}{\sqrt{2}}$ factor, the full state becomes:

$$\begin{aligned}&\tfrac{1}{2}\big(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle \\ &+\beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle\big).\end{aligned}$$

Step 3: Regrouping. Collecting terms by the first two qubits (Alice's measurement outcomes):

$$\tfrac{1}{2}\Big(|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\beta|0\rangle+\alpha|1\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(-\beta|0\rangle+\alpha|1\rangle)\Big). \quad (0.2)$$

Step 4: Measurement and correction. Alice measures her two qubits in the computational basis, obtaining one of four outcomes with equal probability $\frac{1}{4}$. She communicates the two-bit result to Bob, who applies the corresponding correction to recover $|\psi\rangle$:

Outcome	Bob's state	Correction	Result
00	$\alpha\|0\rangle + \beta\|1\rangle$	I	$\|\psi\rangle$
01	$\beta\|0\rangle + \alpha\|1\rangle$	X	$\|\psi\rangle$
10	$\alpha\|0\rangle - \beta\|1\rangle$	Z	$\|\psi\rangle$
11	$-\beta\|0\rangle + \alpha\|1\rangle$	ZX	$\|\psi\rangle$

After correction, Bob's qubit is in state $|\psi\rangle$, and Alice's original qubit has been destroyed by the measurement. The net effect is the transfer of the quantum state from Alice to Bob without physically moving the qubit and without violating the no-cloning theorem, since Alice no longer possesses the state.

0.3 The Lambda Calculus λ°_ρ

The calculus λ°_ρ, introduced in [2], is a quantum extension to the lambda calculus in the quantum data / classical control paradigm, where quantum data is represented by density matrices. Unlike a companion calculus λ_ρ in the same paper which uses probabilistic rewriting and classical branching, λ°_ρ uses deterministic rewriting with probabilistic control: measurements do not reduce individually but always produce a weighted sum of all possible outcomes. This makes λ°_ρ particularly interesting because state does not have to be tracked separately from the computation.

0.3.1 Grammar

The grammar of terms, shown in Table 0.1, consists of standard lambda calculus constructs, terms corresponding to the four quantum postulates, and constructions for probabilistic control.

$$
\begin{aligned}
t := {} & x \mid \lambda x.t \mid tt && \text{(Standard lambda calculus)} \\
& \mid \rho^n \mid U^n t \mid \pi^n t \mid t \otimes t && \text{(Quantum postulates)} \\
& \mid \sum_{i=1}^{n} p_i t_i \mid \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t, \ldots, t\} && \text{(Probabilistic control)}
\end{aligned}
$$

where $p_i \in (0, 1]$, $\sum_{i=1}^n p_i = 1$, and $\sum$ is considered modulo associativity and commutativity.

Tab. 0.1: Grammar of terms of λ°_ρ.

In the term ρ^n, the superscript n indicates the number of qubits. The term $U^n t$ applies a unitary gate to a quantum state; $\pi^n t$ measures it; $t \otimes t$ composes two quantum systems. The linear combination $\sum_i p_i t_i$ represents a probabilistic mixture of terms. The construct $\mathsf{letcase}^\circ$ provides branching based on measurement: it does not inspect the classical result directly but instead produces a weighted sum of all branches.

0.3.2 Rewrite System

The rewrite system, shown in Table 0.2, uses a deterministic (non-probabilistic) relation $\to$. Notably, measurement does not reduce by itself; it only reduces when it is the argument of a $\mathsf{letcase}^\circ$, producing a sum of all possible outcomes.

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

$$\mathsf{letcase}^\circ\ x = \pi^m\rho^n\ \mathsf{in}\ \{t_0,\dots,t_{2^m}-1\} \to \sum_i p_i t_i[\rho_i^n/x] \quad \text{with} \begin{cases} \rho_i^n = \frac{\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger}{p_i} \\ p_i = \mathsf{tr}(\overline{\pi_i}^\dagger\overline{\pi_i}\rho^n) \end{cases}$$

$$U^m\rho^n \to \rho'^n \qquad \text{with } \overline{U^m}\rho^n\overline{U^m}^\dagger = \rho'^n$$

$$\rho\otimes\rho' \to \rho'' \qquad \text{with } \rho'' = \rho\otimes\rho'$$

$$\sum_i p_i\rho_i \to \rho' \qquad \text{with } \rho' = \sum_i p_i\rho_i$$

$$\sum_i p_i t \to t$$

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

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

$$\frac{t\to r}{\lambda x.t\to\lambda x.r} \qquad \frac{t\to r}{\pi^n t\to\pi^n r} \qquad \frac{t\to r}{t\otimes s\to r\otimes s} \qquad \frac{t\to r}{s\otimes t\to s\otimes r}$$

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

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

Tab. 0.2: Rewrite system of λ°_ρ.

0.3.3 Type System

The type system, given in Table 0.3, is affine: variables can be used at most once, preventing the duplication of quantum states (respecting the no-cloning theorem [6, Ch. 12, Box 12.1]). In rules that combine two contexts Γ and Δ (namely $\multimap_e$ and $\otimes$), the two contexts are required to be *disjoint* (no shared variable), which is what enforces linearity.

The type n denotes the type of an n-qubit density matrix, the type (m,n) denotes the result of measuring m out of n qubits (carrying both the classical outcome and the quantum state), and $A\multimap B$ is the linear function type.

0.3.4 Example: Quantum Teleportation in λ°_ρ

The quantum teleportation algorithm (Section 0.2.5) can be expressed in λ°_ρ as follows. Let $\beta_{00} = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$ be a Bell state. The teleportation term is:

$$T = \lambda x.\,\mathsf{letcase}^\circ\ y = \pi^2(\mathsf{H}^1(\mathsf{Cnot}^2(x\otimes\beta_{00})))\ \mathsf{in}\ \{y,\ \mathsf{Z}_3 y,\ \mathsf{X}_3 y,\ \mathsf{Z}_3\mathsf{X}_3 y\}$$

where $\mathsf{Z}_3 = I\otimes I\otimes\mathsf{Z}^1$ and $\mathsf{X}_3 = I\otimes I\otimes\mathsf{X}^1$.

Given an input state ρ, the reduction proceeds by first composing ρ with the Bell pair, applying the CNOT and Hadamard gates, and then the $\mathsf{letcase}^\circ$ produces a sum over all four measurement outcomes.

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

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

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

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

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

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

Tab. 0.3: Type system for λ°_ρ.

0.4 Pauli Decomposition of Density Matrices

The extension we introduce in this thesis relies on the fact that any density matrix can be decomposed as a linear combination of Pauli operators. We present here the decomposition itself; properties of the Pauli basis are proved in [5].

0.4.1 The Pauli Matrices

The Pauli matrices, together with the identity, form a basis for the space of 2×2 Hermitian matrices [6, Ch. 2, §2.1.3]:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definition 0.4.1 (Pauli operator basis)**.** Let $n \in \mathbb{N}^*$. The Pauli operator basis of size n is the set

$$\mathcal{P}_n = \left\{ \bigotimes_{i=1}^n M_i \;\middle|\; M_i \in \{I, X, Y, Z\} \right\}.$$

The set $\mathcal{P}_n$ contains 4^n elements and forms an orthogonal basis of $\mathbb{C}^{2^n \times 2^n}$ with respect to the Hilbert–Schmidt inner product $\langle A, B \rangle = \mathsf{tr}(A^\dagger B)$ [5, Theorem 1].

0.4.2 Pauli Decomposition of a Density Matrix

Since $\mathcal{P}_n$ is a basis, any density matrix ρ^n can be written as:

$$\rho^n = \sum_{P_i \in \mathcal{P}_n} \alpha_i P_i, \quad \text{with } \alpha_i \in \mathbb{R}. \tag{0.3}$$

The coefficients α_i are real because ρ is Hermitian and each Pauli matrix is also Hermitian [5, Theorem 2]. They can be computed as:

$$\alpha_{M_1 \dots M_n} = \frac{1}{2^n} \mathsf{tr}\left(\left(\bigotimes_i M_i \right) \rho \right). \tag{0.4}$$

Example 0.4.2 (Pauli decomposition of the Bell state)**.** Consider the Bell state density matrix $\beta_{00} = |\beta_{00}\rangle\langle\beta_{00}|$ with $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Since $n = 2$, the Pauli basis $\mathcal{P}_2$ has $4^2 = 16$ elements $M_1 \otimes M_2$ with $M_1, M_2 \in \{I, X, Y, Z\}$. We compute all sixteen coefficients $\alpha_{M_1 M_2} = \frac{1}{4}\mathsf{tr}\big((M_1 \otimes M_2)\,\beta_{00}\big)$.

Since β_{00} is a pure state, $\mathsf{tr}(A\beta_{00}) = \langle\beta_{00}|\,A\,|\beta_{00}\rangle$[1], so:

$$\mathsf{tr}\big((M_1 \otimes M_2)\,\beta_{00}\big) = \langle\beta_{00}|\,(M_1 \otimes M_2)\,|\beta_{00}\rangle\,.$$

By linearity of the tensor product:

$$(M_1 \otimes M_2)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}\big(M_1\,|0\rangle \otimes M_2\,|0\rangle + M_1\,|1\rangle \otimes M_2\,|1\rangle\,\big).$$

Computing $(M_1 \otimes M_2)\,|\beta_{00}\rangle$ and then the inner product with $\langle\beta_{00}|$ for each of the sixteen pairs (the full computations are given in Appendix A.1), we obtain:

$$\alpha_{II} = \tfrac{1}{4}, \quad \alpha_{XX} = \tfrac{1}{4}, \quad \alpha_{YY} = -\tfrac{1}{4}, \quad \alpha_{ZZ} = \tfrac{1}{4}, \tag{0.5}$$

with all other twelve coefficients equal to zero. The Pauli decomposition is:

$$\beta_{00} = \tfrac{1}{4}(I \otimes I + X \otimes X - Y \otimes Y + Z \otimes Z). \tag{0.6}$$

0.5 Spectral Decomposition

The spectral decomposition theorem is a fundamental result in linear algebra that will be used in Chapter 2 to decompose the Pauli operators into sums of tensor products of valid 1-qubit density matrices.

Theorem 0.5.1 (Spectral decomposition)**.** *Let A be a normal matrix (i.e. $AA^\dagger = A^\dagger A$) of dimension $d \times d$. Then A can be written as*

$$A = \sum_{i=1}^{d} \lambda_i |v_i\rangle\langle v_i|,$$

where $\lambda_1, \ldots, \lambda_d$ are the eigenvalues of A (counted with multiplicity) and $|v_1\rangle, \ldots, |v_d\rangle$ form an orthonormal basis of eigenvectors.

For a proof, see [6, Ch. 2, Theorem 2.1].

In the particular case of Hermitian matrices, the eigenvalues are real.

[1] $\mathsf{tr}(A\beta_{00}) = \mathsf{tr}(A|\beta_{00}\rangle\langle\beta_{00}|) = \sum_k \langle e_k|\,A\,|\beta_{00}\rangle\langle\beta_{00}|e_k\rangle = \langle\beta_{00}|\big(\sum_k |e_k\rangle\langle e_k|\big)A\,|\beta_{00}\rangle = \langle\beta_{00}|\,A\,|\beta_{00}\rangle$.

1. INTRODUCTION

1.1 Motivation

The λ_ρ° calculus introduced in [2] has the advantage over other related calculi (like [8]) of having the computation state embedded as part of the terms, instead of using registries and tracking it separately. Reasoning on this type of calculus is closer to being representative of the operations of a quantum circuit, which makes it specially interesting for proving properties.

One issue with this calculus is that it lacked a tensor product elimination, which would allow programs to be written in a more composable manner. It is important to note that this does not affect the *expressiveness* of the calculus: any quantum computation can still be expressed by encoding operations directly at the matrix level. However, the absence of such a mechanism affects the *compositionality* of programs written in the calculus.

Consider a concrete scenario: given a 2-qubit state ρ^2, suppose we want to apply a function f to the first qubit and a function g to the second qubit independently. In λ_ρ°, there is no way to express this as $f(x_1)$ and $g(x_2)$ where x_1 and x_2 are the individual qubits of ρ^2. One must instead encode the operation at the matrix level, using operators like $U_f \otimes U_g$ applied to the whole state, losing the modularity that lambda calculi are designed to provide.

Another thing we noticed, was that the semantic interpretation (being informed by the one needed for λ_ρ) was overly complicated, which made it harder to extend and build proofs on top of this calculus.

Lastly, the original calculus lacked a mechanism for discarding qubits, which meant that some quantum programs could not be encoded with it. This was proven in [1].

A further concern (relating to the last point) is physical faithfulness with respect to the no-deleting theorem (Section 0.2.4). The no-deleting theorem states that quantum information cannot be truly erased; the physical operation corresponding to discarding a subsystem is the partial trace over it, which moves information to the environment rather than annihilating it. A compositional let construct whose denotation coincides with partial trace whenever a variable is unused would therefore be not only convenient but physically principled.

1.2 Contributions

In this thesis, we make the following contributions:

1. **A compositional let construct.** We extend the calculus λ_ρ° with a construct

$$\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ t$$

that binds the variables $x_1, \ldots, x_n$ to the individual qubit components of ρ^n within the body t. The decomposition is achieved through the Pauli decomposition and the spectral decomposition of the Pauli matrices: the state ρ^n is expressed as a weighted sum of tensor products of single-qubit density matrices, and the body t is evaluated for each such decomposition, weighted accordingly.

2. **A simplified semantic interpretation.** We provide a new semantic interpretation of λ°_ρ that is simpler than the one in [2]. The original interpretation carries tuples (p_i, b_i, e_i) that track measurement outcomes. Since $\mathsf{letcase}^\circ$ always sums over all measurement branches without inspecting the classical result, this bookkeeping is unnecessary. Our simplified interpretation drops this overhead, interpreting terms directly as density matrices and completely positive maps.

3. **Properties.** We prove that the fundamental properties of Subject Reduction, Progress, Strong Normalisation, Soundness and Adequacy are true for the extended calculus.

   We also note that a linear combination of measurement values $\sum_j q_j w_j$ with each $w_j : (m, n)$ is a well-typed closed value of type (m, n); for Progress we include the distributing rule $\mathsf{letcase}^\circ\ x = \sum_j q_j w_j\ \mathsf{in}\ \{t_0, \dots\} \to \sum_j q_j \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{t_0, \dots\}$.

   We also show a central result of this extension, *Discard as Partial Trace* (Proposition 3.1.2): whenever a variable x_k is not free in the body of a let, the construct reduces exactly as if the partial trace over qubit k had been taken first. This establishes that the let construct is faithful to the no-deleting theorem (Theorem 0.2.9): discarded qubits are not annihilated but marginalised, in accordance with quantum mechanics.

4. **Illustrative examples.** We show an example that illustrates how the let codifies the partial tracing of qubits when used to discard unneeded qubits. We also rework the quantum teleportation protocol from the original paper and present the three-qubit bit-flip error correction code. Both examples demonstrate how the let construct enables compositional programming over multi-qubit states, including clean separation of roles (in teleportation) and ancilla management (in error correction).

1.3 Outline

This thesis is organized as follows.

Chapter 0 (already presented) provides the theoretical background: quantum computing with density matrices (including the no-cloning and no-deleting theorems), the calculus λ°_ρ, the Pauli decomposition, and the spectral decomposition theorem.

Chapter 1 is this introduction.

Chapter 2 presents the core contribution: the extended calculus with the let construct, including its grammar, rewrite system, type system, and semantic interpretation (both the simplified interpretation of λ°_ρ and its extension). We also present examples demonstrating the partial tracing of qubits and the compositionality enabled by the extension: quantum teleportation with an Alice/Bob decomposition and the three-qubit bit-flip error correction code.

Chapter 3 states and proves Subject Reduction, Progress, Strong Normalisation, and Soundness for the extended calculus, and establishes Adequacy.

Appendix A expands on the algebra required for the examples related to the Bell state.

Appendix B collects the complete definition of the extended calculus (grammar, rewrite rules, type system, and denotational semantics) in one place for easy reference.

Appendix C shows the explicit spectral decompositions of the four Pauli matrices.

Appendix D contains the full detailed proofs of Chapter 3.

2. THE COMPOSITIONAL EXTENSION

In this chapter we present the core contributions of this thesis. We first develop the Pauli spectral decomposition machinery needed for the new construct, then present the extended calculus, and finally provide a simplified semantic interpretation. For a compact self-contained summary, Appendix B collects the complete definition of the extended calculus—grammar, rewrite rules, type system, and denotational semantics—in one place.

2.1 Spectral Decomposition of the Pauli Matrices

By the spectral decomposition theorem (Theorem 0.5.1), each Pauli matrix can be written as a linear combination of its eigenprojectors. Since each Pauli matrix has eigenvalues ± 1 (except for I, which has eigenvalue 1 with multiplicity 2), we can write:

$$\begin{aligned} I &= 1 \cdot |0\rangle\langle 0| \;\; + 1 \cdot |1\rangle\langle 1| \\ Z &= 1 \cdot |0\rangle\langle 0| \;\; - 1 \cdot |1\rangle\langle 1| \\ X &= 1 \cdot |+\rangle\langle +| - 1 \cdot |-\rangle\langle -| \\ Y &= 1 \cdot |i\rangle\langle i| \;\; - 1 \cdot |-i\rangle\langle -i| \end{aligned}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)$. The full derivations are given in Appendix C.

More abstractly, each Pauli matrix M_k admits a decomposition:

$$M_k = \lambda_k^1 \gamma_k^1 + \lambda_k^2 \gamma_k^2,$$

where each γ_k^l is a valid single-qubit density matrix (a rank-1 projector) and $\lambda_k^l \in \{-1, +1\}$ are the eigenvalues.

2.2 Combined Decomposition

We now combine the Pauli decomposition (0.3) with the spectral decomposition to express any ρ^n as a weighted sum of tensor products of single-qubit density matrices.

Consider an element $P_i = M_{i_1} \otimes \cdots \otimes M_{i_n}$ of the Pauli basis. Expanding each factor via its spectral decomposition and distributing:

$$\begin{aligned} P_i &= (\lambda_{i_1}^1 \gamma_{i_1}^1 + \lambda_{i_1}^2 \gamma_{i_1}^2) \otimes \cdots \otimes (\lambda_{i_n}^1 \gamma_{i_n}^1 + \lambda_{i_n}^2 \gamma_{i_n}^2) \\ &= \sum_{l_1,\ldots,l_n \in \{1,2\}} \left(\prod_{k=1}^{n} \lambda_{i_k}^{l_k} \right) \bigotimes_{k=1}^{n} \gamma_{i_k}^{l_k}. \end{aligned}$$

Substituting into the Pauli decomposition of ρ^n:

$$\rho^n = \sum_{i=1}^{4^n} \alpha_i \sum_{l_1,\ldots,l_n \in \{1,2\}} \left(\prod_{k=1}^{n} \lambda_{i_k}^{l_k} \right) \bigotimes_{k=1}^{n} \gamma_{i_k}^{l_k}$$

$$= \sum_{i=1}^{4^n} \sum_{\vec{l} \in \{1,2\}^n} p_{i\vec{l}} \bigotimes_{k=1}^{n} \gamma_{i_k}^{l_k}, \tag{2.1}$$

where $p_{i\vec{l}} = \alpha_i \prod_{k=1}^{n} \lambda_{i_k}^{l_k}$.

Remark 2.2.1. The coefficients $p_{i\vec{l}}$ are not necessarily non-negative, so this is not a convex combination in general. However, since $\mathsf{tr}(\rho^n) = 1$, the total sum of coefficients satisfies $\sum_{i,\vec{l}} p_{i\vec{l}} = 1$. The individual terms $\bigotimes_k \gamma_{i_k}^{l_k}$ are genuine density matrices (tensor products of single-qubit density matrices), this is possible for unseparable states, as the interference on entangled qubits gets codified as negative terms on the sum.

This decomposition is the key mathematical tool that enables our let construct: it provides a canonical way to decompose any multi-qubit state into components that can be individually addressed within a program.

Example 2.2.2 (Combined decomposition of the Bell state)**.** We continue from Example 0.4.2 and apply the combined decomposition (2.1) to β_{00}. Each Pauli factor is expanded via its spectral decomposition (Appendix C):

$$\begin{aligned} I &= (+1)|0\rangle\langle 0| \ + (+1)|1\rangle\langle 1|, & Z &= (+1)|0\rangle\langle 0| + (-1)|1\rangle\langle 1|, \\ X &= (+1)|+\rangle\langle +| + (-1)|-\rangle\langle -|, & Y &= (+1)|i\rangle\langle i| \ + (-1)|-i\rangle\langle -i|. \end{aligned}$$

Since only the four pairs II, XX, YY, ZZ carry nonzero α_i (0.5), the sum $\beta_{00} = \sum_i \sum_{\vec{l} \in \{1,2\}^2} p_{i\vec{l}} \gamma_{i_1}^{l_1} \otimes \gamma_{i_2}^{l_2}$ has $4 \times 4 = 16$ nonzero terms, where $p_{i\vec{l}} = \alpha_i \cdot \lambda_{i_1}^{l_1} \cdot \lambda_{i_2}^{l_2}$. Expanding each term (see Appendix A.2 for the detailed computation), the full combined decomposition is:

$$\begin{aligned} \beta_{00} = \ & \tfrac{1}{4}\,|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \tfrac{1}{4}\,|0\rangle\langle 0| \otimes |1\rangle\langle 1| + \tfrac{1}{4}\,|1\rangle\langle 1| \otimes |0\rangle\langle 0| + \tfrac{1}{4}\,|1\rangle\langle 1| \otimes |1\rangle\langle 1| \\ & + \tfrac{1}{4}\,|+\rangle\langle +| \otimes |+\rangle\langle +| - \tfrac{1}{4}\,|+\rangle\langle +| \otimes |-\rangle\langle -| - \tfrac{1}{4}\,|-\rangle\langle -| \otimes |+\rangle\langle +| + \tfrac{1}{4}\,|-\rangle\langle -| \otimes |-\rangle\langle -| \\ & - \tfrac{1}{4}\,|i\rangle\langle i| \otimes |i\rangle\langle i| + \tfrac{1}{4}\,|i\rangle\langle i| \otimes |-i\rangle\langle -i| + \tfrac{1}{4}\,|-i\rangle\langle -i| \otimes |i\rangle\langle i| - \tfrac{1}{4}\,|-i\rangle\langle -i| \otimes |-i\rangle\langle -i| \\ & + \tfrac{1}{4}\,|0\rangle\langle 0| \otimes |0\rangle\langle 0| - \tfrac{1}{4}\,|0\rangle\langle 0| \otimes |1\rangle\langle 1| - \tfrac{1}{4}\,|1\rangle\langle 1| \otimes |0\rangle\langle 0| + \tfrac{1}{4}\,|1\rangle\langle 1| \otimes |1\rangle\langle 1| \end{aligned} \tag{2.2}$$

This is a signed sum of tensor products of single-qubit density matrices. The presence of negative coefficients reflects the entanglement of β_{00} (cf. the remark above).

2.3 Extended Grammar

We extend the grammar of λ_ρ° (Table 0.1) with a single new construct:

The new construct $\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ t$ binds n variables $x_1, \ldots, x_n$, each of type 1 (single-qubit density matrix), within the body t. The superscript $\otimes n$ in $x^{\otimes n}$ indicates that x is being decomposed into n tensor components.

2.4 Extended Rewrite System

The rewrite rules for the existing constructs of λ_ρ° remain unchanged (Table 0.2), with two modifications. First, $\dfrac{t \to r}{\lambda x.t \to \lambda x.r}$ is removed, as it is not needed for expressiveness and removing it simplifies the definition of values for closed terms. Second, we add a distributing rule for $\mathsf{letcase}^\circ$ over linear combinations (analogous to $(\sum_i p_i t_i)\, r \to \sum_i p_i (t_i r)$):

$$
\begin{aligned}
t := {} & x \mid \lambda x.t \mid tt && \text{(Standard lambda calculus)} \\
& \mid \rho^n \mid U^n t \mid \pi^n t \mid t \otimes t && \text{(Quantum postulates)} \\
& \mid \sum_{i=1}^{n} p_i t_i \mid \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t, \ldots, t\} && \text{(Probabilistic control)} \\
& \mid \mathsf{let}\ x^{\otimes n} = \rho\ \mathsf{in}\ t && \text{(Compositional decomposition)}
\end{aligned}
$$

Tab. 2.1: Extended grammar of terms.

$$
\mathsf{letcase}^\circ\ x = \sum_j q_j w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \to \sum_j q_j\, \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}
$$

This rule is needed for Progress: a linear combination $\sum_j q_j w_j$ of measurement values $w_j = \pi^m \rho_j^n$ is a closed value of type (m, n), but the $\mathsf{letcase}^\circ$ main rule only fires on a single $\pi^m \rho^n$. We include this rule in our presentation for completeness. In Table 2.2 we add the new reduction rules for the let construct and its contextual closures.

$$
\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s \to \sum_{i=1}^{4^n} \sum_{\vec{l} \in \{1,2\}^n} p_{i\vec{l}}\, s[\gamma_{i_1}^{l_1}/x_1, \cdots, \gamma_{i_n}^{l_n}/x_n]
$$

where $p_{i\vec{l}}$ and $\gamma_{i_k}^{l_k}$ are given by the combined decomposition of ρ^n (equation 2.1).

$$
\frac{t \to r}{\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s \to \mathsf{let}\ x^{\otimes n} = r\ \mathsf{in}\ s} \qquad \frac{t \to r}{\mathsf{let}\ x^{\otimes n} = s\ \mathsf{in}\ t \to \mathsf{let}\ x^{\otimes n} = s\ \mathsf{in}\ r}
$$

Tab. 2.2: Rewrite rules for the let construct.

The reduction works as follows: when the first argument is a concrete density matrix ρ^n, the combined decomposition (Section 2.2) is applied. Each term $\bigotimes_k \gamma_{i_k}^{l_k}$ assigns a single-qubit density matrix to each position k. The body s is then evaluated with each such assignment, and the results are combined with the weights $p_{i\vec{l}}$. The two contextual rules allow reduction to proceed within either the source term or the body.

2.5 Extended Type System

The type system is extended with a single new rule:

$$
\frac{\Gamma \vdash t : n \quad \Delta, x_1 : 1, \ldots, x_n : 1 \vdash s : A}{\Gamma, \Delta \vdash \mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s : A}\ \mathsf{let}
$$

Tab. 2.3: Typing rule for the let construct.

The rule requires that t has type n (an n-qubit density matrix), and the body s is typed in a context extended with n variables, each of type 1. The contexts Γ and Δ are split, maintaining the affine discipline.

2.6 Simplified Interpretation of λ°_ρ

In the original presentation of λ°_ρ [2], the semantic interpretation carries tuples (p_i, b_i, e_i) where b_i tracks measurement outcomes. However, since $\mathsf{letcase}^\circ$ always sums over all measurement branches without inspecting the classical result, this bookkeeping is unnecessary. We present here a simplified interpretation that drops this overhead.

2.6.1 Semantic Domains

Recall that a *completely positive map* (CPM) is a linear map between spaces of operators that is positive (maps positive operators to positive operators). CPMs are the standard model for physically realisable quantum operations [6, Ch. 8]. We write $\mathsf{CPM}(\mathcal{D}, \mathcal{D}')$ for the set of CPMs from $\mathcal{D}$ to $\mathcal{D}'$.

Types are interpreted as follows:

$$\begin{aligned}
[\![n]\!] &= \mathcal{D}_n && \text{(density matrices on } \mathbb{C}^{2^n}\text{)}\\
[\![(m,n)]\!] &= \mathcal{D}_n && \text{(measurement type, same domain)}\\
[\![A \multimap B]\!] &= \mathsf{CPM}([\![A]\!], [\![B]\!]) && \text{(completely positive maps)}
\end{aligned}$$

2.6.2 Interpretation of Terms

The interpretation is always understood relative to a typing judgment $\Gamma \vdash t : A$ and a valuation $\theta \vDash \Gamma$, i.e. $\theta(x) \in [\![A]\!]$ for every $x : A \in \Gamma$. Given such θ, the interpretation of λ°_ρ terms is:

$$\begin{aligned}
[\![x]\!]_\theta &= \theta(x)\\
[\![\lambda x.t]\!]_\theta &= \rho \mapsto [\![t]\!]_{\theta, x\mapsto\rho}\\
[\![t\ r]\!]_\theta &= [\![t]\!]_\theta([\![r]\!]_\theta)\\
[\![\rho^n]\!]_\theta &= \rho^n\\
[\![U^m t]\!]_\theta &= \overline{U^m}\,[\![t]\!]_\theta\,\overline{U^m}^\dagger\\
[\![t \otimes r]\!]_\theta &= [\![t]\!]_\theta \otimes [\![r]\!]_\theta\\
[\![\pi^m t]\!]_\theta &= \sum_{i=0}^{2^m-1} \overline{\pi_i}\,[\![t]\!]_\theta\,\overline{\pi_i}^\dagger\\
[\![\sum_i p_i t_i]\!]_\theta &= \sum_i p_i\,[\![t_i]\!]_\theta
\end{aligned}$$

For $\mathsf{letcase}^\circ$, let $p_i = \mathsf{tr}(\overline{\pi_i}^\dagger \overline{\pi_i}\,[\![r]\!]_\theta)$ and $\rho_i = \frac{\overline{\pi_i}\,[\![r]\!]_\theta\,\overline{\pi_i}^\dagger}{p_i}$. Then:

$$[\![\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}]\!]_\theta = \sum_{i=0}^{2^m-1} p_i \cdot [\![t_i]\!]_{\theta, x\mapsto\rho_i}.$$

2.6.3 Interpretation of the Let Construct

For the new let construct, let $\mathcal{P}_n = \{P_i\}_{i=1}^{4^n}$ be the n-qubit Pauli basis (Definition 0.4.1), and for each $P_i = M_{i_1} \otimes \cdots \otimes M_{i_n}$, let $\gamma^l_{i_k}$ denote the eigenprojectors of M_{i_k} with eigenvalues

$\lambda_{i_k}^{l}$ for $l \in \{1,2\}$. Define:

$$\alpha_i(\rho) = \frac{1}{2^n}\mathsf{tr}(P_i \cdot \rho).$$

The interpretation is:

$$\begin{aligned}&[\![\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s]\!]_\theta \\ &= \sum_{i=1}^{4^n} \sum_{\vec{l}\in\{1,2\}^n} \left(\alpha_i([\![t]\!]_\theta) \prod_{k=1}^{n} \lambda_{i_k}^{l_k}\right) [\![s]\!]_{\theta, x_1 \mapsto \gamma_{i_1}^{l_1}, \ldots, x_n \mapsto \gamma_{i_n}^{l_n}}.\end{aligned}$$

2.7 Examples

We now show the full reduction of what essentially codifies tracing out the first qubit of the Bell state with the new construct, revisit the teleportation example from [2] and show a new example of another quantum algorithm.

2.7.1 Partial Trace of the Bell State

For this example, we will reduce the term $\mathsf{let}\ x^{\otimes 2} = \beta_{00}\ \mathsf{in}\ x_2$. Since $x_1 \notin FV(x_2)$, the first qubit variable is discarded by the affine type system. We would then expect the resulting density matrix to represent the partial trace $\mathsf{tr}_1(\beta_{00})$.

The combined decomposition of β_{00} was computed in Example 2.2.2 (equation 2.2). Applying the let reduction rule (Table 2.2):

$$\begin{aligned}&\mathsf{let}\ x^{\otimes 2} = \beta_{00}\ \mathsf{in}\ x_2 \\ &\to \sum_{i=1}^{16} \sum_{\vec{l}\in\{1,2\}^2} p_{i\vec{l}}\, x_2[\gamma_{i_1}^{l_1}/x_1, \gamma_{i_2}^{l_2}/x_2]\end{aligned}$$

Since $x_1 \notin FV(x_2)$, the substitution $\gamma_{i_1}^{l_1}/x_1$ is vacuous in every term, and $x_2[\gamma_{i_2}^{l_2}/x_2] = \gamma_{i_2}^{l_2}$. Only four Pauli indices carry nonzero α_i (0.5), giving 16 terms. Reading them from (2.2) and keeping only the second tensor factor, the terms from $X\otimes X$, $Y\otimes Y$, and $Z\otimes Z$ cancel pairwise; only $I\otimes I$ contributes (see Appendix A.3 for the full expansion and coefficient collection). After sum-collapse:

$$\to \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| \to \tfrac{I}{2}.$$

This coincides with the partial trace $\mathsf{tr}_1(\beta_{00}) = \frac{I}{2}$ (Example 0.2.7).

Remark 2.7.1. This example illustrates that the let construct is faithful to the no-deleting theorem (Theorem 0.2.9): the first qubit of β_{00} is not annihilated when x_1 is discarded, but instead marginalised (its contribution sums out exactly as a partial trace). This operational coincidence is not a coincidence of the example but a provable property of the calculus; see Proposition 3.1.2 in Chapter 3.

2.7.2 Teleportation as Alice and Bob

Recall the teleportation term from Section 0.3.4:

$$T = \lambda x.\, \mathsf{letcase}^{\circ}\ y = \pi^2(\mathsf{H}^1(\mathsf{Cnot}^2(x \otimes \beta_{00})))\ \mathsf{in}\ \{y,\ \mathsf{Z}_3 y,\ \mathsf{X}_3 y,\ \mathsf{Z}_3\mathsf{X}_3 y\}$$

The correction operators $\mathsf{Z}_3 = I \otimes I \otimes \mathsf{Z}$ and $\mathsf{X}_3 = I \otimes I \otimes \mathsf{X}$ operate on the global 3-qubit state. This formulation conflates Alice's and Bob's roles: Alice prepares and measures, while Bob corrects, yet the term treats the entire protocol as a monolithic operation. Moreover, the type of T is $1 \multimap 3$, since the branches return the full 3-qubit post-measurement state, even though the teleported qubit is only the third one.

Using the let construct, we can cleanly separate the two roles. The key observation is that since the type system is affine (variables may be used at most once), Bob can bind all three qubit variables via let but only use q_3, his qubit, discarding Alice's qubits q_1 and q_2.

Alice. Alice takes the input qubit, composes it with her half of the Bell pair, applies the CNOT and Hadamard gates, and measures her two qubits:

$$\mathit{alice} = \lambda x.\, \pi^2(\mathsf{H}^1(\mathsf{Cnot}^2(x \otimes \beta_{00})))$$

Bob. Bob receives the measurement result and, in each branch, uses let to decompose the 3-qubit post-measurement state. He applies the appropriate Pauli correction to his qubit q_3 and returns only that qubit:

$$\begin{aligned}\mathit{bob} = \lambda m.\, \mathsf{letcase}^\circ\ y = m\ \mathsf{in}\ \{&\mathsf{let}\ q^{\otimes n} = y\ \mathsf{in}\ q_3,\ \mathsf{let}\ q^{\otimes n} = y\ \mathsf{in}\ \mathsf{Z}^1 q_3,\\ &\mathsf{let}\ q^{\otimes n} = y\ \mathsf{in}\ \mathsf{X}^1 q_3,\ \mathsf{let}\ q^{\otimes n} = y\ \mathsf{in}\ \mathsf{Z}^1(\mathsf{X}^1 q_3)\}\end{aligned}$$

Teleportation. The full teleportation protocol is their composition:

$$\mathit{teleport} = \lambda x.\, \mathit{bob}(\mathit{alice}\ x)$$

The type of *teleport* is $1 \multimap 1$: it takes a single-qubit density matrix and returns a single-qubit density matrix. This type accurately reflects the physical protocol, where Alice's qubits are consumed by the measurement and only Bob's corrected qubit remains.

Type Derivation

We now derive the types of *alice*, *bob*, and *teleport*.

Typing alice.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x{:}1 \vdash x : 1}\,\mathsf{ax} \quad \dfrac{}{\vdash \beta_{00} : 2}\,\mathsf{ax}_\rho}{x{:}1 \vdash x \otimes \beta_{00} : 1{+}2}\,\otimes}{x{:}1 \vdash \mathsf{Cnot}^2(x \otimes \beta_{00}) : 3}\,\mathsf{u}}{x{:}1 \vdash \mathsf{H}^1(\mathsf{Cnot}^2(x \otimes \beta_{00})) : 3}\,\mathsf{u}}{x{:}1 \vdash \pi^2(\mathsf{H}^1(\mathsf{Cnot}^2(x \otimes \beta_{00}))) : (2,3)}\,\mathsf{m}}{\vdash \mathit{alice} : 1 \multimap (2,3)}\,\multimap_i$$

Typing a branch of bob. We show the derivation for the second branch (Z^1 correction); the others are analogous. We write Γ_q for $q_1{:}1, q_2{:}1, q_3{:}1$.

$$\dfrac{\dfrac{}{y{:}3 \vdash y : 3}\,\mathsf{ax} \quad \dfrac{\dfrac{}{\Gamma_q \vdash q_3 : 1}\,\mathsf{ax}}{\Gamma_q \vdash \mathsf{Z}^1 q_3 : 1}\,\mathsf{u}}{y{:}3 \vdash \mathsf{let}\ q^{\otimes n} = y\ \mathsf{in}\ \mathsf{Z}^1 q_3 : 1}\,\mathsf{let}$$

Note that q_1 and q_2 appear in the context but are not used in $\mathsf{Z}^1 q_3$. This is permitted by the affine type system (the ax rule allows extra variables in the context via weakening).

Typing bob. Let $t_0 = \mathsf{let}\ q^{\otimes n} = y\ \mathsf{in}\ q_3$, $t_1 = \mathsf{let}\ q^{\otimes n} = y\ \mathsf{in}\ \mathsf{Z}^1 q_3$, $t_2 = \mathsf{let}\ q^{\otimes n} = y\ \mathsf{in}\ \mathsf{X}^1 q_3$, $t_3 = \mathsf{let}\ q^{\otimes n} = y\ \mathsf{in}\ \mathsf{Z}^1(\mathsf{X}^1 q_3)$. Each branch satisfies $y : 3 \vdash t_i : 1$ as shown above. Then:

$$\dfrac{\dfrac{y{:}3 \vdash t_0{:}1 \quad y{:}3 \vdash t_1{:}1 \quad y{:}3 \vdash t_2{:}1 \quad y{:}3 \vdash t_3{:}1 \quad \overline{m{:}(2,3) \vdash m{:}(2,3)}\ \mathsf{ax}}{m{:}(2,3) \vdash \mathsf{letcase}^{\circ}\ y = m\ \mathsf{in}\ \{t_0, t_1, t_2, t_3\} : 1}\ \mathsf{lc}}{\vdash bob : (2,3) \multimap 1}\ \multimap_i$$

Typing teleport.

$$\dfrac{\dfrac{\vdots}{\vdash bob : (2,3) \multimap 1} \qquad \dfrac{\dfrac{\vdots}{\vdash alice : 1 \multimap (2,3)} \qquad \dfrac{}{x : 1 \vdash x : 1}\ \mathsf{ax}}{x : 1 \vdash alice\ x : (2,3)}\ \multimap_e}{x : 1 \vdash bob(alice\ x) : 1}\ \multimap_e$$
$$\vdash teleport : 1 \multimap 1\ \multimap_i$$

The resulting type $1 \multimap 1$ confirms that teleportation is a function from a single-qubit state to a single-qubit state, as expected from the physical protocol.

2.7.3 Bit-Flip Error Correction

The three-qubit bit-flip code [6, Ch. 10, §10.1.1] is the simplest quantum error-correcting code. It protects a single logical qubit against a single bit-flip (X) error by encoding it into three physical qubits. This example illustrates how the let construct enables clean ancilla management and qubit extraction, resulting in substantially better types compared to the original calculus.

The Protocol

Encoding. The encoding maps a single-qubit state to a three-qubit codeword using two CNOT gates:

$$\alpha\,|0\rangle + \beta\,|1\rangle \;\longmapsto\; \alpha\,|000\rangle + \beta\,|111\rangle\,.$$

Define the encoding unitary $\mathrm{Enc}^3 = \mathrm{CNOT}^3_{13} \cdot \mathrm{CNOT}^3_{12}$, where CNOT^3_{1k} denotes the three-qubit CNOT gate with control on qubit 1 and target on qubit k.

Error model. A bit-flip error on qubit $k \in \{1, 2, 3\}$ is modeled by applying X^3_k (Pauli X on position k, identity elsewhere) to the encoded state.

Syndrome extraction. Two ancilla qubits (initialized to $|00\rangle\langle 00|$) are prepended to the code qubits, forming a five-qubit system. A syndrome extraction circuit Synd^5 uses CNOT gates to transfer parity information from the code qubits (positions 3, 4, 5) to the ancillas (positions 1, 2). The resulting ancilla state reveals which qubit was flipped:

Ancilla state	Error
$\|00\rangle$	No error
$\|10\rangle$	Bit flip on code qubit 1 (position 3)
$\|11\rangle$	Bit flip on code qubit 2 (position 4)
$\|01\rangle$	Bit flip on code qubit 3 (position 5)

Measuring the ancillas with π^2 extracts the syndrome.

Correction and decoding. Based on the syndrome outcome, a Pauli X gate is applied to the affected code qubit to undo the error. The corrected codeword is then decoded by applying $\mathrm{Dec}^3 = (\mathrm{Enc}^3)^\dagger$ to recover the original qubit.

Implementation in λ°_ρ

Let $\beta = |0\rangle\langle 0|$.

Encoding.

$$\mathit{encode} = \lambda x.\, \mathrm{Enc}^3(x \otimes \beta \otimes \beta) \qquad : 1 \multimap 3$$

Correction. The syndrome extraction prepends two ancilla qubits, applies the syndrome circuit, and measures. In the original calculus, each branch must apply the correction as a *global* five-qubit operator, and the ancilla qubits cannot be discarded:

$$\mathit{correct}_0 = \lambda y.\, \mathsf{letcase}^\circ\ z = \pi^2(\mathrm{Synd}^5((\beta \otimes \beta) \otimes y))\ \mathsf{in}\ \{z,\, X_3^5\, z,\, X_4^5\, z,\, X_5^5\, z\}$$

where X_k^5 denotes Pauli X on position k of a five-qubit state (e.g. $X_3^5 = I \otimes I \otimes X \otimes I \otimes I$). Each branch returns the full five-qubit state, so:

$$\mathit{correct}_0 : 3 \multimap 5.$$

Decoding. Since $\mathit{correct}_0$ returns a five-qubit state, decoding requires a five-qubit version of the inverse encoding: $\mathrm{Dec}_5 = I^2 \otimes \mathrm{Dec}^3$. Even after decoding, the two ancilla qubits remain:

$$\mathit{decode}_0 = \lambda w.\, \mathrm{Dec}_5^5\, w \qquad : 5 \multimap 5.$$

Full protocol.

$$\mathit{bitflip}_0 = \lambda x.\, \mathit{decode}_0(\mathit{correct}_0(\mathit{encode}(x))) \qquad : 1 \multimap 5.$$

The output type 5 reflects the fact that, in the original calculus, there is no mechanism to discard the ancilla qubits or extract the logical qubit from the decoded state. The ancillas are carried as irremovable overhead.

Implementation with the let Construct

The encoding is unchanged. The let construct transforms the correction and decoding steps.

Correction. Each branch of $\mathsf{letcase}^\circ$ uses let to decompose the five-qubit post-measurement state, apply the correction to only the affected code qubit, and recombine only the three code qubits, discarding the ancillas:

$$\begin{aligned} \mathit{correct} = \lambda y.\, \mathsf{letcase}^\circ\ z = \pi^2(\mathrm{Synd}^5((\beta \otimes \beta) \otimes y))\ \mathsf{in} \\ \{b_0,\, b_1,\, b_2,\, b_3\} \end{aligned}$$

where:

$$\begin{aligned} b_0 &= \mathsf{let}\ q^{\otimes 5} = z\ \mathsf{in}\ q_3 \otimes q_4 \otimes q_5 \\ b_1 &= \mathsf{let}\ q^{\otimes 5} = z\ \mathsf{in}\ (X^1\, q_3) \otimes q_4 \otimes q_5 \\ b_2 &= \mathsf{let}\ q^{\otimes 5} = z\ \mathsf{in}\ q_3 \otimes (X^1\, q_4) \otimes q_5 \\ b_3 &= \mathsf{let}\ q^{\otimes 5} = z\ \mathsf{in}\ q_3 \otimes q_4 \otimes (X^1\, q_5) \end{aligned}$$

Since each branch returns only the three code qubits:

$$\mathit{correct} : 3 \multimap 3.$$

Compared to $\mathit{correct}_0 : 3 \multimap 5$, the let construct eliminates the ancilla overhead. Moreover, the corrections are manifestly local: b_1 applies X^1 to a single-qubit variable q_3, rather than the global operator $X_3^5 = I \otimes I \otimes X \otimes I \otimes I$.

Decoding. After correction, the three-qubit codeword is decoded by applying the inverse encoding circuit. The let construct then extracts the first qubit, which contains the original logical state:

$$\mathit{decode} = \lambda w.\, \mathsf{let}\ q^{\otimes 3} = \mathrm{Dec}^3\, w\ \mathsf{in}\ q_1 \qquad : 3 \multimap 1.$$

Compared to $\mathit{decode}_0 : 5 \multimap 5$, this function accepts the clean three-qubit output of *correct* and returns the single logical qubit.

Full protocol.

$$\mathit{bitflip} = \lambda x.\, \mathit{decode}(\mathit{correct}(\mathit{encode}(x))) \qquad : 1 \multimap 1.$$

The type $1 \multimap 1$ accurately reflects the physical reality of the protocol: a single qubit is encoded, protected, and recovered. Contrast this with $\mathit{bitflip}_0 : 1 \multimap 5$.

Type Derivation

Typing a branch of correct. We derive the type of b_1 (correction on code qubit 1); the other branches are analogous. Write $\Gamma_q = q_1{:}1,\, q_2{:}1,\, q_3{:}1,\, q_4{:}1,\, q_5{:}1$.

$$\dfrac{\dfrac{}{z{:}5 \vdash z : 5}\,\mathsf{ax} \qquad \dfrac{\dfrac{\dfrac{}{q_1{:}1,\, q_2{:}1,\, q_3{:}1 \vdash q_3 : 1}\,\mathsf{ax}}{q_1{:}1,\, q_2{:}1,\, q_3{:}1 \vdash X^1 q_3 : 1}\,\mathsf{u} \qquad \dfrac{\dfrac{}{q_4{:}1 \vdash q_4 : 1}\,\mathsf{ax} \qquad \dfrac{}{q_5{:}1 \vdash q_5 : 1}\,\mathsf{ax}}{q_4{:}1,\, q_5{:}1 \vdash q_4 \otimes q_5 : 2}\,\otimes}{\Gamma_q \vdash (X^1 q_3) \otimes q_4 \otimes q_5 : 3}\,\otimes}{z{:}5 \vdash \mathsf{let}\ q^{\otimes 5} = z\ \mathsf{in}\ (X^1 q_3) \otimes q_4 \otimes q_5 : 3}\,\mathsf{let}$$

The variables q_1 and q_2 (the ancilla components) appear in the context of the left branch but are unused, which is permitted by the affine type system. This is precisely how ancilla qubits are discarded: they are simply not mentioned in the body of the let.

Typing correct. The syntrome extraction term has the following typing:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \beta : 1}\,\mathsf{ax}_\rho \quad \dfrac{}{\vdash \beta : 1}\,\mathsf{ax}_\rho}{\vdash \beta \otimes \beta : 2}\,\otimes \quad \dfrac{}{y{:}3 \vdash y : 3}\,\mathsf{ax}}{y{:}3 \vdash (\beta \otimes \beta) \otimes y : 5}\,\otimes}{y{:}3 \vdash \mathrm{Synd}^5((\beta \otimes \beta) \otimes y) : 5}\,\mathsf{u}}{y{:}3 \vdash \pi^2(\mathrm{Synd}^5((\beta \otimes \beta) \otimes y)) : (2,5)}\,\mathsf{m}$$

Each branch satisfies $z : 5 \vdash b_i : 3$ as shown above. Then:

$$\dfrac{\dfrac{z{:}5 \vdash b_0{:}3 \quad z{:}5 \vdash b_1{:}3 \quad z{:}5 \vdash b_2{:}3 \quad z{:}5 \vdash b_3{:}3 \quad y{:}3 \vdash \pi^2(\cdots) : (2,5)}{y{:}3 \vdash \mathsf{letcase}^\circ\ z = \cdots\ \mathsf{in}\ \{b_0, b_1, b_2, b_3\} : 3}\,\mathsf{lc}}{\vdash \mathit{correct} : 3 \multimap 3}\,\multimap_i$$

Typing decode.

$$\dfrac{\dfrac{\dfrac{}{w{:}3 \vdash w : 3}\,\mathsf{ax}}{w{:}3 \vdash \mathrm{Dec}^3 w : 3}\,\mathsf{u} \quad \dfrac{}{q_1{:}1, q_2{:}1, q_3{:}1 \vdash q_1 : 1}\,\mathsf{ax}}{w{:}3 \vdash \mathsf{let}\ q^{\otimes 3} = \mathrm{Dec}^3 w\ \mathsf{in}\ q_1 : 1}\,\mathsf{let}}{\vdash \mathit{decode} : 3 \multimap 1}\,\multimap_i$$

Again, q_2 and q_3 are discarded by the affine type system, these correspond to the ancilla qubits $|0\rangle$ that were used during encoding.

Typing bitflip.

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mathit{decode} : 3 \multimap 1} \quad \dfrac{\dfrac{\vdots}{\vdash \mathit{correct} : 3 \multimap 3} \quad \dfrac{\dfrac{\vdots}{\vdash \mathit{encode} : 1 \multimap 3} \quad \dfrac{}{x{:}1 \vdash x : 1}\,\mathsf{ax}}{x{:}1 \vdash \mathit{encode}(x) : 3}\,\multimap_e}{x{:}1 \vdash \mathit{correct}(\mathit{encode}(x)) : 3}\,\multimap_e}{x{:}1 \vdash \mathit{decode}(\mathit{correct}(\mathit{encode}(x))) : 1}\,\multimap_e}{\vdash \mathit{bitflip} : 1 \multimap 1}\,\multimap_i$$

The type $1 \multimap 1$ confirms that the protocol takes a single qubit and returns a single qubit. By contrast, in the original calculus the types compose as $(1 \multimap 3) \to (3 \multimap 5) \to (5 \multimap 5)$, yielding $\mathit{bitflip}_0 : 1 \multimap 5$.

3. PROPERTIES

In this chapter we show that discarding a qubit through the affine type system with the let construct is equivalent to tracing it out.

Then we also show that the extended calculus preserves four fundamental properties: Subject Reduction (well-typedness is preserved by reduction), Progress (well-typed closed terms are either values or can reduce), Strong Normalisation (every closed well-typed term terminates), and Soundness (reduction preserves the denotational interpretation). We also establish Adequacy: two closed terms with equal denotations are observationally equivalent. The proofs for Subject Reduction and Progress extend those in [2] by adding cases for the new let construct. Soundness also follows [2] strategy, but without extending its proof as we changed the interpretation of the calculus. For Strong Normalisation we use Girard's reducibility candidates method [4], extending the reduction relation with projection rules $\sum_i p_i\, t_i \to t_j$ as in [3], with a new per-construct lemma for the let. We present sketches of some of the proofs here; full detailed proofs are given in Appendix D.

3.1 Discard as Partial Trace

A key semantic property of the let construct is that *ignoring* a component in the body (which is permitted by the affine type system) is not merely a syntactic convenience. It is computationally equivalent to first computing the reduced density matrix of the remaining qubits via the partial trace, and then decomposing that reduced state. We make this precise below.

Notation 3.1.1. We write $t \downarrow r$ to mean that t and r reduce to a common term.

Proposition 3.1.2 (Discard as Partial Trace)**.** *Let ρ^n be an n-qubit density matrix with $n \geq 2$, and let s be a term with $x_2 : 1, \ldots, x_n : 1 \vdash s : A$ (note that $x_1 \notin FV(s)$ is then implied by the typing). Then*

$$\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s\ \downarrow\ \mathsf{let}\ y^{\otimes n-1} = \mathsf{tr}_1(\rho^n)\ \mathsf{in}\ s[y_1/x_2, \ldots, y_{n-1}/x_n].$$

The same holds for discarding any other qubit position k by relabeling indices.

Proof. Let $\rho^n = \sum_{i,\vec{l}} p_{i\vec{l}} \bigotimes_{k=1}^{n} \gamma_{i_k}^{l_k}$ be the combined decomposition of ρ^n (equation 2.1), where each $\gamma_{i_k}^{l_k}$ is a single-qubit density matrix, $\vec{l} \in \{1,2\}^n$, and $\sum_{i,\vec{l}} p_{i\vec{l}} = 1$.

Reducing the left-hand side. Applying the main let reduction rule (Table 2.2):

$$\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s\ \to\ \sum_{i,\vec{l}} p_{i\vec{l}}\, s\big[\gamma_{i_1}^{l_1}/x_1,\ \gamma_{i_2}^{l_2}/x_2,\ \ldots,\ \gamma_{i_n}^{l_n}/x_n\big].$$

Since $x_1 \notin FV(s)$, the substitution $[\gamma_{i_1}^{l_1}/x_1]$ leaves s unchanged, so:

$$\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s\ \to\ \sum_{i,\vec{l}} p_{i\vec{l}}\, s\big[\gamma_{i_2}^{l_2}/x_2,\ \ldots,\ \gamma_{i_n}^{l_n}/x_n\big]. \tag{3.1}$$

Grouping by the indices $(l_2, \ldots, l_n)$ and summing over l_1:

$$= \sum_{i,\, l_2,\ldots,l_n} \Big(\sum_{l_1} p_{i\vec{l}}\Big)\; s\big[\gamma_{i_2}^{l_2}/x_2,\; \ldots,\; \gamma_{i_n}^{l_n}/x_n\big]. \tag{3.2}$$

Computing the partial trace. By Definition 0.2.6 and linearity of tr_1:

$$\mathsf{tr}_1(\rho^n) = \mathsf{tr}_1\Big(\sum_{i,\vec{l}} p_{i\vec{l}}\, \gamma_{i_1}^{l_1} \otimes \bigotimes_{k=2}^{n} \gamma_{i_k}^{l_k}\Big) = \sum_{i,\vec{l}} p_{i\vec{l}}\, \mathsf{tr}\big(\gamma_{i_1}^{l_1}\big) \bigotimes_{k=2}^{n} \gamma_{i_k}^{l_k}.$$

Since each $\gamma_{i_1}^{l_1}$ is a single-qubit density matrix, $\mathsf{tr}(\gamma_{i_1}^{l_1}) = 1$, giving:

$$\mathsf{tr}_1(\rho^n) \;=\; \sum_{i,\, l_2,\ldots,l_n} \Big(\sum_{l_1} p_{i\vec{l}}\Big) \bigotimes_{k=2}^{n} \gamma_{i_k}^{l_k}. \tag{3.3}$$

This is precisely the combined decomposition of $\mathsf{tr}_1(\rho^n)$ (cf. equation 2.1), with coefficients $q_{i,l_2,\ldots,l_n} \coloneqq \sum_{l_1} p_{i\vec{l}}$ and components $\gamma_{i_k}^{l_k}$ for $k = 2, \ldots, n$.

Reducing the right-hand side. Write $s' \coloneqq s[y_1/x_2, \ldots, y_{n-1}/x_n]$ and apply the main let reduction rule to $\mathsf{let}\ y^{\otimes n-1} = \mathsf{tr}_1(\rho^n)\ \mathsf{in}\ s'$ using decomposition (3.3):

$$\begin{aligned} \mathsf{let}\ y^{\otimes n-1} = \mathsf{tr}_1(\rho^n)\ \mathsf{in}\ s' \;\to\; & \sum_{i,\, l_2,\ldots,l_n} q_{i,l_2,\ldots,l_n}\; s'\big[\gamma_{i_2}^{l_2}/y_1,\; \ldots,\; \gamma_{i_n}^{l_n}/y_{n-1}\big] \\ = \; & \sum_{i,\, l_2,\ldots,l_n} \Big(\sum_{l_1} p_{i\vec{l}}\Big)\; s\big[\gamma_{i_2}^{l_2}/x_2,\; \ldots,\; \gamma_{i_n}^{l_n}/x_n\big]. \end{aligned} \tag{3.4}$$

The last equality uses $s'[\gamma_{i_2}^{l_2}/y_1, \ldots] = s[\gamma_{i_2}^{l_2}/x_2, \ldots]$ by definition of s'.

Conclusion. Expressions (3.2) and (3.4) are identical, so both sides reduce in one step to the same term. Since $\mathsf{tr}_1(\rho^n)$ is itself an $(n-1)$-qubit density matrix, the right-hand side is well-typed, confirming that the equivalence is well-formed. Finally, the same argument applies to discarding any qubit position k by relabeling: permuting index k to position 1 and applying the result above. □

Remark 3.1.3. This proposition gives an operational reading to affine variable discard and connects it to the no-deleting theorem (Theorem 0.2.9, Section 0.2.4). When a variable x_k is not mentioned in the body s of a let, the reduction rule silently sums out its contribution exactly as the partial trace does in quantum mechanics. The affine type system thus enforces the quantum mechanical principle that ignoring a subsystem is equivalent to computing its reduced state.

The following corollary generalises Proposition 3.1.2 to the simultaneous discard of any subset of qubits.

Corollary 3.1.4 (Multi-Qubit Discard as Partial Trace)**.** *Let ρ^n be an n-qubit density matrix with $n \geq 2$. Let $K = \{k_1 < \cdots < k_m\} \subseteq \{1, \ldots, n\}$ be a non-empty subset of qubit positions to be discarded, with $m < n$, and let $\bar{K} = \{j_1 < \cdots < j_{n-m}\} = \{1, \ldots, n\} \setminus K$ be the remaining positions. Let s be a term with $x_{j_1} : 1, \ldots, x_{j_{n-m}} : 1 \vdash s : A$ (note that $x_k \notin FV(s)$ for all $k \in K$ is then implied by the typing). Then*

$$\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s \;\downarrow\; \mathsf{let}\ y^{\otimes n-m} = \mathsf{tr}_K(\rho^n)\ \mathsf{in}\ s[y_1/x_{j_1}, \ldots, y_{n-m}/x_{j_{n-m}}].$$

Proof. By induction on $m = |K|$.

Base case ($m = 1$). This is exactly Proposition 3.1.2: discarding a single qubit position is the same as applying the single-qubit partial trace.

Inductive step. Assume the result holds for any set K' of m discarded positions, for some $1 \leq m < n - 1$. Let $K = K' \cup \{k^*\}$ with $k^* \notin K'$, so $|K| = m + 1$. We must show that discarding all positions in K from ρ^n is the same as taking $\mathsf{tr}_K(\rho^n)$.

Write $\bar{K}' = \{j_1 < \cdots < j_{n-m}\} = \{1, \ldots, n\} \setminus K'$ for the positions *not* discarded in the first m steps, and note that $k^* \in \bar{K}'$. Let k^{**} be the position of k^* within the ordered set $\bar{K}'$ (i.e. $j_{k^{**}} = k^*$).

Since $x_k \notin FV(s)$ for all $k \in K \supseteq K'$, the induction hypothesis applied to K' gives:

$$\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s \downarrow \mathsf{let}\ y^{\otimes n-m} = \mathsf{tr}_{K'}(\rho^n)\ \mathsf{in}\ s[y_1/x_{j_1}, \ldots, y_{n-m}/x_{j_{n-m}}].$$

In the residual body, x_{k^*} has been renamed to $y_{k^{**}}$ but is still absent from the body (since $k^* \in K$), so $y_{k^{**}} \notin FV(s[y_r/x_{j_r}])$. Applying Proposition 3.1.2 to this $(n-m)$-qubit let, discarding position k^{**}:

$$\mathsf{let}\ y^{\otimes n-m} = \mathsf{tr}_{K'}(\rho^n)\ \mathsf{in}\ s[\cdots] \downarrow \mathsf{let}\ z^{\otimes n-m-1} = \mathsf{tr}_{k^{**}}\big(\mathsf{tr}_{K'}(\rho^n)\big)\ \mathsf{in}\ s[\cdots],$$

where on the right the body has been further renamed, substituting z_r for y_r for each remaining (non-discarded) position. Since partial traces over disjoint subsystems commute, we have $\mathsf{tr}_{k^{**}}(\mathsf{tr}_{K'}(\rho^n)) = \mathsf{tr}_K(\rho^n)$, so the right-hand side is exactly $\mathsf{let}\ z^{\otimes n-m-1} = \mathsf{tr}_K(\rho^n)\ \mathsf{in}\ s[\cdots]$, completing the induction. □

Remark 3.1.5. Note that the order in which the individual partial traces are taken does not matter: $\mathsf{tr}_K = \mathsf{tr}_{k_m} \circ \cdots \circ \mathsf{tr}_{k_1}$ for any ordering of K, since partial traces over disjoint subsystems commute. Corollary 3.1.4 therefore also implies that discarding qubits one at a time (via m sequential applications of Proposition 3.1.2) and discarding all of them simultaneously (via a single application of the corollary) yield the same result, which is consistent with the commutativity of partial traces.

3.2 Substitution Lemma

The proofs of the main theorems rely on the substitution lemma, which also requires a new case for the let construct. We assume standard weakening and strengthening properties for the affine type system throughout.

Lemma 3.2.1 (Substitution)**.** *If* $\Gamma, x : A \vdash t : B$ *and* $\Delta \vdash r : A$*, then* $\Gamma, \Delta \vdash t[r/x] : B$*.*

Proof sketch. By induction on t. The existing cases (variables, abstraction, application, density matrices, unitaries, measurement, tensor, sums, and $\mathsf{letcase}^\circ$) follow as in [2]. The new case is:

Let $t = \mathsf{let}\ y^{\otimes n} = s\ \mathsf{in}\ u$. Then $\Gamma, x : A = \Gamma_1, \Gamma_2$ with $\Gamma_1 \vdash s : n$ and $\Gamma_2, y_1 : 1, \ldots, y_n : 1 \vdash u : B$. If $x : A \in \Gamma_1$, the induction hypothesis gives $\Gamma_1 \setminus \{x : A\}, \Delta \vdash s[r/x] : n$, and since $x \notin FV(u)$ we have $u[r/x] = u$, so the result follows by rule let. The case $x : A \in \Gamma_2$ is symmetric. □

3.3 Subject Reduction

Theorem 3.3.1 (Subject Reduction)**.** *If* $\Gamma \vdash t : A$ *and* $t \to r$*, then* $\Gamma \vdash r : A$*.*

Proof sketch. By induction on the derivation of $t \to r$. The cases for the original constructs of λ°_ρ follow as in [2]. The new cases are:

Distributing rule for $\mathsf{letcase}^\circ$. Let $t = \mathsf{letcase}^\circ\ x = \sum_j q_j w_j\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}$ and $r = \sum_j q_j\, \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}$. By inversion of rule lc, $\Gamma \vdash \sum_j q_j w_j : (m, n)$, so by rule $+$ each $w_j : (m, n)$. Rule lc applied to each w_j gives $\Gamma \vdash \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\} : A$, and rule $+$ then gives $\Gamma \vdash r : A$.

Main reduction. Let $t = \mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s$ and $r = \sum_{j,\vec{t}} p_{j\vec{t}}\, s[\gamma^{t_1}_{i_{j1}}/x_1, \cdots, \gamma^{t_n}_{i_{jn}}/x_n]$. By inversion, $\Gamma \vdash \rho^n : n$ and $\Delta, x_1 : 1, \ldots, x_n : 1 \vdash s : A$. Each $\gamma^{t_k}_{i_{jk}}$ is a single-qubit density matrix, so by rule ax_ρ, $\vdash \gamma^{t_k}_{i_{jk}} : 1$. Repeated application of Lemma 3.2.1 gives $\Delta \vdash s[\gamma^{t_1}_{i_{j1}}/x_1, \cdots, \gamma^{t_n}_{i_{jn}}/x_n] : A$. Since the Pauli decomposition preserves trace ($\sum_{j,\vec{t}} p_{j\vec{t}} = 1$), rule $+$ yields the result.

Contextual closures. For $\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s \to \mathsf{let}\ x^{\otimes n} = r\ \mathsf{in}\ s$ with $t \to r$: by inversion, $\Gamma \vdash t : n$; by the induction hypothesis, $\Gamma \vdash r : n$; by rule let, $\Gamma, \Delta \vdash \mathsf{let}\ x^{\otimes n} = r\ \mathsf{in}\ s : A$. The case for reduction in the body is analogous. □

3.4 Progress

Definition 3.4.1 (Values)**.** A value in the extended λ°_ρ is a term v defined by:

$$w := \lambda x.t \mid \pi^m \rho^n \mid \sum_i p_i w_i \text{ where } \exists j, k : w_j \neq w_k$$

$$v := w \mid \rho^n$$

Note that the let construct is not a value: it always reduces (either by the main rule when its first argument is a concrete density matrix, or by contextual closure otherwise).

Theorem 3.4.2 (Progress)**.** *If* $\vdash t : A$ *then either* t *is a value or there exists* r *such that* $t \to r$*.*

Proof sketch. We prove a stronger statement for open terms: if $\Gamma \vdash t : A$, then either t is a value, there exists r such that $t \to r$, or t contains a free variable and does not rewrite.

The proof is by induction on the typing derivation. The cases for the original constructs of λ°_ρ follow [2]. The new case is:

Let $\Gamma, \Delta \vdash \mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s : A$ as a consequence of $\Gamma \vdash t : n$ and $\Delta, x_1 : 1, \ldots, x_n : 1 \vdash s : A$. By the induction hypothesis on t:

- If $t = \rho^n$ (a density matrix value), then $\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s$ reduces by the main rule.
- If t contains a free variable and does not rewrite, then $\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s$ also contains a free variable and does not rewrite.
- If there exists t' such that $t \to t'$, then $\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s \to \mathsf{let}\ x^{\otimes n} = t'\ \mathsf{in}\ s$ by contextual closure.

In all cases, the property is preserved. □

3.5 Strong Normalisation

We now show that every closed well-typed term terminates.

Theorem 3.5.1 (Strong Normalisation)**.** *Every closed, well-typed term* $\vdash t : A$ *is strongly normalising.*

Proof. Strong normalisation is proved using Girard's reducibility candidates method [4], defining typed reducibility sets and a fundamental substitution lemma.

Typed reducibility sets. Following Díaz-Caro and Dowek [3], we first extend the reduction relation with projection rules $\sum_i p_i\, t_i \to t_j$ for any j — these are not part of the operational semantics but make sums reducible to each summand, which is the key technical device for handling the distributivity rule $(\sum_i p_i\, t_i)\, s \to \sum_i p_i\, (t_i\, s)$ without duplication issues. Let SN denote the set of terms strongly normalising under this extended relation.

We define typed reducibility sets $SN(A)$ by induction on A: $SN(n) = SN((m,n)) = SN$, and $SN(A \multimap B) = \{t \in SN \mid t \to^* \lambda x.\, u \Rightarrow \forall v \in SN(A),\, u[v/x] \in SN(B)\}$. A forward-closure lemma (CR3) establishes that any neutral term all of whose one-step reducts are in $SN(A)$ is itself in $SN(A)$.

Per-construct lemmas. For each typing rule, a dedicated lemma shows that the construct preserves membership in the appropriate reducibility set. The key new case is the let construct: if $t \in SN(n)$ and for all density matrices $\gamma_k \in SN(1)$, the body $s[\gamma_1/x_1, \ldots, \gamma_n/x_n] \in SN(A)$, then $\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s \in SN(A)$. The proof uses induction on $\ell(t)$ and CR3: when t normalises to a density matrix ρ^n, the main rule fires and produces a sum of substituted bodies; each body is in $SN(A)$ by hypothesis and the density matrices substituted for each x_k are in $SN(1)$; the sum is in $SN(A)$ by the sum adequacy lemma.

Fundamental lemma and conclusion. A fundamental substitution lemma shows: if $\Gamma \vdash t : A$ and $\theta \vDash \Gamma$ (every variable's image is in the appropriate SN set), then $\theta(t) \in SN(A)$. Applying this with the empty substitution gives strong normalisation for every closed well-typed term.

Full details are given in Appendix D. □

3.6 Soundness

The soundness proof relies on the following semantic substitution lemma, which states that syntactic substitution in a term commutes with the denotational interpretation.

Lemma 3.6.1 (Semantic Substitution)**.** *Let* $\Gamma, x : A \vdash t : B$*,* $\Delta \vdash s : A$*, and* $\theta \vDash \Gamma, \Delta$*. Then:*

$$[\![t[s/x]]\!]_\theta \;=\; [\![t]\!]_{\theta, x \mapsto [\![s]\!]_\theta}.$$

Proof sketch. By induction on t. The base cases (variables, density matrices) and the cases for application, λ-abstraction, unitary, measurement, tensor, and linear combination follow from the definitions and linearity of the interpretation. The case for $\mathsf{letcase}^\circ$ is analogous to those in [2]. The new case is:

Let $t = \mathsf{let}\ y^{\otimes n} = u\ \mathsf{in}\ v$ with $\Gamma, x : A = \Gamma_1, \Gamma_2$ and $\Gamma_1 \vdash u : n$, $\Gamma_2, y_1 : 1, \ldots, y_n : 1 \vdash v : B$. If $x : A \in \Gamma_1$, then $t[s/x] = \mathsf{let}\ y^{\otimes n} = u[s/x]\ \mathsf{in}\ v$ and both sides reduce to the same expression by the induction hypothesis on u and linearity. If $x : A \in \Gamma_2$, then $t[s/x] = \mathsf{let}\ y^{\otimes n} = u\ \mathsf{in}\ v[s/x]$ and the result follows by the induction hypothesis on v.

Full details are given in Appendix D. □

Theorem 3.6.2 (Soundness)**.** *If $\Gamma \vdash t : A$, $\theta \vDash \Gamma$, and $t \to r$, then $[\![t]\!]_\theta = [\![r]\!]_\theta$.*

Proof sketch. By induction on the derivation of $t \to r$. The cases for the original constructs of λ°_ρ follow the same structure as Theorem 2.7 in [2], adapted to the simplified interpretation that drops measurement-bookkeeping tuples. The new cases are:

Main let *reduction.* Let $t = \mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s$ and $r = \sum_{i,\vec{l}} p_{i\vec{l}}\, s[\gamma^{l_1}_{i_1}/x_1, \ldots, \gamma^{l_n}_{i_n}/x_n]$, where $p_{i\vec{l}} = \alpha_i(\rho^n) \prod_k \lambda^{l_k}_{i_k}$ are the combined decomposition coefficients (equation 2.1).

Unfolding the interpretation of the let construct:

$$[\![\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s]\!]_\theta = \sum_{i,\vec{l}} \Big(\alpha_i(\rho^n) \prod_{k=1}^{n} \lambda^{l_k}_{i_k}\Big) [\![s]\!]_{\theta, x_1 \mapsto \gamma^{l_1}_{i_1}, \ldots, x_n \mapsto \gamma^{l_n}_{i_n}} = \sum_{i,\vec{l}} p_{i\vec{l}}\, [\![s]\!]_{\theta, x_1 \mapsto \gamma^{l_1}_{i_1}, \ldots, x_n \mapsto \gamma^{l_n}_{i_n}}.$$

By Lemma 3.6.1 applied n times:

$$[\![s]\!]_{\theta, x_1 \mapsto \gamma^{l_1}_{i_1}, \ldots, x_n \mapsto \gamma^{l_n}_{i_n}} = [\![s[\gamma^{l_1}_{i_1}/x_1, \ldots, \gamma^{l_n}_{i_n}/x_n]]\!]_\theta.$$

On the other hand, $[\![r]\!]_\theta = [\![\sum_{i,\vec{l}} p_{i\vec{l}}\, s[\gamma^{l_1}_{i_1}/x_1, \ldots, \gamma^{l_n}_{i_n}/x_n]]\!]_\theta = \sum_{i,\vec{l}} p_{i\vec{l}} [\![s[\gamma^{l_1}_{i_1}/x_1, \ldots, \gamma^{l_n}_{i_n}/x_n]]\!]_\theta$ by linearity of the interpretation. Both expressions coincide.

Distributing rule for letcase°. Let $t = \mathsf{letcase}^\circ\ x = \sum_j q_j w_j\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}$ and $r = \sum_j q_j\, \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}$. The interpretation of t uses $\rho = [\![\sum_j q_j w_j]\!]_\theta = \sum_j q_j\, [\![w_j]\!]_\theta$. Because $p_i \cdot \rho_i = \overline{\pi_i}\, \rho\, \overline{\pi_i}^\dagger$ (the normalisation factor p_i cancels), we have

$$[\![t]\!]_\theta = \sum_i \overline{\pi_i}\, \rho\, \overline{\pi_i}^\dagger \cdot F_i = \sum_j q_j \sum_i \overline{\pi_i}\, [\![w_j]\!]_\theta\, \overline{\pi_i}^\dagger \cdot F_i = \sum_j q_j\, [\![\mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{s_0, \ldots\}]\!]_\theta = [\![r]\!]_\theta,$$

where F_i denotes the (linear) function $\rho_i \mapsto [\![s_i]\!]_{\theta, x \mapsto \rho_i}$.

Contextual closures. For $\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s \to \mathsf{let}\ x^{\otimes n} = r\ \mathsf{in}\ s$ with $t \to r$: by the induction hypothesis $[\![t]\!]_\theta = [\![r]\!]_\theta$, so $\alpha_i([\![t]\!]_\theta) = \alpha_i([\![r]\!]_\theta)$ for all i, and the two let interpretations are equal. The case for reduction in the body is analogous, using linearity and the induction hypothesis.

Full details are given in Appendix D. □

Remark 3.6.3. The key insight behind the let case is that the operational semantics (the combined Pauli decomposition used in the reduction rule) and the denotational semantics (the definition of $[\![\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s]\!]_\theta$) are defined by exactly the same mathematical object: the coefficients $p_{i\vec{l}} = \alpha_i(\rho) \prod_k \lambda^{l_k}_{i_k}$. Soundness then reduces to an application of Lemma 3.6.1.

3.7 Adequacy

The soundness result tells us that the denotational interpretation is invariant under reduction. But invariance alone does not imply that the interpretation carries useful information: a trivial interpretation mapping every term to some fixed density matrix I would be sound. We now explore the converse direction property to soundness, which is *completeness*.

A completeness theorem would state that if $\Gamma \vdash t : A$, $\Gamma \vdash r : A$, and $[\![t]\!]_\theta = [\![r]\!]_\theta$, then there exists a value v such that $t \to^* v$ and $r \to^* v$.

However, this would say that denotationally equal programs always reduce to the same value, which is too strong for function types: the same quantum operation can be programmed in syntactically distinct ways that the semantics cannot distinguish. For example, consider

$$r = \lambda f.\, f \qquad \text{and} \qquad t = \lambda f.\, \lambda x.\, f(x),$$

both of type $(A \multimap A) \multimap (A \multimap A)$. The term r returns its argument f directly, while t constructs a new function that applies f to its own argument — two operationally different descriptions of the same transformation. Both denote the identity completely positive map on $A \multimap A$: for any $\varphi \in [\![A \multimap A]\!]$, $[\![r]\!]_\theta(\varphi) = \varphi = [\![t]\!]_\theta(\varphi)$. Both are λ-values and hence normal forms (the subterm $f(x)$ inside t is already stuck, as f is a variable, so no reduction applies even in the presence of a lambda-body rule). Thus t and r are distinct normal forms with the same interpretation and no common reduct. This counterexample shows that the statement above cannot hold in general.

Since full completeness cannot be proved in general, we instead characterise semantic equality by *observational equivalence*: two terms are equivalent if no program context can distinguish them.

Definition 3.7.1 (Context)**.** A *context* C is a term with exactly one free variable, written $[\cdot]$, such that $[\cdot] : A \vdash C : n$ for some type A and $n \in \mathbb{N}$. We call A the *hole type* and n the *output type* of C. The substitution of $[\cdot]$ by a closed term t of type A is denoted $C[t]$; by construction $\vdash C[t] : n$.

Definition 3.7.2 (Observational equivalence)**.** Two closed terms $\vdash t : A$ and $\vdash r : A$ are *observationally equivalent*, written $t \equiv r$, if for every context C with hole type A there exists a density matrix ρ such that $C[t] \to^* \rho$ and $C[r] \to^* \rho$.

Returning to the earlier example, it is easy to see that $r = \lambda f.\, f$ and $t = \lambda f.\, \lambda x.\, f(x)$ are observationally equivalent. Any context C with $[\cdot] : (A \multimap A) \multimap (A \multimap A) \vdash C : n$ must eventually apply the plugged-in term to some argument and reduce the result to a density matrix ρ^n. Since r and t both act as the identity on $A \multimap A$, the context receives the same function in both cases and there is no way for it to produce different density matrices. Hence $t \equiv r$, confirming that the two terms are genuinely indistinguishable by any observation, not merely by the denotational semantics.

The proof of Adequacy rests on two lemmas.

Lemma 3.7.3. *Let C be a context with hole type A and output type B. Let θ be any valuation of the free variables of C (those not contributed by the hole). For any closed terms $\vdash t : A$ and $\vdash r : A$,*

$$[\![t]\!]_\theta = [\![r]\!]_\theta \implies [\![C[t]]\!]_\theta = [\![C[r]]\!]_\theta.$$

Proof sketch. By structural induction on C. In every case the interpretation is defined compositionally: the semantic value of a compound term depends on the semantic values of its immediate subterms. Therefore, replacing the subterm occupying the hole position from t to r (which have the same denotation by hypothesis) leaves the overall denotation unchanged. □

Lemma 3.7.4 (Normalisation)**.** *If $\vdash t : n$ is a closed well-typed term of type n, then there exists a density matrix ρ^n such that $t \to^* \rho^n$.*

Proof. By Theorem 3.5.1 (Strong Normalisation), t is strongly normalising. By Theorem 3.4.2 (Progress) and Theorem 3.3.1 (Subject Reduction), every closed well-typed term either is a value or reduces, with type preserved. Since t has type n, its normal form must be a value of type n, which can only be a density matrix ρ^n. □

Theorem 3.7.5 (Adequacy)**.** *If $\vdash t : A$, $\vdash r : A$, and $[\![t]\!]_\theta = [\![r]\!]_\theta$, then $t \equiv r$.*

Proof. Let C be any context with hole type A and output type n, so that $\vdash C[t] : n$ and $\vdash C[r] : n$ are closed ground-type terms. We exhibit a single density matrix ρ to which both reduce.

Step 1: Equal denotations after plugging. By Lemma 3.7.3 applied to the hypothesis $[\![t]\!]_\theta = [\![r]\!]_\theta$,

$$[\![C[t]]\!]_\theta = [\![C[r]]\!]_\theta.$$

Step 2: Both sides normalise. By Lemma 3.7.4 applied to the closed ground-type terms $C[t]$ and $C[r]$, there exist density matrices ρ_1 and ρ_2 such that

$$C[t] \to^* \rho_1 \qquad \text{and} \qquad C[r] \to^* \rho_2.$$

Step 3: Soundness ties the normal forms to the denotation. By Theorem 3.6.2 applied iteratively along the two reduction sequences,

$$[\![C[t]]\!]_\theta = [\![\rho_1]\!]_\theta \qquad \text{and} \qquad [\![C[r]]\!]_\theta = [\![\rho_2]\!]_\theta.$$

By definition, $[\![\rho_1]\!]_\theta = \rho_1$ and $[\![\rho_2]\!]_\theta = \rho_2$.

Step 4: The normal forms coincide. Combining the equalities from Steps 1–3:

$$\rho_1 = [\![\rho_1]\!]_\theta = [\![C[t]]\!]_\theta = [\![C[r]]\!]_\theta = [\![\rho_2]\!]_\theta = \rho_2.$$

Setting $\rho := \rho_1 = \rho_2$, we have $C[t] \to^* \rho$ and $C[r] \to^* \rho$. Since C was an arbitrary context with output type n, this shows $t \equiv r$. □

Remark 3.7.6. The adequacy result makes the denotational semantics *observationally complete*: if two programs are semantically equal (same denotation), then no ground-type experiment can distinguish them operationally.

BIBLIOGRAPHY

[1] Agustín Borgna. Simulación del lambda cálculo de matrices de densidad en el lambda cálculo cuántico de Selinger y Valiron. Tesis de grado, Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales, 2019.

[2] Alejandro Díaz-Caro. A lambda calculus for density matrices with classical and probabilistic controls. In *Programming Languages and Systems (APLAS 2017)*, volume 10695 of *LNCS*, pages 448–467. Springer, 2017. arXiv:1705.00097.

[3] Alejandro Díaz-Caro and Gilles Dowek. A linear linear lambda-calculus. *Mathematical Structures in Computer Science*, 34(10):1103–1137, 2024. arXiv:2201.11221.

[4] Jean-Yves Girard, Yves Lafont, and Paul Taylor. *Proofs and Types*. Number 7 in Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1989.

[5] Océane Koska, Marc Baboulin, and Arnaud Gazda. A tree-approach Pauli decomposition algorithm with application to quantum computing. In *IEEE International Conference on Quantum Computing and Engineering (QCE)*, 2024. arXiv:2403.11644.

[6] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[7] Arun K. Pati and Samuel L. Braunstein. Impossibility of deleting an unknown quantum state. *Nature*, 404(6774):164–165, 2000.

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

Appendix A

BELL STATE COMPUTATIONS

This appendix contains the detailed computations for the Bell state examples in Examples 0.4.2, 2.2.2, and Subsection 2.7.1.

A.1 Pauli Decomposition Coefficients (Example 0.4.2)

We compute $\langle\beta_{00}|\,(M_1 \otimes M_2)\,|\beta_{00}\rangle$ for all sixteen pairs $M_1, M_2 \in \{I, X, Y, Z\}$, using the Pauli actions:

$$\begin{aligned} I\,|0\rangle = |0\rangle\,, \quad X\,|0\rangle = |1\rangle\,, \quad Y\,|0\rangle = i\,|1\rangle\,, \qquad Z\,|0\rangle = |0\rangle\,, \\ I\,|1\rangle = |1\rangle\,, \quad X\,|1\rangle = |0\rangle\,, \quad Y\,|1\rangle = -i\,|0\rangle\,, \quad Z\,|1\rangle = -\,|1\rangle\,. \end{aligned}$$

In each case we first compute $(M_1 \otimes M_2)\,|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(M_1\,|0\rangle \otimes M_2\,|0\rangle + M_1\,|1\rangle \otimes M_2\,|1\rangle)$ and then take the inner product with $\langle\beta_{00}| = \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)$.

Pairs with $M_1 = I$

$$\begin{aligned} (I \otimes I)\,|\beta_{00}\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle) = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ \langle\beta_{00}|\,(I \otimes I)\,|\beta_{00}\rangle &= \tfrac{1}{2}(\langle 00|+\langle 11|)(|00\rangle+|11\rangle) = \tfrac{1}{2}(1+1) = 1. \end{aligned}$$

$$\begin{aligned} (I \otimes X)\,|\beta_{00}\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle\otimes|1\rangle + |1\rangle\otimes|0\rangle) = \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ \langle\beta_{00}|\,(I \otimes X)\,|\beta_{00}\rangle &= \tfrac{1}{2}(\langle 00|+\langle 11|)(|01\rangle+|10\rangle) = \tfrac{1}{2}(0+0) = 0. \end{aligned}$$

$$\begin{aligned} (I \otimes Y)\,|\beta_{00}\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle\otimes i\,|1\rangle + |1\rangle\otimes(-i)\,|0\rangle) = \tfrac{1}{\sqrt{2}}(i\,|01\rangle - i\,|10\rangle), \\ \langle\beta_{00}|\,(I \otimes Y)\,|\beta_{00}\rangle &= \tfrac{1}{2}(\langle 00|+\langle 11|)(i\,|01\rangle-i\,|10\rangle) = \tfrac{1}{2}(0+0) = 0. \end{aligned}$$

$$\begin{aligned} (I \otimes Z)\,|\beta_{00}\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle + |1\rangle\otimes(-\,|1\rangle)) = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ \langle\beta_{00}|\,(I \otimes Z)\,|\beta_{00}\rangle &= \tfrac{1}{2}(\langle 00|+\langle 11|)(|00\rangle-|11\rangle) = \tfrac{1}{2}(1-1) = 0. \end{aligned}$$

Pairs with $M_1 = X$

$$\begin{aligned} (X \otimes I)\,|\beta_{00}\rangle &= \tfrac{1}{\sqrt{2}}(|1\rangle\otimes|0\rangle + |0\rangle\otimes|1\rangle) = \tfrac{1}{\sqrt{2}}(|10\rangle + |01\rangle), \\ \langle\beta_{00}|\,(X \otimes I)\,|\beta_{00}\rangle &= \tfrac{1}{2}(\langle 00|+\langle 11|)(|10\rangle+|01\rangle) = \tfrac{1}{2}(0+0) = 0. \end{aligned}$$

$$\begin{aligned} (X \otimes X)\,|\beta_{00}\rangle &= \tfrac{1}{\sqrt{2}}(|1\rangle\otimes|1\rangle + |0\rangle\otimes|0\rangle) = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ \langle\beta_{00}|\,(X \otimes X)\,|\beta_{00}\rangle &= \tfrac{1}{2}(\langle 00|+\langle 11|)(|00\rangle+|11\rangle) = \tfrac{1}{2}(1+1) = 1. \end{aligned}$$

$$\begin{aligned} (X \otimes Y)\,|\beta_{00}\rangle &= \tfrac{1}{\sqrt{2}}(|1\rangle\otimes i\,|1\rangle + |0\rangle\otimes(-i)\,|0\rangle) = \tfrac{1}{\sqrt{2}}(i\,|11\rangle - i\,|00\rangle), \\ \langle\beta_{00}|\,(X \otimes Y)\,|\beta_{00}\rangle &= \tfrac{1}{2}(\langle 00|+\langle 11|)(i\,|11\rangle-i\,|00\rangle) = \tfrac{1}{2}(-i+i) = 0. \end{aligned}$$

$$(X \otimes Z)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(|1\rangle\otimes|0\rangle + |0\rangle\otimes(-|1\rangle)) = \tfrac{1}{\sqrt{2}}(|10\rangle - |01\rangle),$$
$$\langle\beta_{00}|\,(X \otimes Z)\,|\beta_{00}\rangle = \tfrac{1}{2}(\langle 00|+\langle 11|)(|10\rangle - |01\rangle) = \tfrac{1}{2}(0+0) = 0.$$

Pairs with $M_1 = Y$

$$(Y \otimes I)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(i\,|1\rangle\otimes|0\rangle + (-i)\,|0\rangle\otimes|1\rangle) = \tfrac{1}{\sqrt{2}}(i\,|10\rangle - i\,|01\rangle),$$
$$\langle\beta_{00}|\,(Y \otimes I)\,|\beta_{00}\rangle = \tfrac{1}{2}(\langle 00|+\langle 11|)(i\,|10\rangle - i\,|01\rangle) = \tfrac{1}{2}(0+0) = 0.$$

$$(Y \otimes X)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(i\,|1\rangle\otimes|1\rangle + (-i)\,|0\rangle\otimes|0\rangle) = \tfrac{1}{\sqrt{2}}(i\,|11\rangle - i\,|00\rangle),$$
$$\langle\beta_{00}|\,(Y \otimes X)\,|\beta_{00}\rangle = \tfrac{1}{2}(\langle 00|+\langle 11|)(i\,|11\rangle - i\,|00\rangle) = \tfrac{1}{2}(-i+i) = 0.$$

$$(Y \otimes Y)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(i\,|1\rangle\otimes i\,|1\rangle + (-i)\,|0\rangle\otimes(-i)\,|0\rangle) = \tfrac{1}{\sqrt{2}}(-|11\rangle - |00\rangle),$$
$$\langle\beta_{00}|\,(Y \otimes Y)\,|\beta_{00}\rangle = \tfrac{1}{2}(\langle 00|+\langle 11|)(-|00\rangle - |11\rangle) = \tfrac{1}{2}(-1-1) = -1.$$

$$(Y \otimes Z)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(i\,|1\rangle\otimes|0\rangle + (-i)\,|0\rangle\otimes(-|1\rangle)) = \tfrac{1}{\sqrt{2}}(i\,|10\rangle + i\,|01\rangle),$$
$$\langle\beta_{00}|\,(Y \otimes Z)\,|\beta_{00}\rangle = \tfrac{1}{2}(\langle 00|+\langle 11|)(i\,|10\rangle + i\,|01\rangle) = \tfrac{1}{2}(0+0) = 0.$$

Pairs with $M_1 = Z$

$$(Z \otimes I)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle + (-|1\rangle)\otimes|1\rangle) = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$\langle\beta_{00}|\,(Z \otimes I)\,|\beta_{00}\rangle = \tfrac{1}{2}(\langle 00|+\langle 11|)(|00\rangle - |11\rangle) = \tfrac{1}{2}(1-1) = 0.$$

$$(Z \otimes X)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle\otimes|1\rangle + (-|1\rangle)\otimes|0\rangle) = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$
$$\langle\beta_{00}|\,(Z \otimes X)\,|\beta_{00}\rangle = \tfrac{1}{2}(\langle 00|+\langle 11|)(|01\rangle - |10\rangle) = \tfrac{1}{2}(0+0) = 0.$$

$$(Z \otimes Y)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle\otimes i\,|1\rangle + (-|1\rangle)\otimes(-i)\,|0\rangle) = \tfrac{1}{\sqrt{2}}(i\,|01\rangle + i\,|10\rangle),$$
$$\langle\beta_{00}|\,(Z \otimes Y)\,|\beta_{00}\rangle = \tfrac{1}{2}(\langle 00|+\langle 11|)(i\,|01\rangle + i\,|10\rangle) = \tfrac{1}{2}(0+0) = 0.$$

$$(Z \otimes Z)\,|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle + (-|1\rangle)\otimes(-|1\rangle)) = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$
$$\langle\beta_{00}|\,(Z \otimes Z)\,|\beta_{00}\rangle = \tfrac{1}{2}(\langle 00|+\langle 11|)(|00\rangle + |11\rangle) = \tfrac{1}{2}(1+1) = 1.$$

A.2 Combined Decomposition Terms (Example 2.2.2)

We expand each nonzero Pauli pair from equation (0.6) via the spectral decomposition. For each pair, $p_{i\vec{l}} = \alpha_i \cdot \lambda_{i_1}^{l_1} \cdot \lambda_{i_2}^{l_2}$.

From $I \otimes I$ ($\alpha_{II} = \frac{1}{4}$)

Since all eigenvalues of I are $+1$, every $p_{i\vec{l}} = \frac{1}{4}$.

$$\vec{l} = (1,1)\colon\ \tfrac{1}{4}(+1)(+1)\ |0\rangle\langle 0| \otimes |0\rangle\langle 0| = \tfrac{1}{4}\ |0\rangle\langle 0| \otimes |0\rangle\langle 0|$$
$$\vec{l} = (1,2)\colon\ \tfrac{1}{4}(+1)(+1)\ |0\rangle\langle 0| \otimes |1\rangle\langle 1| = \tfrac{1}{4}\ |0\rangle\langle 0| \otimes |1\rangle\langle 1|$$
$$\vec{l} = (2,1)\colon\ \tfrac{1}{4}(+1)(+1)\ |1\rangle\langle 1| \otimes |0\rangle\langle 0| = \tfrac{1}{4}\ |1\rangle\langle 1| \otimes |0\rangle\langle 0|$$
$$\vec{l} = (2,2)\colon\ \tfrac{1}{4}(+1)(+1)\ |1\rangle\langle 1| \otimes |1\rangle\langle 1| = \tfrac{1}{4}\ |1\rangle\langle 1| \otimes |1\rangle\langle 1|$$

From $X \otimes X$ ($\alpha_{XX} = \frac{1}{4}$)

The eigenvalues of X are $+1$ and -1.

$$\begin{aligned}
\vec{l} = (1,1)\colon&\ \tfrac{1}{4}(+1)(+1)\ |+\rangle\langle+| \otimes |+\rangle\langle+| = \tfrac{1}{4}\ |+\rangle\langle+| \otimes |+\rangle\langle+| \\
\vec{l} = (1,2)\colon&\ \tfrac{1}{4}(+1)(-1)\ |+\rangle\langle+| \otimes |-\rangle\langle-| = -\tfrac{1}{4}\ |+\rangle\langle+| \otimes |-\rangle\langle-| \\
\vec{l} = (2,1)\colon&\ \tfrac{1}{4}(-1)(+1)\ |-\rangle\langle-| \otimes |+\rangle\langle+| = -\tfrac{1}{4}\ |-\rangle\langle-| \otimes |+\rangle\langle+| \\
\vec{l} = (2,2)\colon&\ \tfrac{1}{4}(-1)(-1)\ |-\rangle\langle-| \otimes |-\rangle\langle-| = \tfrac{1}{4}\ |-\rangle\langle-| \otimes |-\rangle\langle-|
\end{aligned}$$

From $Y \otimes Y$ ($\alpha_{YY} = -\frac{1}{4}$)

The eigenvalues of Y are $+1$ and -1.

$$\begin{aligned}
\vec{l} = (1,1)\colon&\ (-\tfrac{1}{4})(+1)(+1)\ |i\rangle\langle i| \otimes |i\rangle\langle i| = -\tfrac{1}{4}\ |i\rangle\langle i| \otimes |i\rangle\langle i| \\
\vec{l} = (1,2)\colon&\ (-\tfrac{1}{4})(+1)(-1)\ |i\rangle\langle i| \otimes |-i\rangle\langle -i| = \tfrac{1}{4}\ |i\rangle\langle i| \otimes |-i\rangle\langle -i| \\
\vec{l} = (2,1)\colon&\ (-\tfrac{1}{4})(-1)(+1)\ |-i\rangle\langle -i| \otimes |i\rangle\langle i| = \tfrac{1}{4}\ |-i\rangle\langle -i| \otimes |i\rangle\langle i| \\
\vec{l} = (2,2)\colon&\ (-\tfrac{1}{4})(-1)(-1)\ |-i\rangle\langle -i| \otimes |-i\rangle\langle -i| = -\tfrac{1}{4}\ |-i\rangle\langle -i| \otimes |-i\rangle\langle -i|
\end{aligned}$$

From $Z \otimes Z$ ($\alpha_{ZZ} = \frac{1}{4}$)

The eigenvalues of Z are $+1$ and -1.

$$\begin{aligned}
\vec{l} = (1,1)\colon&\ \tfrac{1}{4}(+1)(+1)\ |0\rangle\langle 0| \otimes |0\rangle\langle 0| = \tfrac{1}{4}\ |0\rangle\langle 0| \otimes |0\rangle\langle 0| \\
\vec{l} = (1,2)\colon&\ \tfrac{1}{4}(+1)(-1)\ |0\rangle\langle 0| \otimes |1\rangle\langle 1| = -\tfrac{1}{4}\ |0\rangle\langle 0| \otimes |1\rangle\langle 1| \\
\vec{l} = (2,1)\colon&\ \tfrac{1}{4}(-1)(+1)\ |1\rangle\langle 1| \otimes |0\rangle\langle 0| = -\tfrac{1}{4}\ |1\rangle\langle 1| \otimes |0\rangle\langle 0| \\
\vec{l} = (2,2)\colon&\ \tfrac{1}{4}(-1)(-1)\ |1\rangle\langle 1| \otimes |1\rangle\langle 1| = \tfrac{1}{4}\ |1\rangle\langle 1| \otimes |1\rangle\langle 1|
\end{aligned}$$

A.3 Reduction of the let Term (Example 2.7.1)

After applying the let reduction rule to let $x^{\otimes 2} = \beta_{00}$ in x_2 and dropping the vacuous substitution on x_1, the 16 terms (grouped by Pauli pair) are:

$$\begin{aligned}
&\tfrac{1}{4}|0\rangle\langle 0| + \tfrac{1}{4}|1\rangle\langle 1| + \tfrac{1}{4}|0\rangle\langle 0| + \tfrac{1}{4}|1\rangle\langle 1| \\
&+ \tfrac{1}{4}|+\rangle\langle +| - \tfrac{1}{4}|-\rangle\langle -| - \tfrac{1}{4}|+\rangle\langle +| + \tfrac{1}{4}|-\rangle\langle -| \\
&- \tfrac{1}{4}|i\rangle\langle i| + \tfrac{1}{4}|-i\rangle\langle -i| + \tfrac{1}{4}|i\rangle\langle i| - \tfrac{1}{4}|-i\rangle\langle -i| \\
&+ \tfrac{1}{4}|0\rangle\langle 0| - \tfrac{1}{4}|1\rangle\langle 1| - \tfrac{1}{4}|0\rangle\langle 0| + \tfrac{1}{4}|1\rangle\langle 1|
\end{aligned} \tag{A.1}$$

Collecting coefficients of equal density matrices:

$$\begin{aligned}
|0\rangle\langle 0|\colon&\quad \tfrac{1}{4} + \tfrac{1}{4} + \tfrac{1}{4} - \tfrac{1}{4} = \tfrac{1}{2} \\
|1\rangle\langle 1|\colon&\quad \tfrac{1}{4} + \tfrac{1}{4} - \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2} \\
|+\rangle\langle +|\colon&\quad \tfrac{1}{4} - \tfrac{1}{4} = 0 \\
|-\rangle\langle -|\colon&\quad \tfrac{1}{4} - \tfrac{1}{4} = 0 \\
|i\rangle\langle i|\colon&\quad \tfrac{1}{4} - \tfrac{1}{4} = 0 \\
|-i\rangle\langle -i|\colon&\quad \tfrac{1}{4} - \tfrac{1}{4} = 0
\end{aligned}$$

Appendix B

FULL DEFINITION OF THE EXTENDED CALCULUS

This appendix collects the complete formal definition of the extended λ°_ρ calculus in one place, for easy reference. The base calculus is from [2]; the let extension is developed in Chapter 2.

B.1 Types

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

where $m \leq n \in \mathbb{N}$. The type n is the type of an n-qubit density matrix; (m,n) is the measurement type produced by measuring m qubits of an n-qubit system; and $A \multimap B$ is the linear function type.

B.2 Terms

$t := x \mid \lambda x.t \mid tt$	(Standard lambda calculus)
$\mid \rho^n \mid U^n t \mid \pi^n t \mid t \otimes t$	(Quantum postulates)
$\mid \sum_{i=1}^{n} p_i t_i \mid \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t,\ldots,t\}$	(Probabilistic control)
$\mid \mathsf{let}\ x^{\otimes n} = \rho\ \mathsf{in}\ t$	(Compositional decomposition)

where $p_i \in (0,1]$, $\sum_{i=1}^{n} p_i = 1$, and $\sum$ is considered modulo associativity and commutativity.

Tab. B.1: Extended grammar of λ°_ρ.

The new construct $\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ t$ binds n variables $x_1,\ldots,x_n$, each of type 1, in the body t. The superscript $\otimes n$ indicates that x is decomposed into n tensor components via the combined Pauli spectral decomposition (Section 2.2).

B.3 Rewrite System

The reduction relation $\to$ consists of the base rules (Table B.2) and their contextual closure (Table B.3). The λ-body reduction rule $\dfrac{t \to r}{\lambda x.t \to \lambda x.r}$ is deliberately excluded from the extended calculus (see Section 2.3 of Chapter 2).

B.4 Type System

The type system is affine: every variable may be used at most once, which reflects the no-cloning theorem.

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

$$\mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \to \sum_i p_i t_i[\rho_i^n/x] \qquad \text{with} \begin{cases} \rho_i^n = \dfrac{\overline{\pi_i}\rho^n\overline{\pi_i}^\dagger}{p_i} \\ p_i = \mathsf{tr}(\overline{\pi_i}^\dagger\overline{\pi_i}\rho^n) \end{cases}$$

$$U^m\rho^n \to \rho'^n \qquad \text{with } \rho'^n = \overline{U^m}\rho^n\overline{U^m}^\dagger$$

$$\rho \otimes \rho' \to \rho'' \qquad \text{with } \rho'' = \rho \otimes \rho'$$

$$\sum_i p_i\rho_i \to \rho' \qquad \text{with } \rho' = \sum_i p_i\rho_i$$

$$\sum_i p_i t \to t$$

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

$$\mathsf{letcase}^\circ\ x = \sum_j q_j w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \ \to \sum_j q_j\, \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$$

$$\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s \to \sum_{i=1}^{4^n} \sum_{\vec{l}\in\{1,2\}^n} p_{i\vec{l}}\, s[\gamma_{i_1}^{l_1}/x_1, \cdots, \gamma_{i_n}^{l_n}/x_n]$$

where $p_{i\vec{l}} = \alpha_i(\rho^n)\prod_{k=1}^n \lambda_{i_k}^{l_k}$, and $\gamma_{i_k}^{l_k}$, $\lambda_{i_k}^{l_k}$ are the eigenprojectors and eigenvalues of the k-th Pauli factor of P_i, as in the combined decomposition (2.1).

Tab. B.2: Reduction rules of the extended λ_ρ°.

B.5 Denotational Semantics

The simplified interpretation of Section 2.6, which drops the measurement-outcome bookkeeping of [2].

Semantic Domains

$$\begin{aligned} [\![n]\!] &= \mathcal{D}_n && \text{(density matrices on } \mathbb{C}^{2^n}) \\ [\![(m,n)]\!] &= \mathcal{D}_n && \text{(measurement type, same domain)} \\ [\![A \multimap B]\!] &= \mathsf{CPM}([\![A]\!], [\![B]\!]) && \text{(completely positive maps)} \end{aligned}$$

Interpretation of Terms

Let θ be a valuation assigning semantic values to free variables.

$$\begin{aligned} [\![x]\!]_\theta &= \theta(x) \\ [\![\lambda x.t]\!]_\theta &= \rho \mapsto [\![t]\!]_{\theta, x\mapsto\rho} \\ [\![t\ r]\!]_\theta &= [\![t]\!]_\theta([\![r]\!]_\theta) \end{aligned}$$

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

$$\frac{t \to r}{t \otimes s \to r \otimes s} \qquad \frac{t \to r}{s \otimes t \to s \otimes r} \qquad \frac{t_j \to r_j}{\sum_{i=1}^n p_i t_i \to \sum_{i=1}^n p_i r_i} \ (\forall i \neq j,\ t_i = r_i)$$

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

$$\frac{t \to r}{\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s \to \mathsf{let}\ x^{\otimes n} = r\ \mathsf{in}\ s} \qquad \frac{t \to r}{\mathsf{let}\ x^{\otimes n} = s\ \mathsf{in}\ t \to \mathsf{let}\ x^{\otimes n} = s\ \mathsf{in}\ r}$$

Tab. B.3: Contextual rules of the extended λ°_ρ.

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

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

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

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

$$\frac{\Gamma \vdash t : n \quad \Delta, x_1 : 1, \ldots, x_n : 1 \vdash s : A}{\Gamma, \Delta \vdash \mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s : A}\ \mathsf{let}$$

Tab. B.4: Type system of the extended λ°_ρ.

$$\begin{aligned}
[\![\rho^n]\!]_\theta &= \rho^n \\
[\![U^m t]\!]_\theta &= \overline{U^m}\,[\![t]\!]_\theta\,\overline{U^m}^\dagger \\
[\![t \otimes r]\!]_\theta &= [\![t]\!]_\theta \otimes [\![r]\!]_\theta \\
[\![\pi^m t]\!]_\theta &= \textstyle\sum_{i=0}^{2^m-1} \overline{\pi_i}\,[\![t]\!]_\theta\,\overline{\pi_i}^\dagger \\
[\![\sum_i p_i t_i]\!]_\theta &= \sum_i p_i\,[\![t_i]\!]_\theta
\end{aligned}$$

For $\mathsf{letcase}^\circ$, let $p_i = \mathsf{tr}(\overline{\pi_i}^\dagger \overline{\pi_i}\,[\![r]\!]_\theta)$ and $\rho_i = \overline{\pi_i}\,[\![r]\!]_\theta\,\overline{\pi_i}^\dagger / p_i$. Then:

$$[\![\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}]\!]_\theta = \sum_{i=0}^{2^m-1} p_i \cdot [\![t_i]\!]_{\theta, x \mapsto \rho_i}.$$

For the let construct, let $\mathcal{P}_n = \{P_i\}_{i=1}^{4^n}$ be the n-qubit Pauli basis (0.4.1), and for each $P_i = M_{i_1} \otimes \cdots \otimes M_{i_n}$, let $\gamma^l_{i_k}$ and $\lambda^l_{i_k}$ denote the eigenprojectors and eigenvalues of M_{i_k} for $l \in \{1, 2\}$. Define $\alpha_i(\rho) = \frac{1}{2^n}\mathsf{tr}(P_i \cdot \rho)$. Then:

$$\begin{aligned}
&[\![\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s]\!]_\theta \\
&\quad = \sum_{i=1}^{4^n} \sum_{\vec{l} \in \{1,2\}^n} \Big(\alpha_i([\![t]\!]_\theta) \prod_{k=1}^n \lambda_{i_k}^{l_k}\Big) [\![s]\!]_{\theta,\, x_1 \mapsto \gamma_{i_1}^{l_1},\, \ldots,\, x_n \mapsto \gamma_{i_n}^{l_n}}.
\end{aligned}$$

Appendix C

SPECTRAL DECOMPOSITION OF THE PAULI MATRICES

We compute the spectral decomposition of each of the four Pauli matrices explicitly. In each case, we find the eigenvalues and an orthonormal basis of eigenvectors, and verify that $M = \sum_i \lambda_i |v_i\rangle\langle v_i|$.

C.1 Identity I

The identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has eigenvalue $\lambda = 1$ with multiplicity 2. The standard basis vectors $|0\rangle$ and $|1\rangle$ are eigenvectors, so:

$$I = 1 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1|.$$

C.2 Pauli Z

The matrix $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is already diagonal. Reading off the diagonal:

- Eigenvalue $\lambda_1 = +1$ with eigenvector $|0\rangle$.
- Eigenvalue $\lambda_2 = -1$ with eigenvector $|1\rangle$.

Verification. The characteristic polynomial is $\det(Z - \lambda I) = (1 - \lambda)(-1 - \lambda) = 0$, giving $\lambda = \pm 1$. The spectral decomposition is:

$$Z = (+1)|0\rangle\langle 0| + (-1)|1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z. \quad \checkmark$$

C.3 Pauli X

The matrix $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

The characteristic polynomial is $\det(X - \lambda I) = \lambda^2 - 1 = 0$, giving eigenvalues $\lambda = \pm 1$.

For $\lambda_1 = +1$: solving $(X - I)v = 0$ gives $\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} v = 0$, so $v_1 = v_2$. The normalized eigenvector is $|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

For $\lambda_2 = -1$: solving $(X + I)v = 0$ gives $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} v = 0$, so $v_1 = -v_2$. The normalized eigenvector is $|-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

Verification.

$$(+1)|+\rangle\langle +| + (-1)|-\rangle\langle -| = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X. \quad \checkmark$$

C.4 Pauli Y

The matrix $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$.

The characteristic polynomial is $\det(Y - \lambda I) = \lambda^2 - 1 = 0$, giving eigenvalues $\lambda = \pm 1$.

For $\lambda_1 = +1$: solving $(Y - I)v = 0$ gives $\begin{pmatrix} -1 & -i \\ i & -1 \end{pmatrix} v = 0$. From the first row: $v_1 = -iv_2$, so $v = \begin{pmatrix} -i \\ 1 \end{pmatrix}$ up to normalization. The normalized eigenvector is $|i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} -i \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(-i\,|0\rangle + |1\rangle) = \frac{-i}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$.

It is conventional to write $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ (absorbing the global phase $-i$, which does not affect the projector $|i\rangle\langle i|$). With this convention:

$$|i\rangle\langle i| = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}.$$

For $\lambda_2 = -1$: solving $(Y + I)v = 0$ gives $\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} v = 0$. From the first row: $v_1 = iv_2$. With the convention $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$:

$$|-i\rangle\langle -i| = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}.$$

Verification.

$$(+1)|i\rangle\langle i| + (-1)|-i\rangle\langle -i| = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} - \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$$
$$= \frac{1}{2}\begin{pmatrix} 0 & -2i \\ 2i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = Y. \quad \checkmark$$

Appendix D

FULL PROOFS

This appendix contains the complete proofs of theorems stated in Chapter 3. Throughout, we assume standard weakening and strengthening properties for the affine type system.

D.1 Proof of Lemma 3.2.1 (Substitution)

Proof. By induction on t.

- Let $t = x$. Then $B = A$. By weakening, $\Gamma, \Delta \vdash r : A$. Notice that $t[r/x] = r$.
- Let $t = y$. Then, by weakening and strengthening, $\Gamma, \Delta \vdash y : B$. Notice that $t[r/x] = y$.
- Let $t = \lambda y.s$. Then $B = C \multimap D$ and, by inversion, $\Gamma, x : A, y : C \vdash s : D$. Then, by the induction hypothesis, $\Gamma, y : C, \Delta \vdash s[r/x] : D$, so, by rule $\multimap_i$, $\Gamma, \Delta \vdash \lambda y.(s[r/x]) : C \multimap D$. Notice that $\lambda y.(s[r/x]) = (\lambda y.s)[r/x]$.
- Let $t = t_1 t_2$. Then $\Gamma, x : A = \Gamma_1, \Gamma_2$, with $\Gamma_1 \vdash t_1 : C \multimap B$ and $\Gamma_2 \vdash t_2 : C$.
  - If $x : A \in \Gamma_1$, then, by the induction hypothesis $\Gamma_1 \setminus \{x : A\}, \Delta \vdash t_1[r/x] : C \multimap B$, so by rule $\multimap_e$, $\Gamma_1 \setminus \{x : A\}, \Gamma_2, \Delta \vdash t_1[r/x]t_2 : B$. Notice that $\Gamma_1 \setminus \{x : A\}, \Gamma_2 = \Gamma$ and $t_1[r/x]t_2 = (t_1 t_2)[r/x]$.
  - If $x : A \in \Gamma_2$, then, by the induction hypothesis $\Gamma_2 \setminus \{x : A\}, \Delta \vdash t_2[r/x] : C$, so by rule $\multimap_e$, $\Gamma_1, \Gamma_2 \setminus \{x : A\}, \Delta \vdash t_1(t_2[r/x]) : B$. Notice that $\Gamma_1, \Gamma_2 \setminus \{x : A\} = \Gamma$ and $t_1(t_2[r/x]) = (t_1 t_2)[r/x]$.
- Let $t = \rho^n$. Then $B = n$. By weakening and strengthening, $\Gamma, \Delta \vdash \rho^n : n$. Notice that $t[r/x] = \rho^n$.
- Let $t = U^m s$. Then $B = n$ and $\Gamma, x : A \vdash s : n$. Then, by the induction hypothesis, $\Gamma, \Delta \vdash s[r/x] : n$. So, by rule u, $\Gamma, \Delta \vdash U^m(s[r/x]) : n$. Notice that $U^m(s[r/x]) = (U^m s)[r/x]$.
- Let $t = \pi^m s$. Then $B = (m, n)$ and $\Gamma, x : A \vdash s : n$. Then, by the induction hypothesis, $\Gamma, \Delta \vdash s[r/x] : n$. So, by rule m, $\Gamma, \Delta \vdash \pi^m(s[r/x]) : (m, n)$. Notice that $\pi^m(s[r/x]) = (\pi^m s)[r/x]$.
- Let $t = t_1 \otimes t_2$. Then $B = n_1 + n_2$, $\Gamma, x : A = \Gamma_1, \Gamma_1$ with $\Gamma_i \vdash t_i : n_i$ for $i = 1, 2$. Let $x : A \in \Gamma_i$ for some $i = 1, 2$. Then, by the induction hypothesis, $\Gamma_i \setminus \{x : A\}, \Delta \vdash t_i[r/x]$, so by rule $\otimes$, either $\Gamma, \Delta \vdash t_1[r/x] \otimes t_2 : n_1 + n_2$, or $\Gamma, \Delta \vdash t_1 \otimes t_2[r/x] : n_1 + n_2$. In the first case, notice that $t_1[r/x] \otimes t_2 = (t_1 \otimes t_2)[r/x]$, and in the second, $t_1 \otimes t_2[r/x] = (t_1 \otimes t_2)[r/x]$.
- Let $t = \sum_i p_i t_i$. Then $\Gamma, x : A \vdash t_i : B$ and so, by the induction hypothesis, $\Gamma, \Delta \vdash t_i[r/x] : B$. Therefore, by rule $+$, $\Gamma, \Delta \vdash \sum_i p_i t_i[r/x] : B$. Notice that $\sum_i p_i t_i[r/x] = (\sum_i p_i t_i)[r/x]$.

- Let $t = \mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$. $y : n \vdash t_i : B$, for $i = 0, \ldots, 2^m - 1$, and, $\Gamma \vdash s : (m, n)$. By the induction hypothesis, $\Gamma, \Delta \vdash s[r/x] : (m, n)$. So, by rule lc, $\Gamma, \Delta \vdash \mathsf{letcase}^\circ\ y = s[r/x]\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$: B. Notice that $(\mathsf{letcase}^\circ\ y = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\})[r/x] = \mathsf{letcase}^\circ\ y = s[r/x]\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$.

- Let $t = \mathsf{let}\ y^{\otimes n} = s\ \mathsf{in}\ u$. Then $\Gamma, x : A = \Gamma_1, \Gamma_2$ with $\Gamma_1 \vdash s : n$ and $\Gamma_2, y_1 : 1, \ldots, y_n : 1 \vdash u : B$.

  - If $x : A \in \Gamma_1$, then by the induction hypothesis, $\Gamma_1 \setminus \{x : A\}, \Delta \vdash s[r/x] : n$. Since $x \notin FV(u)$, we have $u[r/x] = u$. By rule let, $\Gamma_1 \setminus \{x : A\}, \Gamma_2, \Delta \vdash \mathsf{let}\ y^{\otimes n} = s[r/x]\ \mathsf{in}\ u : B$.
  - If $x : A \in \Gamma_2$, then by the induction hypothesis, $\Gamma_2 \setminus \{x : A\}, \Delta, y_1 : 1, \ldots, y_n : 1 \vdash u[r/x] : B$. Since $x \notin FV(s)$, we have $s[r/x] = s$. By rule let, $\Gamma_1, \Gamma_2 \setminus \{x : A\}, \Delta \vdash \mathsf{let}\ y^{\otimes n} = s\ \mathsf{in}\ u[r/x] : B$.

□

D.2 Proof of Theorem 3.3.1 (Subject Reduction)

Proof.

- Let $t = (\lambda x.t')s$, $r = t'[s/x]$. Then $\Gamma \vdash (\lambda x.t')s : A$, so, $\Gamma_1 \vdash \lambda x.t' : B \multimap A$ and $\Gamma_2 \vdash s : B$, with $\Gamma = \Gamma_1, \Gamma_2$. Hence, $\Gamma_1, x : B \vdash t' : A$, and so, by Lemma 3.2.1, $\Gamma \vdash t'[s/x] : A$.

- Let $t = U^m \rho^n$, $r = \rho'^n$, with $\rho'^n = \overline{U^m} \rho^n \overline{U^m}^\dagger$. Then $A = n$. By rule ax_ρ, $\Gamma \vdash \rho'^n : n$.

- Let $t = \rho_1^n \otimes \rho_2^m$ and $r = \rho$, with $\rho = \rho_1^n \otimes \rho_2^m$. Then, $A = n + m$, with $\vdash \rho_1^n : n$ and $\vdash \rho_2^m : m$. Since ρ is a density matrix of $(n + m)$-qubits, $\vdash \rho : n + m$.

- Let $t = \mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$ and $r = \sum_i p_i t_i[\rho_i^n/x]$, with $\rho_i^n = \frac{\overline{\pi_i} \rho^n \overline{\pi_i}^\dagger}{p_i}$ and $p_i = \mathsf{tr}(\overline{\pi_i}^\dagger \overline{\pi_i} \rho^n)$. Then $\Gamma \vdash \pi^m \rho^n : (m, n)$ and $x : n \vdash t_i : A$. By Lemma 3.2.1, $\Gamma \vdash t_i[\rho_i^n/x] : A$, then, by rule $+$, $\Gamma \vdash \sum_i p_i t_i[\rho_i^n/x] : A$.

- Let $t = \mathsf{letcase}^\circ\ x = \sum_j q_j w_j\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}$ and $r = \sum_j q_j\, \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}$. By inversion of rule lc, $\Gamma \vdash \sum_j q_j w_j : (m, n)$ and $x : n \vdash s_i : A$ for each i. By rule $+$, each $w_j : (m, n)$. Applying rule lc to each w_j gives $\Gamma \vdash \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\} : A$, and then rule $+$ gives $\Gamma \vdash r : A$.

- Let $t = \sum_i p_i \rho_i$ and $r = \rho'$, with $\rho' = \sum_i p_i \rho_i$. Then, $\Gamma \vdash \sum_i p_i \rho_i : n$, and by rule ax_ρ, $\Gamma \vdash \rho' : n$.

- Let $t = \sum_i p_i r$. Then, $\Gamma \vdash r : A$.

- Let $t = (\sum_i p_i t_i) r$ and $\sum_i p_i (t_i r)$. Then, $\Gamma = \Gamma_1, \Gamma_2$, $\Gamma_1 \vdash t_i : B \multimap A$ and $\Gamma_2 \vdash r : B$. Therefore, by rule $\multimap_e$, $\Gamma_1, \Gamma_2 \vdash t_i r : A$, and by rule $+$, $\Gamma_1, \Gamma_2 \vdash \sum_i p_i (t_i r) : A$.

- Let $t = \mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s$ and $r = \sum_{i=1}^{4^n} \sum_{\vec{l} \in \{1,2\}^n} p_{i\vec{l}}\, s[\gamma_{i_1}^{l_1}/x_1, \cdots, \gamma_{i_n}^{l_n}/x_n]$, where $p_{i\vec{l}}$ are the combined decomposition coefficients. We have $\Gamma, \Delta \vdash \mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s : A$. By inversion, $\Gamma \vdash \rho^n : n$ and $\Delta, x_1 : 1, \ldots, x_n : 1 \vdash s : A$.
  As each $\gamma_{i_k}^{l_k}$ is a 1-qubit density matrix by construction, by rule ax_ρ we have $\vdash \gamma_{i_k}^{l_k} : 1$.

Then, by repeated application of Lemma 3.2.1, we have that $\Delta \vdash s[\gamma_{i_1}^{l_1}/x_1, \cdots, \gamma_{i_n}^{l_n}/x_n] : A$. Since the Pauli decomposition preserves trace, we have that $\sum_{i=1}^{4^n} \sum_{\vec{l} \in \{1,2\}^n} p_{i\vec{l}} = 1$. Then, by rule $+$, we have $\Gamma, \Delta \vdash \sum_{i=1}^{4^n} \sum_{\vec{l} \in \{1,2\}^n} p_{i\vec{l}} s[\gamma_{i_1}^{l_1}/x_1, \cdots, \gamma_{i_n}^{l_n}/x_n] : A$.

- Contextual cases: Let $s \to s'$, then
  - Consider $t = t's$ and $r = t's'$. Then $\Gamma = \Gamma_1, \Gamma_2$, with $\Gamma_1 \vdash t' : B \multimap A$ and $\Gamma_2 \vdash s : B$. By the induction hypothesis, $\Gamma_2 \vdash s' : B$, so by rule $\multimap_e$, $\Gamma \vdash t's' : A$.
  - Consider $t = st'$ and $r = s't'$. Then $\Gamma = \Gamma_1, \Gamma_2$, with $\Gamma_1 \vdash s : B \multimap A$ and $\Gamma_2 \vdash t' : B$. By the induction hypothesis, $\Gamma_1 \vdash s' : B \multimap A$, so by rule $\multimap_e$, $\Gamma \vdash s't' : A$.
  - Consider $t = U^m s$ and $r = U^m s'$. Then $A = n$ and $\Gamma \vdash s : n$. By the induction hypothesis $\Gamma \vdash s' : n$, so by rule u, $\Gamma \vdash U^m s' : n$.
  - Consider $t = \pi^m s$ and $r = \pi^m s'$. Then $A = (m, n)$ and $\Gamma \vdash s : n$. By the induction hypothesis $\Gamma \vdash s' : n$, so by rule m, $\Gamma \vdash \pi^m s' : (m, n)$.
  - Consider $t = t' \otimes s$ and $r = t' \otimes s'$. Then $A = n + m$ and $\Gamma = \Gamma_1, \Gamma_2$, with $\Gamma_1 \vdash t' : n$ and $\Gamma_2 \vdash s : m$. By the induction hypothesis $\Gamma_2 \vdash s' : m$, so by rule $\otimes$, $\Gamma \vdash t' \otimes s' : n + m$.
  - Consider $t = s \otimes t'$ and $r = s' \otimes t'$. Then $A = n + m$ and $\Gamma = \Gamma_1, \Gamma_2$, with $\Gamma_1 \vdash s : n$ and $\Gamma_2 \vdash t' : m$. By the induction hypothesis $\Gamma_1 \vdash s' : n$, so by rule $\otimes$, $\Gamma \vdash s' \otimes t' : n + m$.
  - Consider $t = \mathsf{letcase}^\circ\ x = s\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$ and $r = \mathsf{letcase}^\circ\ x = s'\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$. Then $x : n \vdash t_i : A$ for $i = 0, \ldots, 2^m - 1$, and $\Gamma \vdash s : (m, n)$. By the induction hypothesis, $\Gamma \vdash s' : (m, n)$ and by rule lc, $\Gamma \vdash \mathsf{letcase}^\circ\ x = s'\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} : A$.
  - Consider $t = \sum_i p_i t_i$ and $r = \sum_i p_i r_i$, with $t_j \to r_j$, and $\forall i \neq j$, $t_i = r_i$. By inversion, $\Gamma \vdash t_i : A$. By the induction hypothesis, $\forall i$, $\Gamma \vdash r_i : A$. Then, by rule $+$, $\Gamma \vdash \sum_i p_i r_i : A$.
  - Consider $t = \mathsf{let}\ y^{\otimes n} = s\ \mathsf{in}\ u$ and $r = \mathsf{let}\ y^{\otimes n} = s'\ \mathsf{in}\ u$. Then $\Gamma = \Gamma_1, \Gamma_2$, with $\Gamma_1 \vdash s : n$ and $\Gamma_2, y_1 : 1, \ldots, y_n : 1 \vdash u : A$. By the induction hypothesis $\Gamma_1 \vdash s' : n$, so by rule let, $\Gamma \vdash \mathsf{let}\ y^{\otimes n} = s'\ \mathsf{in}\ u : A$.
  - Consider $t = \mathsf{let}\ y^{\otimes n} = u\ \mathsf{in}\ s$ and $r = \mathsf{let}\ y^{\otimes n} = u\ \mathsf{in}\ s'$. Then $\Gamma = \Gamma_1, \Gamma_2$, with $\Gamma_1 \vdash u : n$ and $\Gamma_2, y_1 : 1, \ldots, y_n : 1 \vdash s : A$. By the induction hypothesis $\Gamma_2, y_1 : 1, \ldots, y_n : 1 \vdash s' : A$, so by rule let, $\Gamma \vdash \mathsf{let}\ y^{\otimes n} = u\ \mathsf{in}\ s' : A$.

□

D.3 Proof of Theorem 3.4.2 (Progress)

Proof. We relax the hypotheses and prove the theorem for open terms as well. That is: If $\Gamma \vdash t : A$, then either t is a value, there exists r such that $t \to r$, or t contains a free variable, and t does not rewrite.

- Let $\Gamma, x : A \vdash x : A$ as a consequence of rule ax. Then, we are done since x is a free variable and does not rewrite.

- Let $\Gamma \vdash \lambda x.t : A \multimap B$ as a consequence of $\Gamma, x : A \vdash t : B$ and rule $\multimap_i$. Since reduction under λ is not part of the rewrite system, $\lambda x.t$ is always a value by Definition 3.4.1.

- Let $\Gamma, \Delta \vdash tr : B$ as a consequence of $\Gamma \vdash t : A \multimap B$, $\Delta \vdash r : A$ and rule $\multimap_e$. Then, by the induction hypothesis, one of the following cases happens:

  - There exists t' such that $t \to t'$, in which case $tr \to t'r$.
  - There exists r' such that $r \to r'$, in which case $tr \to tr'$.
  - t is a value and r does not rewrite. The only value[s] which can be typed by $A \multimap B$ are:
    - $t = x$, in which case xr contains a free variable and does not rewrite.
    - $t = \lambda x.v$, in which case $(\lambda x.v)r \to v[r/x]$.
    - $t = \sum_i p_i t_i$, where $\Gamma \vdash t_i : A \multimap B$. Then, $tr \to \sum_i p_i(t_i r)$.
  - t is not a value, contains a free variable, and does not rewrite, and r does not rewrite, in which case, if t is not a sum, tr contains a free variable and does not rewrite. If $t = \sum_i p_i t_i$ is a sum, $tr \to \sum_i p_i(t_i r)$.

- Let $\Gamma \vdash \rho^n : n$ as a consequence of rule ax_ρ. Then, we are done since ρ^n is a value.

- Let $\Gamma \vdash U^m t : n$ as a consequence of $\Gamma \vdash t : n$ and rule u. Then, by the induction hypothesis, one of the following cases happens:

  - t is a value. Since $\lambda x.v$ cannot be typed by n, the only value[s] that can be typed by n are either ρ^n, or they contain free variables:
    - Let $t = \rho^n$, then $U^m \rho^n \to \rho'$, with $\rho' = \overline{U^m} \rho^n \overline{U^m}^\dagger$.
    - Let t contain a free variable. Notice that it can only be either a free variable by itself, a tensor of value[s] containing free variables, or a linear combination of different value[s] containing free variables. In any case, t contains a free variable and does not rewrite. Hence, $U^m t$ contains a free variable and does not rewrite.
  - There exists r such that $t \to r$, in which case $U^m t \to U^m r$;
  - t contains a free variable and does not rewrite, in which case the same is true for $U^m t$.

- Let $\Gamma \vdash \pi^m t : (m, n)$ as a consequence of $\Gamma \vdash t : n$ and rule m. Then, by the induction hypothesis, one of the following cases happens:

  - t is a value. Then $\pi^m t$ is also a value and does not rewrite.
  - t contains a free variable and does not rewrite, in which case the same is true for $\pi^m t$.

- Let $\Gamma, \Delta, \vdash t \otimes r : n + m$ as a consequence of $\Gamma \vdash t : n$, $\Delta \vdash r : m$ and rule $\otimes$. Then, by the induction hypothesis, one of the following happens:

  - There exists t' such that $t \to t'$, in which case $t \otimes r \to t' \otimes r$.
  - There exists r' such that $r \to r'$, in which case $t \otimes r \to t \otimes r'$.

  - t is a value and r does not rewrite. The only value[s] that can be typed by n are either ρ^n, or they contain free variables.
    * Let $t = \rho^n$, then:
      · If $r = \rho^m$, $t \otimes r \to \rho'$, with $\rho' = \rho^n \otimes \rho^m$.
      · If r contains a free variable and does not rewrite, then the same is true for $t \otimes r$.
    * Let t contain a free variable. Then $t \otimes r$ contains a free variable and does not rewrite.
  - t contains a free variable and does not rewrite, and r does not rewrite, in which case $t \otimes r$ contains a free variable and does not rewrite.

- Let $\Gamma \vdash \mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} : A$ as a consequence of $x : n \vdash t_i : A$ for $i = 0, \ldots, 2^m - 1$, $\Gamma \vdash r : (m, n)$, and rule lc. By the induction hypothesis, the possible cases for r are:
  - $r = \pi^m \rho^n$ (a measurement value on a concrete density matrix). Then $\mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \to \sum_i p_i t_i[\rho_i^n/x]$ by the main $\mathsf{letcase}^\circ$ rule.
  - $r = \sum_j q_j w_j$ is a closed non-trivial linear combination of values $w_j : (m, n)$ (necessarily each $w_j = \pi^m \rho_j^n$). Then the distributing rule fires: $\mathsf{letcase}^\circ\ x = \sum_j q_j w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \to \sum_j q_j\, \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$.
  - r contains a free variable and does not rewrite, in which case the same is true for $\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$.
  - There exists r' such that $r \to r'$, in which case $\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\} \to \mathsf{letcase}^\circ\ x = r'\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$ by contextual closure.

- Let $\Gamma \vdash \sum_i p_i t_i : A$ as a consequence of $\Gamma \vdash t_i : A$, $\sum_i p_i = 1$, and rule $+$. If $\sum_i p_i t_i$ is a value, then we are done. If it is not a value, then one of the following cases is true:
  - $t_j = t_k$ for some $j \neq k$, in which case $\sum_i p_i t_i \to (\sum_{i \neq j,k} p_i t_i) + (p_j + p_k) t_j$.
  - At least one t_i is not a value. By the induction hypothesis, if t_i is not a value, either it rewrites, or it contains a free variable and does not rewrite. If at least one t_i rewrites, then $\sum_i p_i t_i$ rewrites. If none of these rewrites and at least one contains a free variable, then $\sum_i p_i t_i$ does not rewrite and contain a free variable.

- Let $\Gamma, \Delta \vdash \mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s : A$ as a consequence of $\Gamma \vdash t : n$, $\Delta, x_1 : 1, \ldots, x_n : 1 \vdash s : A$ and rule let. By induction, the possible cases for t are:
  - t is a value. Since $\lambda x.v$ cannot be typed by n, the only value[s] that can be typed by n are either ρ^n, or they contain free variables:
    * Let $t = \rho^n$, then $\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s \to \sum_{i=1}^{4^n} \sum_{l_1, \cdots, l_n \in \{1,2\}} p_{i\vec{l}}\, s[\gamma_{i_1}^{l_1}/x_1, \cdots, \gamma_{i_n}^{l_n}/x_n]$.
    * Let t contain a free variable. Notice that it can only be either a free variable by itself, a tensor of value[s] containing free variables, or a linear combination of different value[s] containing free variables. In any case, t contains a free variable and does not rewrite. Hence, $\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s$ contains a free variable and does not rewrite.

– There exists t' such that $t \to t'$, in which case $\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s \to \mathsf{let}\ x^{\otimes n} = t'\ \mathsf{in}\ s$.
– t contains a free variable and does not rewrite, in which case the same is true for $\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s$.

□

D.4 Proof of Theorem 3.5.1 (Strong Normalization)

The proof uses Girard's reducibility candidates method [4]: strong normalisation is established by defining typed reducibility sets $SN(A)$, proving a forward-closure lemma (Lemma D.4.3), establishing per-construct closure lemmas, and concluding by a fundamental substitution lemma.

Extended reduction relation

Following Díaz-Caro and Dowek [3], we augment the reduction relation with the following *projection rules*:

$$\textstyle\sum_i p_i\, t_i \ \to\ t_j \qquad \text{for any index } j.$$

These rules are not part of the operational semantics of the calculus; they are added solely for the purpose of the strong normalisation argument. Since the original reduction relation is a subset of the extended one, strong normalisation for the extended relation implies strong normalisation for the original.

The set SN and the typed sets $SN(A)$

Let SN denote the set of all terms that are strongly normalising under the extended relation. The *length* $\ell(t)$ of a term $t \in SN$ is the maximal length of any reduction sequence from t.

We define, by induction on the type A, a set $SN(A)$ of *reducible* terms of type A:

$$\begin{aligned} SN(n) &= SN, \\ SN((m,n)) &= SN, \\ SN(A \multimap B) &= \big\{\, t \in SN \;\big|\; t \to^* \lambda x.\, u \ \Rightarrow\ \forall v \in SN(A),\ u[v/x] \in SN(B) \,\big\}. \end{aligned}$$

Lemma D.4.1 (SN is closed under sums)**.** *If $t_1, \ldots, t_k \in SN$ then $\sum_i p_i\, t_i \in SN$.*

Proof. By induction on $\sum_i \ell(t_i)$ and then on the size of the term. Any one-step reduct of $\sum_i p_i\, t_i$ either reduces one summand (covered by the induction hypothesis on ℓ), applies a sum-collapse rule to produce a density matrix or a single term t (both in SN), or fires a projection rule to produce some t_j (in SN by assumption). In each case the reduct is in SN, so $\sum_i p_i\, t_i \in SN$. □

Definition D.4.2 (Neutral terms)**.** A term t is *neutral* if it is not a λ-abstraction and not a probabilistic sum.

Lemma D.4.3 (CR3: forward closure for neutral terms)**.** *Let t be neutral of type A. If every one-step reduct of t belongs to $SN(A)$, then $t \in SN(A)$.*

Proof. Since every one-step reduct of t is in $SN(A) \subseteq SN$, every reduction sequence from t is finite, so $t \in SN$.

For ground and measurement types $A \in \{n, (m, n)\}$, membership in $SN(A)$ is just membership in SN, which we just established.

For $A = B \multimap C$: suppose $t \to^* \lambda x.\, u$. Since t is neutral, the first step of this sequence goes $t \to t'$ for some reduct t', and $t' \to^* \lambda x.\, u$. By hypothesis, $t' \in SN(B \multimap C)$, so for any $v \in SN(B)$ we have $u[v/x] \in SN(C)$. Hence $t \in SN(B \multimap C)$. □

Per-construct closure lemmas

Lemma D.4.4 (Closed under sums in $SN(A)$)**.** *If $t_1, \ldots, t_k \in SN(A)$ then $\sum_i p_i\, t_i \in SN(A)$.*

Proof. By Lemma D.4.1, $\sum_i p_i\, t_i \in SN$. It remains to check the additional condition for function types. Suppose $A = B \multimap C$ and $\sum_i p_i\, t_i \to^* \lambda x.\, u$. By the projection rules, some t_j satisfies $t_j \to^* \lambda x.\, u$ (since the only reduction that produces a λ from a sum is via a summand). Since $t_j \in SN(B \multimap C)$, for any $v \in SN(B)$ we get $u[v/x] \in SN(C)$. Hence $\sum_i p_i\, t_i \in SN(B \multimap C)$. □

Lemma D.4.5 (Closed under λ-abstraction)**.** *If for all $v \in SN(A)$, $t[v/x] \in SN(B)$, then $\lambda x.\, t \in SN(A \multimap B)$.*

Proof. We check the two conditions in the definition of $SN(A \multimap B)$.

$\lambda x.\, t \in SN$. Since the calculus has no body reduction rule, $\lambda x.\, t$ is a normal form and hence trivially in SN.

Body condition. Since there is no body reduction rule, $\lambda x.\, t \to^* \lambda x.\, u$ implies $u = t$. So the condition reduces to: for all $v \in SN(A)$, $t[v/x] \in SN(B)$, which is exactly the hypothesis. □

Lemma D.4.6 (Closed under application)**.** *If $t \in SN(A \multimap B)$ and $s \in SN(A)$, then $t\, s \in SN(B)$.*

Proof. By induction on $\ell(t) + \ell(s)$ and Lemma D.4.3. The term $t\, s$ is neutral. We show every one-step reduct of $t\, s$ is in $SN(B)$, then conclude by CR3.

Reduction inside t or s. If $t \to t'$ then $t' \in SN(A \multimap B)$ (since $SN(A \multimap B)$ is downward closed: $t' \in SN$ because $t \in SN$, and the body condition transfers by transitivity of $\to^*$), and $\ell(t') < \ell(t)$, so the induction hypothesis gives $t'\, s \in SN(B)$. Symmetrically if $s \to s'$.

Both values, $t = \lambda x.\, u$. The rule $(\lambda x.\, u)\, s \to u[s/x]$ fires. Since $t \to^* \lambda x.\, u$ (zero steps) and $s \in SN(A)$, the body condition of $t \in SN(A \multimap B)$ gives $u[s/x] \in SN(B)$.

Both values, $t = \sum_i p_i\, t_i$. The distribution rule $(\sum_i p_i\, t_i)\, s \to \sum_i p_i\, (t_i\, s)$ fires. By the projection rules, $t \to t_i$ in the extended relation, so $\ell(t_i) < \ell(t)$ and $t_i \in SN(A \multimap B)$ (by downward closure). The induction hypothesis gives each $t_i\, s \in SN(B)$. Lemma D.4.4 then gives $\sum_i p_i\, (t_i\, s) \in SN(B)$.

In every case the one-step reduct is in $SN(B)$, so CR3 gives $t\, s \in SN(B)$. □

Lemma D.4.7 (Closed under unitary operation and measurement)**.** *If $t \in SN(n)$ then $U^m t \in SN(n)$ and $\pi^m t \in SN((m, n))$.*

Proof. Both $U^m t$ and $\pi^m t$ are neutral. Any reduction either applies inside t (giving a reduct in SN by the induction hypothesis on $\ell(t)$) or fires the outermost rule: $U^m \rho^n \to \rho'^n \in SN(n)$; and $\pi^m t$ has no outermost rule at all (it only participates in a reduction as the argument of $\mathsf{letcase}^\circ$, not by itself), so the first case always applies. By Lemma D.4.3, both terms are in the appropriate SN set. □

Lemma D.4.8 (Closed under tensor)**.** *If $t \in SN(m)$ and $s \in SN(n)$, then $t \otimes s \in SN(m+n)$.*

Proof. The term $t \otimes s$ is neutral. Reductions apply inside t or s (both stay in SN by induction), or fire the collapse rule $\rho_1^m \otimes \rho_2^n \to \rho^{m+n}$ (a density matrix, hence in $SN(m+n)$). Lemma D.4.3 gives the result. □

Lemma D.4.9 (Closed under $\mathsf{letcase}^\circ$)**.** *If $r \in SN((m,n))$ and, for all density matrices $\rho^n \in SN(n)$, $s_i[\rho^n/x] \in SN(A)$ for each i, then $\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\} \in SN(A)$.*

Proof. By induction on $\ell(r)$ and Lemma D.4.3. The term is neutral. If a reduction applies inside r, the induction hypothesis applies. If r is a closed value of type (m,n), there are two sub-cases (λ-abstractions cannot have measurement types):

- $r = \pi^m \rho^n$: the main $\mathsf{letcase}^\circ$ rule fires, giving $\sum_i p_i\, s_i[\rho_i^n/x]$. Each $\rho_i^n \in SN(n)$; by hypothesis each $s_i[\rho_i^n/x] \in SN(A)$; by Lemma D.4.4 the sum is in $SN(A)$.
- $r = \sum_j q_j (\pi^m \rho_j^n)$: the distributing rule fires, giving

$$\sum_j q_j\, \mathsf{letcase}^\circ\ x = \pi^m \rho_j^n\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}.$$

  Each $\pi^m \rho_j^n$ has smaller $\ell(r)$, so by the previous sub-case each summand is in $SN(A)$; by Lemma D.4.4 the sum is in $SN(A)$.

Lemma D.4.3 concludes. □

Lemma D.4.10 (Closed under let)**.** *If $t \in SN(n)$ and, for all density matrices $\gamma_k \in SN(1)$ ($k = 1, \ldots, n$), $s[\gamma_1/x_1, \ldots, \gamma_n/x_n] \in SN(A)$, then $\mathsf{let}\ x^{\otimes n} = t\ \mathsf{in}\ s \in SN(A)$.*

Proof. By induction on $\ell(t)$ and Lemma D.4.3. The term is neutral. If a reduction applies inside t, the induction hypothesis applies (the reduct t' still satisfies $t' \in SN(n)$ as a reduct of a strongly normalising term). If t is a value of ground type n, it must be a density matrix ρ^n (no λ- or π-value has type n). The main let rule fires:

$$\mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s\ \to\ \sum_{i,\vec{l}} p_{i\vec{l}}\, s[\gamma_{i_1}^{l_1}/x_1, \ldots, \gamma_{i_n}^{l_n}/x_n].$$

Each $\gamma_{i_k}^{l_k}$ is a density matrix, hence in $SN(1)$. By the hypothesis, each substituted body $s[\gamma_{i_1}^{l_1}/x_1, \ldots, \gamma_{i_n}^{l_n}/x_n]$ belongs to $SN(A)$. By Lemma D.4.4 the entire sum belongs to $SN(A)$. Lemma D.4.3 concludes.

If a reduction applies inside s instead, the body reduces to s' and the induction hypothesis on s (which inherits the same property because any density matrix substituted into s' also appeared in s) gives the result. □

Fundamental lemma

A *substitution* θ is *valid for* Γ, written $\theta \vDash \Gamma$, if $\theta(x) \in SN(A)$ for every $x : A \in \Gamma$.

Lemma D.4.11 (Fundamental lemma)**.** *If* $\Gamma \vdash t : A$ *and* $\theta \vDash \Gamma$*, then* $\theta(t) \in SN(A)$.

Proof. By induction on the typing derivation of $\Gamma \vdash t : A$.

- **Variable** $x : A \in \Gamma$. Then $\theta(x) \in SN(A)$ by hypothesis.
- **Density matrix** ρ^n. Then $\theta(\rho^n) = \rho^n$, which is a normal form, hence in $SN = SN(n)$.
- **λ-abstraction** $\lambda x.\, u$ of type $A \multimap B$. Let $v \in SN(A)$. Define $\theta' = (\theta, x \mapsto v)$; then $\theta' \vDash \Gamma, x : A$. By the induction hypothesis on u, $\theta'(u) = (\theta(u))[v/x] \in SN(B)$. By Lemma D.4.5, $\theta(\lambda x.\, u) = \lambda x.\, \theta(u) \in SN(A \multimap B)$.
- **Application** $t_1\, t_2$. By the induction hypotheses, $\theta(t_1) \in SN(A \multimap B)$ and $\theta(t_2) \in SN(A)$. Lemma D.4.6 gives $\theta(t_1\, t_2) \in SN(B)$.
- **Unitary** $U^m t$. By induction, $\theta(t) \in SN(n)$. Lemma D.4.7 gives $U^m\, \theta(t) \in SN(n)$.
- **Measurement** $\pi^m t$. Analogous, giving $\pi^m\, \theta(t) \in SN((m, n))$.
- **Tensor** $t_1 \otimes t_2$. By induction, $\theta(t_1) \in SN(m)$ and $\theta(t_2) \in SN(n)$. Lemma D.4.8 gives $\theta(t_1) \otimes \theta(t_2) \in SN(m + n)$.
- **Probabilistic sum** $\sum_i p_i\, u_i$. By induction, each $\theta(u_i) \in SN(A)$. Lemma D.4.4 gives $\theta(\sum_i p_i\, u_i) = \sum_i p_i\, \theta(u_i) \in SN(A)$.
- **Letcase** $\mathsf{letcase}^\circ\ x = r\ \mathsf{in}\ \{s_0, \ldots, s_{2^m-1}\}$. By induction, $\theta(r) \in SN((m, n))$. For any density matrix $\rho^n \in SN(n)$, define $\theta'' = (\theta, x \mapsto \rho^n)$; then $\theta'' \vDash \Gamma, x : n$, and the induction hypothesis gives each $\theta(s_i)[\rho^n/x] = \theta''(s_i) \in SN(A)$. Lemma D.4.9 gives the result.
- **Let** $\mathsf{let}\ x^{\otimes n} = u\ \mathsf{in}\ s$ with $\Gamma \vdash u : n$ and $\Delta, x_1 : 1, \ldots, x_n : 1 \vdash s : A$. By induction, $\theta(u) \in SN(n)$. For any density matrices $\gamma_k \in SN(1)$ $(k = 1, \ldots, n)$, define $\theta'' = (\theta|_\Delta, x_1 \mapsto \gamma_1, \ldots, x_n \mapsto \gamma_n)$; then $\theta'' \vDash \Delta, x_1 : 1, \ldots, x_n : 1$, and by the induction hypothesis $\theta''(s) = \theta(s)[\gamma_1/x_1, \ldots, \gamma_n/x_n] \in SN(A)$. Lemma D.4.10 gives $\mathsf{let}\ x^{\otimes n} = \theta(u)\ \mathsf{in}\ \theta(s) \in SN(A)$.

□

Strong normalisation

Proof. Taking θ to be the empty substitution (valid for any closed term), the Fundamental Lemma D.4.11 gives: for every closed $\vdash t : A$, we have $t \in SN(A) \subseteq SN$. Hence every closed well-typed term is strongly normalising under the extended relation, and therefore also under the original relation. □

D.5 Proof of Lemma 3.6.1 (Semantic Substitution)

Proof. By induction on t.

- Let $t = x$. Then $t[s/x] = s$, and $[\![x]\!]_{\theta, x\mapsto[\![s]\!]_\theta} = [\![s]\!]_\theta$, so both sides equal $[\![s]\!]_\theta$.
- Let $t = y$ with $y \neq x$. Then $t[s/x] = y$, and $[\![y]\!]_{\theta, x\mapsto[\![s]\!]_\theta} = \theta(y) = [\![y]\!]_\theta$.
- Let $t = \lambda y.u$. Then $t[s/x] = \lambda y.(u[s/x])$ (assuming $y \neq x$ and $y \notin FV(s)$ by renaming). By definition of the interpretation and the induction hypothesis on u:

$$\begin{aligned}[\![\lambda y.(u[s/x])]\!]_\theta &= \rho \mapsto [\![u[s/x]]\!]_{\theta,\, y\mapsto\rho} \\ &= \rho \mapsto [\![u]\!]_{\theta,\, x\mapsto[\![s]\!]_\theta,\, y\mapsto\rho} \qquad \text{(induction hypothesis on } u\text{)} \\ &= [\![\lambda y.u]\!]_{\theta, x\mapsto[\![s]\!]_\theta}.\end{aligned}$$

- Let $t = t_1 t_2$, with $\Gamma, x : A = \Gamma_1, \Gamma_2$ and $x : A \in \Gamma_j$. By the induction hypothesis applied to the subterm containing x:

$$[\![(t_1 t_2)[s/x]]\!]_\theta = [\![t_1[s/x]]\!]_\theta([\![t_2[s/x]]\!]_\theta) = [\![t_1]\!]_{\theta, x\mapsto[\![s]\!]_\theta}\big([\![t_2]\!]_{\theta, x\mapsto[\![s]\!]_\theta}\big) = [\![t_1 t_2]\!]_{\theta, x\mapsto[\![s]\!]_\theta}.$$

- Let $t = \rho^n$. The variable x does not appear, so $t[s/x] = \rho^n$ and $[\![\rho^n]\!]_{\theta, x\mapsto[\![s]\!]_\theta} = \rho^n = [\![\rho^n]\!]_\theta$.
- Let $t = U^m u$. Then $(U^m u)[s/x] = U^m(u[s/x])$. By the induction hypothesis:

$$[\![U^m(u[s/x])]\!]_\theta = \overline{U^m}[\![u[s/x]]\!]_\theta \overline{U^m}^\dagger = \overline{U^m}[\![u]\!]_{\theta, x\mapsto[\![s]\!]_\theta}\, \overline{U^m}^\dagger = [\![U^m u]\!]_{\theta, x\mapsto[\![s]\!]_\theta}.$$

- Let $t = \pi^m u$. Then $(\pi^m u)[s/x] = \pi^m(u[s/x])$. By the induction hypothesis:

$$[\![\pi^m(u[s/x])]\!]_\theta = \sum_i \overline{\pi_i}[\![u[s/x]]\!]_\theta \overline{\pi_i}^\dagger = \sum_i \overline{\pi_i}[\![u]\!]_{\theta, x\mapsto[\![s]\!]_\theta}\, \overline{\pi_i}^\dagger = [\![\pi^m u]\!]_{\theta, x\mapsto[\![s]\!]_\theta}.$$

- Let $t = t_1 \otimes t_2$, with $\Gamma, x : A = \Gamma_1, \Gamma_2$ and $x : A \in \Gamma_j$. By the induction hypothesis on the relevant subterm:

$$[\![(t_1 \otimes t_2)[s/x]]\!]_\theta = [\![t_1[s/x]]\!]_\theta \otimes [\![t_2[s/x]]\!]_\theta = [\![t_1]\!]_{\theta, x\mapsto[\![s]\!]_\theta} \otimes [\![t_2]\!]_{\theta, x\mapsto[\![s]\!]_\theta} = [\![t_1 \otimes t_2]\!]_{\theta, x\mapsto[\![s]\!]_\theta}.$$

- Let $t = \sum_j q_j t_j$. Then $t[s/x] = \sum_j q_j (t_j[s/x])$. By the induction hypothesis and linearity of the interpretation:

$$[\![\sum_j q_j (t_j[s/x])]\!]_\theta = \sum_j q_j [\![t_j[s/x]]\!]_\theta = \sum_j q_j [\![t_j]\!]_{\theta, x\mapsto[\![s]\!]_\theta} = [\![\sum_j q_j t_j]\!]_{\theta, x\mapsto[\![s]\!]_\theta}.$$

- Let $t = \mathsf{letcase}^\circ\ y = r\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$, with $\Gamma' \vdash r : (m, n)$ and $y : n \vdash t_i : B$. Since the t_i are typed in $y : n$ alone, $x \notin FV(t_i)$, so $t[s/x] = \mathsf{letcase}^\circ\ y = r[s/x]\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$. By the induction hypothesis on r, $[\![r[s/x]]\!]_\theta = [\![r]\!]_{\theta, x\mapsto[\![s]\!]_\theta}$, so the post-measurement states ρ_i and probabilities p_i are the same on both sides:

$$[\![t[s/x]]\!]_\theta = \sum_i p_i\, [\![t_i]\!]_{\theta, y\mapsto\rho_i} = [\![t]\!]_{\theta, x\mapsto[\![s]\!]_\theta}.$$

- Let $t = \mathsf{let}\ y^{\otimes n} = u\ \mathsf{in}\ v$, with $\Gamma, x : A = \Gamma_1, \Gamma_2$, $\Gamma_1 \vdash u : n$ and $\Gamma_2, y_1 : 1, \ldots, y_n : 1 \vdash v : B$ (with $y_k \neq x$ by α-renaming).

  - If $x : A \in \Gamma_1$, then $t[s/x] = \mathsf{let}\ y^{\otimes n} = u[s/x]\ \mathsf{in}\ v$, since $x \notin FV(v)$. By the induction hypothesis on u, $[\![u[s/x]]\!]_\theta = [\![u]\!]_{\theta, x \mapsto [\![s]\!]_\theta}$, so the combined decomposition coefficients α_i are the same on both sides:

$$\begin{aligned}[\![t[s/x]]\!]_\theta &= \sum_{i,\vec{l}} p_{i\vec{l}} [\![v]\!]_{\theta,\, y_1 \mapsto \gamma_{i_1}^{l_1}, \ldots, y_n \mapsto \gamma_{i_n}^{l_n}} \\ &= [\![\mathsf{let}\ y^{\otimes n} = u\ \mathsf{in}\ v]\!]_{\theta, x \mapsto [\![s]\!]_\theta} = [\![t]\!]_{\theta, x \mapsto [\![s]\!]_\theta}.\end{aligned}$$

  - If $x : A \in \Gamma_2$, then $t[s/x] = \mathsf{let}\ y^{\otimes n} = u\ \mathsf{in}\ v[s/x]$, since $x \notin FV(u)$. The combined decomposition coefficients of $[\![u]\!]_\theta$ are unchanged. By the induction hypothesis on v:

$$\begin{aligned}[\![t[s/x]]\!]_\theta &= \sum_{i,\vec{l}} p_{i\vec{l}} [\![v]\!]_{\theta,\, x \mapsto [\![s]\!]_\theta,\, y_1 \mapsto \gamma_{i_1}^{l_1}, \ldots, y_n \mapsto \gamma_{i_n}^{l_n}} \\ &= [\![\mathsf{let}\ y^{\otimes n} = u\ \mathsf{in}\ v]\!]_{\theta, x \mapsto [\![s]\!]_\theta} = [\![t]\!]_{\theta, x \mapsto [\![s]\!]_\theta}.\end{aligned}$$

□

D.6 Proof of Theorem 3.6.2 (Soundness)

Proof. By induction on the derivation of $t \to r$.

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

$$[\![(\lambda x.t')s]\!]_\theta = [\![\lambda x.t']\!]_\theta([\![s]\!]_\theta) = [\![t']\!]_{\theta, x \mapsto [\![s]\!]_\theta} = [\![t'[s/x]]\!]_\theta,$$

  where the last step uses Lemma 3.6.1.

- Let $t = U^m \rho^n$, $r = \rho'^n$ with $\rho'^n = \overline{U^m} \rho^n \overline{U^m}^\dagger$.

$$[\![U^m \rho^n]\!]_\theta = \overline{U^m} \rho^n \overline{U^m}^\dagger = \rho'^n = [\![\rho'^n]\!]_\theta.$$

- Let $t = \rho_1^m \otimes \rho_2^n$, $r = \rho$ with $\rho = \rho_1^m \otimes \rho_2^n$.

$$[\![\rho_1^m \otimes \rho_2^n]\!]_\theta = [\![\rho_1^m]\!]_\theta \otimes [\![\rho_2^n]\!]_\theta = \rho_1^m \otimes \rho_2^n = \rho = [\![\rho]\!]_\theta.$$

- Let $t = \sum_i p_i \rho_i$, $r = \rho'$ with $\rho' = \sum_i p_i \rho_i$.

$$[\![\sum_i p_i \rho_i]\!]_\theta = \sum_i p_i \rho_i = \rho' = [\![\rho']\!]_\theta.$$

- Let $t = \sum_i p_i u$, $r = u$.

$$[\![\sum_i p_i u]\!]_\theta = \sum_i p_i [\![u]\!]_\theta = \left(\textstyle\sum_i p_i\right) [\![u]\!]_\theta = [\![u]\!]_\theta.$$

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

  $$[\![(\sum_i p_i t_i) r']\!]_\theta = \Big(\sum_i p_i [\![t_i]\!]_\theta\Big)([\![r']\!]_\theta) = \sum_i p_i \big([\![t_i]\!]_\theta([\![r']\!]_\theta)\big) = \sum_i p_i [\![t_i r']\!]_\theta = [\![\sum_i p_i (t_i r')]\!]_\theta.$$

- Let $t = \mathsf{letcase}^\circ\ x = \pi^m \rho^n\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$, $r = \sum_i p_i\, t_i[\rho_i^n / x]$ with $p_i = \mathsf{tr}(\overline{\pi_i}^\dagger \overline{\pi_i} \rho^n)$ and $\rho_i^n = \overline{\pi_i} \rho^n \overline{\pi_i}^\dagger / p_i$. Using linearity and Lemma 3.6.1:

  $$[\![r]\!]_\theta = \sum_i p_i\, [\![t_i[\rho_i^n/x]]\!]_\theta = \sum_i p_i\, [\![t_i]\!]_{\theta, x \mapsto \rho_i^n} = [\![t]\!]_\theta.$$

- Let

  $$t = \mathsf{letcase}^\circ\ x = \sum_j q_j w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\},$$
  $$r = \sum_j q_j\, \mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}.$$

  Write $F_i(\rho) \coloneqq [\![t_i]\!]_{\theta, x \mapsto \rho}$; this is linear in ρ because the type system is affine (x appears at most once in t_i). Let $\rho = [\![\sum_j q_j w_j]\!]_\theta = \sum_j q_j [\![w_j]\!]_\theta$, and define $p_i = \mathsf{tr}(\overline{\pi_i}^\dagger \overline{\pi_i} \rho)$ and $\rho_i = \overline{\pi_i} \rho\, \overline{\pi_i}^\dagger / p_i$ as in the semantics. Note that $p_i \rho_i = \overline{\pi_i} \rho\, \overline{\pi_i}^\dagger$. Using linearity of F_i:

  $$p_i \cdot F_i(\rho_i) = F_i(p_i \rho_i) = F_i\big(\overline{\pi_i} \rho\, \overline{\pi_i}^\dagger\big).$$

  Therefore, substituting $\rho = \sum_j q_j [\![w_j]\!]_\theta$ and using linearity of F_i and of $\overline{\pi_i}(\cdot)\overline{\pi_i}^\dagger$:

  $$\begin{aligned}
  [\![t]\!]_\theta = \sum_i p_i \cdot F_i(\rho_i) &= \sum_i F_i\big(\overline{\pi_i} \rho\, \overline{\pi_i}^\dagger\big) \\
  &= \sum_i F_i\Big(\overline{\pi_i}\Big(\sum_j q_j [\![w_j]\!]_\theta\Big)\overline{\pi_i}^\dagger\Big) \\
  &= \sum_j q_j \sum_i F_i\big(\overline{\pi_i} [\![w_j]\!]_\theta \overline{\pi_i}^\dagger\big).
  \end{aligned}$$

  For each fixed j, let $p_i^j = \mathsf{tr}(\overline{\pi_i}^\dagger \overline{\pi_i} [\![w_j]\!]_\theta)$ and $\rho_i^j = \overline{\pi_i} [\![w_j]\!]_\theta \overline{\pi_i}^\dagger / p_i^j$. By linearity of F_i:

  $$\sum_i F_i\big(\overline{\pi_i} [\![w_j]\!]_\theta \overline{\pi_i}^\dagger\big) = \sum_i p_i^j F_i(\rho_i^j) = [\![\mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}]\!]_\theta.$$

  Hence $[\![t]\!]_\theta = \sum_j q_j\, [\![\mathsf{letcase}^\circ\ x = w_j\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}]\!]_\theta = [\![r]\!]_\theta$.

- Let $t = \mathsf{let}\ x^{\otimes n} = \rho^n\ \mathsf{in}\ s$, $r = \sum_{i,\vec{l}} p_{i\vec{l}}\, s[\gamma_{i_1}^{l_1}/x_1, \ldots, \gamma_{i_n}^{l_n}/x_n]$, where $p_{i\vec{l}} = \alpha_i(\rho^n) \prod_k \lambda_{i_k}^{l_k}$. Unfolding the interpretation of let and applying Lemma 3.6.1 n times:

  $$\begin{aligned}
  [\![t]\!]_\theta &= \sum_{i,\vec{l}} p_{i\vec{l}}\, [\![s]\!]_{\theta,\, x_1 \mapsto \gamma_{i_1}^{l_1},\, \ldots,\, x_n \mapsto \gamma_{i_n}^{l_n}} \\
  &= \sum_{i,\vec{l}} p_{i\vec{l}}\, [\![s[\gamma_{i_1}^{l_1}/x_1, \ldots, \gamma_{i_n}^{l_n}/x_n]]\!]_\theta \\
  &= [\![\sum_{i,\vec{l}} p_{i\vec{l}}\, s[\gamma_{i_1}^{l_1}/x_1, \ldots, \gamma_{i_n}^{l_n}/x_n]]\!]_\theta = [\![r]\!]_\theta.
  \end{aligned}$$

- Contextual cases. Let $s \to s'$.
  - Let $t = s\,u$, $r = s'\,u$ with $s \to s'$. By the induction hypothesis $[\![s]\!]_\theta = [\![s']\!]_\theta$, so $[\![s\,u]\!]_\theta = [\![s]\!]_\theta([\![u]\!]_\theta) = [\![s']\!]_\theta([\![u]\!]_\theta) = [\![s'\,u]\!]_\theta$.
  - Let $t = u\,s$, $r = u\,s'$ with $s \to s'$. By the induction hypothesis $[\![s]\!]_\theta = [\![s']\!]_\theta$, so $[\![u\,s]\!]_\theta = [\![u]\!]_\theta([\![s]\!]_\theta) = [\![u]\!]_\theta([\![s']\!]_\theta) = [\![u\,s']\!]_\theta$.
  - Let $t = U^m s$, $r = U^m s'$ with $s \to s'$. $[\![U^m s]\!]_\theta = \overline{U^m}[\![s]\!]_\theta\overline{U^m}^\dagger = \overline{U^m}[\![s']\!]_\theta\overline{U^m}^\dagger = [\![U^m s']\!]_\theta$.
  - Let $t = \pi^m s$, $r = \pi^m s'$ with $s \to s'$. $[\![\pi^m s]\!]_\theta = \sum_i \overline{\pi_i}[\![s]\!]_\theta\overline{\pi_i}^\dagger = \sum_i \overline{\pi_i}[\![s']\!]_\theta\overline{\pi_i}^\dagger = [\![\pi^m s']\!]_\theta$.
  - Let $t = s \otimes u$, $r = s' \otimes u$ with $s \to s'$. $[\![s \otimes u]\!]_\theta = [\![s]\!]_\theta \otimes [\![u]\!]_\theta = [\![s']\!]_\theta \otimes [\![u]\!]_\theta = [\![s' \otimes u]\!]_\theta$.
  - Let $t = u \otimes s$, $r = u \otimes s'$ with $s \to s'$. Analogous.
  - Let $t = \sum_j p_j u_j$, $r = \sum_j p_j v_j$ where $u_k \to v_k$ and $u_j = v_j$ for $j \neq k$. By the induction hypothesis $[\![u_k]\!]_\theta = [\![v_k]\!]_\theta$, so $[\![\sum_j p_j u_j]\!]_\theta = \sum_j p_j [\![u_j]\!]_\theta = \sum_j p_j [\![v_j]\!]_\theta = [\![\sum_j p_j v_j]\!]_\theta$.
  - Let $t = \mathsf{letcase}^\circ\ x = s\ \mathsf{in}\ \{u_0, \ldots, t_{2^m-1}\}$, $r = \mathsf{letcase}^\circ\ x = s'\ \mathsf{in}\ \{u_0, \ldots, u_{2^m-1}\}$ with $s \to s'$. By the induction hypothesis $[\![s]\!]_\theta = [\![s']\!]_\theta$, so the post-measurement states and probabilities are the same, giving $[\![t]\!]_\theta = [\![r]\!]_\theta$.
  - Let $t = \mathsf{let}\ x^{\otimes n} = s\ \mathsf{in}\ u$, $r = \mathsf{let}\ x^{\otimes n} = s'\ \mathsf{in}\ u$ with $s \to s'$. By the induction hypothesis $[\![s]\!]_\theta = [\![s']\!]_\theta$, so $\alpha_i([\![s]\!]_\theta) = \alpha_i([\![s']\!]_\theta)$ for all i, and the two interpretations agree term by term.
  - Let $t = \mathsf{let}\ x^{\otimes n} = u\ \mathsf{in}\ s$, $r = \mathsf{let}\ x^{\otimes n} = u\ \mathsf{in}\ s'$ with $s \to s'$. The combined decomposition of $[\![u]\!]_\theta$ is unchanged. For each fixed $i, \vec{l}$, the induction hypothesis applied to $s \to s'$ under the extended valuation $\theta' = \theta, x_1 \mapsto \gamma_{i_1}^{l_1}, \ldots, x_n \mapsto \gamma_{i_n}^{l_n}$ gives $[\![s]\!]_{\theta'} = [\![s']\!]_{\theta'}$. Multiplying by $p_{i\vec{l}}$ and summing over all $i, \vec{l}$ gives $[\![t]\!]_\theta = [\![r]\!]_\theta$.

□

D.7 Proof of Lemma 3.7.3 (Compositionality)

Proof. We prove the lemma by structural induction on the context C. In each case we write t and r for the two closed terms with $[\![t]\!]_\theta = [\![r]\!]_\theta$, and θ for any fixed valuation of the free variables of C.

- Let $C = [\cdot]$. $C[t] = t$ and $C[r] = r$, so $[\![C[t]]\!]_\theta = [\![t]\!]_\theta = [\![r]\!]_\theta = [\![C[r]]\!]_\theta$ directly from the hypothesis.
- Let $C = \lambda x.C'$. Suppose $x : A$, so $[\![A]\!]$ is the semantic domain of x. For any $v \in [\![A]\!]$,

  $$[\![\lambda x.C'[t]]\!]_\theta = v \mapsto [\![C'[t]]\!]_{\theta, x \mapsto v}.$$

  By the induction hypothesis applied to C' with valuation $\theta' = (\theta, x \mapsto v)$ and the same hypothesis $[\![t]\!]_\theta = [\![r]\!]_\theta$, we get $[\![C'[t]]\!]_{\theta'} = [\![C'[r]]\!]_{\theta'}$ for every $v \in [\![A]\!]$. Hence the two functions $v \mapsto [\![C'[t]]\!]_{\theta'}$ and $v \mapsto [\![C'[r]]\!]_{\theta'}$ agree pointwise on all of $[\![A]\!]$, giving $[\![\lambda x.C'[t]]\!]_\theta = [\![\lambda x.C'[r]]\!]_\theta$.

- Let $C = C'\,s$.
$$[\![C'[t]\,s]\!]_\theta = [\![C'[t]]\!]_\theta\big([\![s]\!]_\theta\big).$$
By the induction hypothesis, $[\![C'[t]]\!]_\theta = [\![C'[r]]\!]_\theta$, so $[\![C'[t]]\!]_\theta\big([\![s]\!]_\theta\big) = [\![C'[r]]\!]_\theta\big([\![s]\!]_\theta\big) = [\![C'[r]\,s]\!]_\theta$.

- Let $C = s\,C'$.
$$[\![s\,C'[t]]\!]_\theta = [\![s]\!]_\theta\big([\![C'[t]]\!]_\theta\big).$$
By the induction hypothesis, $[\![C'[t]]\!]_\theta = [\![C'[r]]\!]_\theta$, so the two expressions are equal.

- Let $C = U^m C'$.
$$[\![U^m C'[t]]\!]_\theta = \overline{U^m}\,[\![C'[t]]\!]_\theta\,\overline{U^m}^\dagger = \overline{U^m}\,[\![C'[r]]\!]_\theta\,\overline{U^m}^\dagger = [\![U^m C'[r]]\!]_\theta,$$
where the middle equality uses the induction hypothesis.

- Let $C = \pi^m C'$.
$$[\![\pi^m C'[t]]\!]_\theta = \sum_i \overline{\pi_i}\,[\![C'[t]]\!]_\theta\,\overline{\pi_i}^\dagger = \sum_i \overline{\pi_i}\,[\![C'[r]]\!]_\theta\,\overline{\pi_i}^\dagger = [\![\pi^m C'[r]]\!]_\theta.$$

- Let $C = C' \otimes s$.
$$[\![C'[t] \otimes s]\!]_\theta = [\![C'[t]]\!]_\theta \otimes [\![s]\!]_\theta = [\![C'[r]]\!]_\theta \otimes [\![s]\!]_\theta = [\![C'[r] \otimes s]\!]_\theta.$$

- Let $C = s \otimes C'$. Symmetric to the previous case.

- Let $C = \sum_i p_i s_i[C'/s_j]$. Write $u_i = s_i$ for $i \neq j$, $u_j = C'[t]$, and $v_j = C'[r]$. Then
$$[\![\textstyle\sum_i p_i u_i]\!]_\theta = \textstyle\sum_i p_i [\![u_i]\!]_\theta = \sum_{i\neq j} p_i [\![s_i]\!]_\theta + p_j [\![C'[t]]\!]_\theta.$$
By the induction hypothesis, $[\![C'[t]]\!]_\theta = [\![C'[r]]\!]_\theta$, so the sum equals $\sum_{i\neq j} p_i [\![s_i]\!]_\theta + p_j [\![C'[r]]\!]_\theta = [\![\sum_i p_i v_i]\!]_\theta$.

- Let $C = \mathsf{letcase}^\circ\ x = C'\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}$. Let $\sigma = [\![C'[t]]\!]_\theta$ and $\sigma' = [\![C'[r]]\!]_\theta$. By the induction hypothesis $\sigma = \sigma'$. The probabilities $p_i = \mathsf{tr}(\overline{\pi_i}^\dagger \overline{\pi_i}\,\sigma)$ and post-measurement states $\sigma_i = \overline{\pi_i}\,\sigma\,\overline{\pi_i}^\dagger / p_i$ depend only on σ, so they are the same for $C'[t]$ and $C'[r]$. Hence
$$[\![\mathsf{letcase}^\circ\ x = C'[t]\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}]\!]_\theta = \sum_i p_i [\![t_i]\!]_{\theta, x\mapsto\sigma_i} = [\![\mathsf{letcase}^\circ\ x = C'[r]\ \mathsf{in}\ \{t_0, \ldots, t_{2^m-1}\}]\!]_\theta.$$

- Let $C = \mathsf{letcase}^\circ\ x = s\ \mathsf{in}\ \{t_0, \ldots, C', \ldots, t_{2^m-1}\}$. The probabilities p_i and post-measurement states σ_i of s are independent of the hole. For the j-th branch, by the induction hypothesis (with valuation $\theta, x \mapsto \sigma_j$), $[\![C'[t]]\!]_{\theta, x\mapsto\sigma_j} = [\![C'[r]]\!]_{\theta, x\mapsto\sigma_j}$. All other branches are unchanged, so the total expression is unchanged.

- Let $C = \mathsf{let}\ x^{\otimes n} = C'\ \mathsf{in}\ s$. The combined decomposition of $\mathsf{let}\ x^{\otimes n} = C'[t]\ \mathsf{in}\ s$ is computed from $[\![C'[t]]\!]_\theta$. By the induction hypothesis, $[\![C'[t]]\!]_\theta = [\![C'[r]]\!]_\theta$, so the Pauli coefficients α_i and hence the weights $p_{i\vec{l}} = \alpha_i \prod_k \lambda_{i_k}^{l_k}$ and eigenprojectors $\gamma_{i_k}^{l_k}$ are identical for both sides. Therefore
$$[\![\mathsf{let}\ x^{\otimes n} = C'[t]\ \mathsf{in}\ s]\!]_\theta = \sum_{i,\vec{l}} p_{i\vec{l}} [\![s]\!]_{\theta, x_1\mapsto\gamma_{i_1}^{l_1}, \ldots, x_n\mapsto\gamma_{i_n}^{l_n}} = [\![\mathsf{let}\ x^{\otimes n} = C'[r]\ \mathsf{in}\ s]\!]_\theta.$$

- Let $C = \mathsf{let}\ x^{\otimes n} = s\ \mathsf{in}\ C'$. The combined decomposition of s is fixed (it does not involve the hole). For each index pair $(i, \vec{l})$, let $\theta_{i\vec{l}} = \theta, x_1 \mapsto \gamma_{i_1}^{l_1}, \ldots, x_n \mapsto \gamma_{i_n}^{l_n}$. By the induction hypothesis applied to C' with valuation $\theta_{i\vec{l}}$,

$$[\![C'[t]]\!]_{\theta_{i\vec{l}}} = [\![C'[r]]\!]_{\theta_{i\vec{l}}}.$$

  Multiplying by $p_{i\vec{l}}$ and summing over all $(i, \vec{l})$:

$$[\![\mathsf{let}\ x^{\otimes n} = s\ \mathsf{in}\ C'[t]]\!]_\theta = \sum_{i,\vec{l}} p_{i\vec{l}} [\![C'[t]]\!]_{\theta_{i\vec{l}}} = \sum_{i,\vec{l}} p_{i\vec{l}} [\![C'[r]]\!]_{\theta_{i\vec{l}}} = [\![\mathsf{let}\ x^{\otimes n} = s\ \mathsf{in}\ C'[r]]\!]_\theta.$$

In every case $[\![C[t]]\!]_\theta = [\![C[r]]\!]_\theta$, completing the induction. □

D.8 Proof of Theorem 3.7.5 (Adequacy)

Proof. The argument is assembled directly from the two lemmas and the soundness theorem proved above.

Let C be any context with hole type A and output type n (so $\vdash C[t] : n$ and $\vdash C[r] : n$ are closed). We exhibit a density matrix ρ such that $C[t] \to^* \rho$ and $C[r] \to^* \rho$.

Step 1 (Compositionality). By Lemma 3.7.3 applied with the empty valuation and the hypothesis $[\![t]\!]_\theta = [\![r]\!]_\theta$,

$$[\![C[t]]\!]_\theta = [\![C[r]]\!]_\theta.$$

Step 2 (Normalization). By Lemma 3.7.4, since $\vdash C[t] : n$ and $\vdash C[r] : n$ are closed ground-type terms, there exist density matrices ρ_1 and ρ_2 with

$$C[t] \to^* \rho_1 \qquad \text{and} \qquad C[r] \to^* \rho_2.$$

Step 3 (Soundness, iterated). Write the first sequence as $C[t] = s_0 \to s_1 \to \cdots \to s_k = \rho_1$. By Theorem 3.6.2 (Soundness) applied at each step, $[\![s_0]\!]_\theta = [\![s_1]\!]_\theta = \cdots = [\![s_k]\!]_\theta$, so $[\![C[t]]\!]_\theta = [\![\rho_1]\!]_\theta$. By definition, $[\![\rho_1]\!]_\theta = \rho_1$. Applying the same argument to the second sequence, $[\![C[r]]\!]_\theta = \rho_2$.

Step 4 (Identification).

$$\rho_1 = [\![\rho_1]\!]_\theta = [\![C[t]]\!]_\theta = [\![C[r]]\!]_\theta = [\![\rho_2]\!]_\theta = \rho_2.$$

Setting $\rho := \rho_1 = \rho_2$, we have $C[t] \to^* \rho$ and $C[r] \to^* \rho$. Since C was an arbitrary context with output type n, Definition 3.7.2 gives $t \equiv r$. □