Effect Semantics for Quantum Process Calculi

Lorenzo Ceragioli
IMT School for Advanced Studies Lucca, Italy

Fabio Gadducci
University of Pisa, Italy

Giuseppe Lomurno
University of Pisa, Italy

Gabriele Tedeschi
University of Pisa, Italy

Abstract

The development of quantum communication protocols sparked the interest in quantum extensions of process calculi and behavioural equivalences, but defining a bisimilarity that matches the observational properties of a quantum-capable system is a surprisingly difficult task. The two proposals explicitly addressing this issue, qCCS and lqCCS, do not define an algorithmic verification scheme: the bisimilarity of two processes is proven by comparing their behaviour under all input states. We introduce a new semantic model based on effects, i.e. probabilistic predicates on quantum states that represent their observable properties. We define and investigate the properties of effect distributions and effect labelled transition systems (eLTSs), generalizing probability distributions and probabilistic labelled transition systems (pLTSs), respectively. As a proof of concept, we provide an eLTS-based semantics for a minimal quantum process algebra, which we prove sound and complete with respect to the observable probabilistic behaviour of quantum processes. To the best of our knowledge, ours is the first algorithmically verifiable proposal that abides to the properties of quantum theory.

2012 ACM Subject Classification Theory of computation → Quantum computation theory; Theory of computation → Process calculi; Theory of computation → Operational semantics

Keywords and phrases Quantum process calculi, probabilistic LTSs, effect LTSs

Digital Object Identifier 10.4230/LIPIcs.CONCUR.2024.16

Funding This study was carried out within the National Centre on HPC, Big Data and Quantum Computing - SPOKE 10 (Quantum Computing) and received funding from the European Union Next-GenerationEU - National Recovery and Resilience Plan (NRRP) – MISSION 4 COMPONENT 2, INVESTMENT N. 1.4 – CUP N. I53C22000690001.

1 Introduction

Recent years have seen a flourishing development of quantum technologies for computer science, in the form of *quantum computation* and *quantum communication*. Both of them exploit quantum phenomena like superposition and entanglement: the former is interested in harvesting the (supposedly) higher computational power of quantum computers, while the latter strives to achieve secure and reliable communication, featuring solutions for key distribution [31], cryptographic coin tossing [2], direct communication [28], and private information retrieval [14]. Protocols like BB84 QKD [2] are *unconditionally secure* [29], meaning that they are protected against all physically possible attackers. Quantum communication also promises to allow linking multiple computers via the *Quantum Internet* [5, 35], therefore providing quantum algorithms with large enough memories for practical applications.

Despite the rich theory and the potential applications, there is no accepted standard to model and verify quantum concurrent systems and protocols. Numerous works [25, 15, 12, 34, 7] rely on *process calculi*, an algebraic formalism that has been successfully applied to

classical protocols and concurrent systems. The semantics of a calculus is given by means of a *labelled transition system* (LTS), i.e. a triple $(S, Act, \to)$ with S a set of states, Act a set of actions, and $\to$ a transition relation that specifies how states evolve. The standard equivalence for LTSs is *bisimilarity*, the largest relation on states that is "stable" for $\to$, meaning that bisimilar states evolve with the same action in bisimilar states.

There have been several attempts [24, 8, 10, 9, 7] to adapt known techniques to the quantum setting, mainly in terms of *probabilistic* LTSs (pLTSs) $(Conf, Act, \to)$, where $Conf = \mathcal{H} \times S$ is a set of *configurations* $\langle \rho, P \rangle$ composed by a quantum state ρ (an element of a Hilbert space $\mathcal{H}$) and a process P, and $\to \subseteq Conf \times Act \times \mathcal{D}(Conf)$ with $\mathcal{D}(Conf)$ probability distributions of configurations. This approach led to a plethora of different bisimilarities, most of them unsatisfactory since they distinguish processes that are deemed indistinguishable by the prescriptions of quantum theory [8, 23, 13]. Moreover, only configuration bisimilarity is directly considered in these works. Two processes P and Q are instead deemed bisimilar if and only if for any quantum state ρ the configurations $\langle \rho, P \rangle$ and $\langle \rho, Q \rangle$ are bisimilar. Assessing bisimilarity of processes thus requires comparing infinitely many pLTSs (one for each quantum state), and algorithmic verification is still missing. In [7], the root of these problems is identified in the peculiarities of the semantic model described above, a non-deterministic pLTS made of quantum states and processes.

We propose *effect labelled transition systems* (eLTSs) as a new semantic model for quantum systems, generalizing pLTSs. In physics, *effects* represent the observable behaviour of quantum states, as they model atomic experiments that you can perform on a quantum system. Building on them allows us to express the correct observable properties of quantum processes. *Effect distributions* generalize probability distributions by using effects as weights, and the transition relation of an eLTS associates states with effect distributions. We study effect distributions and eLTSs, either generalizing the known results on probabilistic systems when possible, or proving they do not hold otherwise. We explore different notions of bisimilarity, namely Aczel-Mendler and Larsen-Skou, and show that they disagree on which quantum processes should be bisimilar, even if they coincide in the probabilistic case. Then, we consider two correctness criteria for quantum bisimilarity, through which we show that a Larsen-Skou-style bisimilarity is adequate for comparing quantum systems, as it is correct and complete with respect to the observable probabilistic behaviour of quantum protocols.

To assess our proposal, we define a *minimal quantum process algebra* (mQPA) featuring actions, restriction, synchronization, non-determinism, parallel composition, destructive measurements, and unitary transformations, and we equip it with two different semantics: a stateful Schrödinger-style semantics that given a quantum state returns a pLTS representing the observable behaviour of the system; and a Heisenberg-style semantics in the form of an eLTS that is independent of the quantum input, in the style of [20, 11]. We show that the Heisenberg eLTS is indeed the "symbolic" version of the Schrödinger pLTSs of the same system, thus proving bisimilarity just once for the Heisenberg-style semantics makes it automatically verified for all "ground" systems obtained by instantiating the quantum input. Notably, our notion of bisimilarity can be efficiently verified with standard techniques [22].

Synopsis. Section 2 provides some background on probability distributions and quantum theory. Section 3 introduces effect distributions and eLTSs, investigating their properties and comparing eLTS bisimilarities. Section 4 presents our minimal process algebra with both a stateful and a stateless semantics, which are proved to coincide. Finally, Section 5 compares related works and Section 6 draws our conclusions. The full proofs are in the Appendix.

2 Background

We recall some background on probability distributions, quantum computing, and effects, referring the reader to [18, 30] for further information.

2.1 Probability Distributions

A *probability (sub)distribution* over a set S is a function $\Delta : S \to [0,1]$ such that $\sum_{s\in S} \Delta(s) \leq 1$. We write $\mathcal{D}S$ for the set of finitely supported distributions over S, i.e. with $\Delta(s) = 0$ for all but a finite set of elements. We let $\overline{s}$ be the point distribution $\overline{s}(s) = 1$.

Probability distributions form a *convex set* [4]: for any two distributions Δ, Θ and real $p \in [0,1]$ there is a distribution $\Delta \,{}_p\!\oplus\, \Theta$ defined as $p \cdot \Delta + (1-p) \cdot \Theta$. A function f between convex sets is convex if it preserves the ${}_p\!\oplus$ operator, i.e. if $f(x_1 \,{}_p\!\oplus\, x_2) = f(x_1) \,{}_p\!\oplus\, f(x_2)$. We denote as $\mathbf{Conv}(X, Y)$ the set of convex functions between X and Y.

2.2 Quantum Computing

We assume a denumerable set of indexed qubits $\mathbf{Q} = \{q_0, q_1, \dots\}$, the quantum mechanical analogues of classical bits. The states of a qubit q are *unit vectors* $|\psi\rangle$ in the Hilbert space $\mathcal{H}_q$, i.e. column vectors in $\mathbb{C}^2$ such that $\langle\psi|\psi\rangle = 1$, with $\langle\psi|$ the conjugate transpose of $|\psi\rangle$, and $\langle\cdot|\cdot\rangle$ the usual *inner product*. The vectors $|0\rangle = (1,0)^T$ and $|1\rangle = (0,1)^T$ form an orthonormal basis of $\mathbb{C}^2$, called the *computational basis*. Other important states are $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, which form the *Hadamard basis*.

The *Kronecker product* $\otimes$ is defined as follows (we often write $|\psi\phi\rangle$ for $|\psi\rangle \otimes |\phi\rangle$)

$$\begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{m,1} & \cdots & x_{m,n} \end{bmatrix} \otimes L = \begin{bmatrix} x_{1,1}L & \cdots & x_{1,n}L \\ \vdots & \ddots & \vdots \\ x_{m,1}L & \cdots & x_{m,n}L \end{bmatrix}$$

Note that $\otimes$ is not commutative. Given $\mathcal{H}_q$ with $\{|\psi_i\rangle\}_{i\in I}$ one of its bases, and $\mathcal{H}_{q'}$ with $\{|\phi_j\rangle\}_{j\in I}$ one of its bases, we let $\mathcal{H}_q \otimes \mathcal{H}_{q'}$ be the Hilbert space with bases $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{(i,j)\in I\times J}$. A quantum register is a finite set of n qubits $Q \subseteq \mathbf{Q}$, representing composite physical systems. Its states are in $\mathcal{H}_Q = \bigotimes_{i=1,q_i\in Q}^{\infty} \mathcal{H}_{q_i} = \mathbb{C}^{2^n}$. Note that the Kronecker product is applied in an ordered manner, according to the indexing of $\mathbf{Q}$. The state of a quantum register $\mathcal{H}_{\{q,q'\}}$ is *separable* when it can be expressed as the tensor of two vectors of $\mathcal{H}_q$ and $\mathcal{H}_{q'}$. Otherwise, it is *entangled*, like the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

For each linear operator A on $\mathcal{H}_Q$, its *adjoint* $A^\dagger$ is the unique linear operator such that $\langle\psi|A|\phi\rangle = \langle A^\dagger\psi|\phi\rangle$. A linear operator U is *unitary* when $UU^\dagger = U^\dagger U = \mathbb{I}$. In quantum physics, the evolution of a closed system is described by a unitary transformation: the state $|\psi\rangle$ at time t_0 is related to $|\psi'\rangle$ at time t_1 by a unitary operator U, which only depends on t_0 and t_1, i.e. $|\psi'\rangle = U|\psi\rangle$. Accordingly, quantum computers allow the programmer to manipulate registers via unitaries like H, X, Z and $CNOT$, satisfying: $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$; $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$; $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$; $CNOT|10\rangle = |11\rangle$, $CNOT|11\rangle = |10\rangle$ and $CNOT|0\psi\rangle = |0\psi\rangle$ (all the other cases are defined by linearity).

Let Q and Q' be sets of qubits, we write $Q \uplus Q'$ for $Q \cup Q'$ when $Q \cap Q' = \emptyset$, and we allow composing a pair of states in $\mathcal{H}_Q$ and $\mathcal{H}_{Q'}$ to obtain a state in $\mathcal{H}_{Q\uplus Q'}$. To preserve the ordering induced by the indices, we build on top of $\otimes$ to define a partial commutative tensor product $\boxtimes$. We let $\boxtimes$ be the operation that applies $\otimes$ and then sorts the qubits according to their indices: $|\psi\rangle \boxtimes |\phi\rangle = \mathit{Sort}(|\psi\rangle \otimes |\phi\rangle) \in \mathcal{H}_{Q\uplus Q'}$, with Sort a unitary operator.

The density operator formalism puts together quantum systems and probability by considering mixed states, i.e. *probability sub-distributions of quantum states*. A point distribution $\overline{|\psi\rangle}$ (called a pure state) is represented by the matrix $|\psi\rangle\langle\psi|$. In general, a probability distribution Δ is represented as the matrix $\rho = \sum_i \Delta(\psi_i)\,|\psi_i\rangle\langle\psi_i|$, known as its *(partial) density operator*. Recall that a complex matrix N is called *positive semi-definite*, shortly positive, when $\langle\psi|N|\psi\rangle \geq 0$ for any $|\psi\rangle$. The *Löwner order* is the partial order defined by $L \sqsubseteq L'$ whenever $L' - L$ is positive. Given $\mathcal{H}_Q$ of dimension d, the density operators over $\mathcal{H}_Q$ coincide with the positive matrices in $\mathbb{C}^{d\times d}$ of trace smaller of equal to one, and we denote them as $DM_Q = \left\{\, \rho \in \mathbb{C}^{d\times d} \mid \rho \sqsupseteq 0_Q,\ \mathrm{tr}(\rho) \leq 1 \,\right\}$, where 0_Q is the $d \times d$ all-zero operator on $\mathcal{H}_Q$. Density operators form a convex set, meaning that for any real $p \in [0,1]$ and any $\rho, \sigma \in DM_Q$, there is a *convex combination* $\rho\ {}_p\!\oplus\ \sigma \in DM_Q$ defined as $p\rho + (1-p)\sigma$. A function between convex sets is called convex if it preserves the ${}_p\!\oplus$ operator.

Given $\mathcal{H}_Q$ and $\mathcal{H}_{Q'}$ of dimensions n and m respectively, a *trace non-increasing superoperator* $\mathcal{E} : DM_Q \to DM_{Q'}$ is defined as $\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger$ for a set of operators $\{K_i \in \mathbb{C}^{m\times n}\}_{i=1,\ldots,n\times m}$ (called *Kraus operators*), such that $\sum_i K_i^\dagger K_i \sqsubseteq \mathbb{I}_Q$. Superoperators model the evolution of mixed quantum states, and are closed with respect to composition. Any unitary transformation U is represented as the superoperator with Kraus decomposition $\{U\}$. The Kronecker product also defines composition of mixed states and superoperators on different quantum registers. We lift our commutative tensor product $\boxtimes$ to density operators and to superoperators by reordering the qubits when needed.

Density operators can be used to describe the state of a subsystem of a composite quantum system. Given a $\rho \in DM_{Q\uplus Q'}$, the *reduced density operator* of Q, $\rho_Q = \mathrm{tr}_{Q'}(\rho) \in DM_Q$, describes the state of Q, with $\mathrm{tr}_{Q'}$ the *partial trace over* Q', defined as the linear transformation such that $\mathrm{tr}_{Q'}(|\psi\rangle\langle\psi'| \boxtimes |\phi\rangle\langle\phi'|) = |\psi\rangle\langle\psi'|\,\mathrm{tr}(|\phi\rangle\langle\phi'|)$ for each $|\psi\rangle\langle\psi'| \in DM_Q$ and $|\phi\rangle\langle\phi'| \in DM_{Q'}$.

2.3 Quantum Effects

Quantum measurements allow describing systems that exchange information with the environment. Performing a measurement on a quantum register returns a probabilistic result and it either destroys or changes the qubits. We focus on destructive measurements.

The simplest kind of measurements are *quantum effects* (simply called effects in quantum textbooks [18]), i.e. yes-no tests over quantum systems. Each effect can be represented as a positive matrix smaller than the identity in the Löwner order. We denote the set of effects on the d-dimensional $\mathcal{H}_Q$ as $Ef_Q = \left\{\, E \in \mathbb{C}^{d\times d} \mid 0_Q \sqsubseteq E \sqsubseteq \mathbb{I}_Q \,\right\}$, where $\mathbb{I}_Q$ is the $d \times d$ identity operator over the Hilbert space $\mathcal{H}_Q$. The probability of getting a "yes" outcome when measuring an effect E on a state ρ is $\mathrm{tr}(E\rho)$, as given by the *Born rule*.

Density operators and effects are dual, as effects are isomorphic (via the Born rule) to the convex functions from the set of density operators to the probability interval.

▶ **Theorem 1** ([18]). *$Ef_Q \cong \mathbf{Conv}(DM_Q, [0,1])$ through the isomorphism $E \mapsto \lambda\rho.\,\mathrm{tr}(E\rho)$.*

Effects can thus be seen as probabilities *parameterized* on an unknown quantum state.

Following this duality, to each superoperator $\mathcal{E} : DM_Q \to DM_{Q'}$ with Kraus operators $\{K_i\}$ corresponds a *dual superoperator* $\mathcal{J} : Ef_{Q'} \to Ef_Q$ (note the inversion), whose Kraus operators are $\{K_i^\dagger\}$. The defining property of such superoperators is $\mathrm{tr}(E \cdot \mathcal{E}(\rho)) = \mathrm{tr}(\mathcal{J}(E) \cdot \rho)$.

In general, a measurement with n different outcomes is a set $\{E_1, \ldots, E_n\}$ of effects satisfying the *completeness* equation $\sum_{i=1}^n E_i = \mathbb{I}$. The probability of the i outcome occurring is again given by the Born rule $p_i = \mathrm{tr}(E_i\rho)$.

As examples of measurements, consider M_{01} and $M_{\pm}$ that project a qubit state into the elements of the computational and Hadamard basis, respectively, with M_{01} defined as $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and $M_{\pm}$ as $\{|+\rangle\langle +|, |-\rangle\langle -|\}$. Applying the measurement M_{01} on $|0\rangle$ returns the outcome associated with $|0\rangle\langle 0|$ with probability 1. When measuring instead $|+\rangle$ the same result occurs with probability $\frac{1}{2}$. For measurements over registers, we allow composing effects via the $\boxtimes$ tensor product. Note that a measurement may measure only some of the qubits of a register, e.g. $\{|0\rangle\langle 0| \boxtimes \mathbb{I}, |1\rangle\langle 1| \boxtimes \mathbb{I}\}$ measures (in the computational basis) the first qubit.

3 Effect-Based Models

We generalize probability distributions and pLTSs to effect distributions and eLTSs, and we investigate which properties of probability distributions can be lifted to the quantum case. We adapt the two most used definitions of bisimilarity for pLTS to eLTS, namely, the *Aczel-Mendler* and *Larsen-Skou* bisimilarities. Even if the two coincide in the probabilistic case, this is not the same for eLTSs, and we argue that the latter is adequate for comparing the behaviour of quantum systems.

3.1 Effect Distribution

Given a set of qubits Q, we introduce effect distributions, i.e. functions associating each element of a given set X with some effect in Ef_Q.

▶ **Definition 2.** *Let $Q \subseteq \mathbf{Q}$. The set of* finite Ef_Q-(sub)distributions *over a set X is*

$$\mathcal{Q}_Q X = \left\{ \mathfrak{D} \in {Ef_Q}^X \;\middle|\; \mathrm{supp}(\mathfrak{D}) \text{ is finite and } \sum_{x \in \mathrm{supp}(\mathfrak{D})} \mathfrak{D}(x) \sqsubseteq \mathbb{I}_Q \right\}$$

where $\mathrm{supp}(\mathfrak{D})$ *is the support of $\mathfrak{D}$, i.e. the set* $\{ x \in X \mid \mathfrak{D}(x) \neq 0_Q \}$. *We say that a distribution $\mathfrak{D}$ is* full *when* $\sum_{x \in \mathrm{supp}(\mathfrak{D})} \mathfrak{D}(x) = \mathbb{I}_Q$.

Effect distributions are a conservative generalization of probability distributions. More in detail, 1×1 positive matrices are isomorphic to real numbers, hence $\mathcal{Q}_\emptyset X$ coincides with the usual set of probability distributions $\mathcal{D}X$.

We represent effect distributions as sets of pairs $\mathfrak{D} = \{x_1 \rhd E_1, x_2 \rhd E_2, \ldots, x_n \rhd E_n\}$ with possibly repeated x_i, meaning $\mathfrak{D}(x) = \sum_{x_i = x} E_i$. For example, $\{x \rhd E_1, x \rhd E_2, y \rhd E_3\}$ and $\{x \rhd E_1 + E_2, y \rhd E_3\}$ denote the same distribution.

▶ **Example 3.** Let $X = \{x, y\}$. The distribution $\mathfrak{D} = \{x \rhd \frac{1}{2}, y \rhd \frac{1}{2}\}$ is indeed just a uniform probability distribution, i.e. an effect distribution in the 1-dimensional Hilbert space $\mathcal{H}_\emptyset$.

Two more interesting effect distributions, in the two-dimensional Hilbert space $\mathcal{H}_{\{q_1\}}$, are $\mathfrak{G} = \{x \rhd \frac{1}{2}\mathbb{I}, y \rhd \frac{1}{2}\mathbb{I}\}$ and $\mathfrak{T} = \{x \rhd |0\rangle\langle 0|, y \rhd |1\rangle\langle 1|\}$. Both represent a measurement performed on q_1: $\mathfrak{G}$ returns the outcomes x and y with the same probability, regardless of the state of q_1; while $\mathfrak{T}$ returns x when it observes $|0\rangle\langle 0|$ and y when it observes $|1\rangle\langle 1|$.

Since effects can be regarded as functions from states to probabilities, an effect distribution $\mathfrak{D} \in \mathcal{Q}_Q X$ denotes a function $\mathfrak{D}{\downarrow}\_ \in (\mathcal{D}X)^{DM_Q}$ associating a $\rho \in DM_Q$ with the probability distribution $\mathfrak{D}{\downarrow_\rho}$ such that $\mathfrak{D}{\downarrow_\rho}(x) = \mathrm{tr}(\mathfrak{D}(x) \cdot \rho)$ for any $x \in X$. Hence, an effect distribution corresponds to the parameterized probabilistic outcome of performing a finite destructive measurement on some unknown input quantum state.

In particular, we have the following isomorphism (formally, a convex set isomorphism).

▶ **Theorem 4.** *Effect distributions correspond to all and only the parameterized sub-probability distributions that are convex and have an "overall" finite support.*

$$\mathcal{Q}_Q \cong \left\{ \mathfrak{D}{\downarrow_{\_}} \in (\mathcal{D}X)^{DM_Q} \;\middle|\; \mathfrak{D}{\downarrow_{\rho\,{}_p\!\oplus\,\sigma}} = (\mathfrak{D}{\downarrow_\rho})\;{}_p\!\oplus\;(\mathfrak{D}{\downarrow_\sigma}) \text{ and } \bigcup_{\rho\in DM_Q} \mathrm{supp}(\mathfrak{D}{\downarrow_\rho}) \text{ is finite} \right\}$$

This isomorphism tells us that we can see effect distributions as measurements.

▶ **Example 5.** Consider $\mathfrak{T}$ of Example 3 and the quantum input $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$. The probability distribution $\mathfrak{T}{\downarrow_\rho}$ maps x to $\frac{3}{4}$ and y to $\frac{1}{4}$. Intuitively, $\mathfrak{T}{\downarrow_\rho}$ corresponds to the probabilistic outcome of performing the measurement $\mathfrak{T}$ over a system in state ρ.

As for probabilities, we compose effect distributions via an effect-weighted sum, provided that they are defined over different qubits. This is a partial operation, being $E \boxtimes F$ defined only when E and F uses disjoint sets of qubits.

▶ **Definition 6.** *Given a family of Ef_Q-distributions $\{\mathfrak{D}_i\}_{i\in I}$ and effects $\{E_i\}_{i\in I}$ in $Ef_{Q'}$ where $Q \cap Q' = \emptyset$ and such that $\sum_{i\in I} E_i \sqsubseteq \mathbb{I}$, the weighted sum $\sum_{i\in I} E_i \boxtimes \mathfrak{D}_i$ is the $Ef_{Q\uplus Q'}$-distribution defined as $(\sum_{i\in I} E_i \boxtimes \mathfrak{D}_i)(x) = \sum_{i\in I} E_i \boxtimes \mathfrak{D}_i(x)$.*

This composition coincides with the usual weighted sum of probability distributions if $Q = Q' = \emptyset$. Intuitively, $\mathfrak{D}$ measures some qubits to choose between the distributions $\mathfrak{D}_i$ (which in turn behave accordingly to the remaining qubits). We will sometimes write $E_1 \boxtimes \mathfrak{D}_1 + \cdots + E_n \boxtimes \mathfrak{D}_n$ for $\sum_i E_i \boxtimes \mathfrak{D}_i$.

▶ **Example 7.** Take $\mathfrak{G}, \mathfrak{T}$ of Example 3. The $Ef_{\{q_1,q_2\}}$-distribution $(|+\rangle\langle +| \boxtimes \mathfrak{G}) + (|-\rangle\langle -| \boxtimes \mathfrak{T})$ can be rewritten as $\{x \rhd \mathbb{I}\otimes\frac{1}{2}|+\rangle\langle +|, y \rhd \mathbb{I}\otimes\frac{1}{2}|+\rangle\langle +|, x \rhd |0-\rangle\langle 0-|, y \rhd |1-\rangle\langle 1-|\}$. Intuitively, this represents the following cascade of two measurements: first measure the qubit q_2 over the Hadamard basis, if it is in $|+\rangle$ then return either x or y with the same probability, otherwise measure the qubit q_1 in the computational basis and return x or y accordingly.

In the probabilistic case, it is usual to consider just the binary composition $\Delta\;{}_p\!\oplus\;\Theta$. This is a safe simplification as any finite probability distribution can be obtained by repeatedly applying ${}_p\!\oplus$ over point distributions. Unfortunately, this is not the case for effect distributions in general, as we show in the following.

▶ **Definition 8.** *Let $\mathfrak{D}\;{}_E\!\boxplus\;\mathfrak{T}$ be the weighted sum $E \boxtimes \mathfrak{D} + (\mathbb{I} - E) \boxtimes \mathfrak{T}$.*

Some effect distributions with support bigger than two can be defined by a nesting of ${}_E\!\boxplus$ expressions over point distributions.

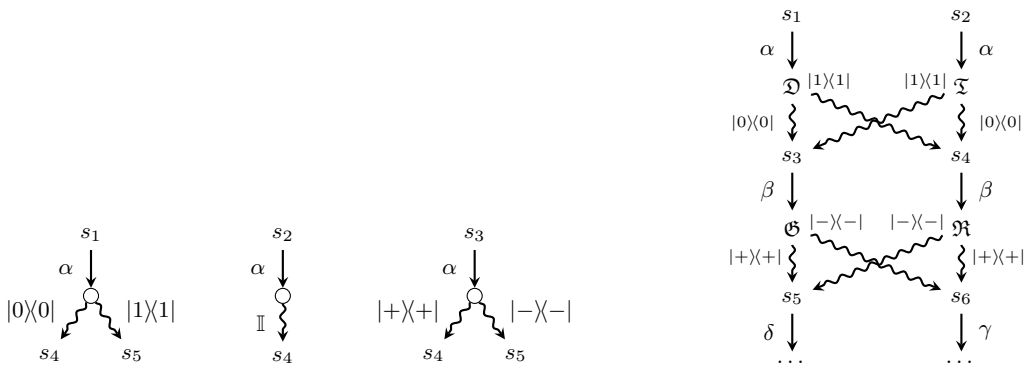
▶ **Example 9.** The distribution $\{x_1 \rhd |0+\rangle\langle 0+|, x_2 \rhd |0-\rangle\langle 0-|, x_3 \rhd |1+\rangle\langle 1+|, x_4 \rhd |1-\rangle\langle 1-|\}$ over $S = \{x_1, x_2, x_3, x_4\}$ can be obtained as $(\overline{x_1}\;{}_{|+\rangle\langle +|}\!\boxplus\;\overline{x_2})\;{}_{|0\rangle\langle 0|}\!\boxplus\;(\overline{x_3}\;{}_{|+\rangle\langle +|}\!\boxplus\;\overline{x_4})$.

We define now the set of distributions that can be obtained starting from point distributions and applying (an arbitrary number of times) the binary operator $\boxplus$.

▶ **Definition 10.** *Given a set X, let $\mathcal{Q}^{\boxplus}X$ be the least family of sets $\mathcal{Q}^{\boxplus}_Q X \subseteq \mathcal{Q}_Q X$ such that $\overline{x} \in \mathcal{Q}^{\boxplus}_\emptyset X$ for any $x \in X$, and if $\mathfrak{D}, \mathfrak{T} \in \mathcal{Q}^{\boxplus}_Q X$ then $\mathfrak{D}\;{}_E\!\boxplus\;\mathfrak{T} \in \mathcal{Q}^{\boxplus}_{Q\uplus Q'} X$ for any $E \in Ef_{Q'}$.*

Despite having finite support, some effect distributions cannot be defined using $\boxplus$, roughly because of entangled pairs. Hence, we will use the general n-ary composition.

▶ **Theorem 11.** *If $|X| \geq 4$ and $|Q| \geq 2$, with $|\cdot|$ the cardinality, then $\mathcal{Q}^{\boxplus}_Q X \neq \mathcal{Q}_Q X$.*



(a) The eLTS of Example 16.

(b) An eLTS where $s_1 \not\sim_{lpp} s_2$.

Figure 1 Examples of eLTSs.

As it is common for the probabilistic case, it is sometimes useful to see a relation between elements of a given set X as a relation over effect distributions over X. In particular, we lift a relation on states to one on effect distributions of states by taking the smallest relation that pairs the point distributions of related states and that is closed for weighted composition.

▶ **Definition 12.** *Given $\mathcal{R} \subseteq X \times X$, we let the* effect liftings *of $\mathcal{R} \subseteq X \times X$ be the least family of relations $\widehat{\mathcal{R}}_Q \subseteq \mathcal{Q}_Q X \times \mathcal{Q}_Q X$ such that $\overline{s}\,\widehat{\mathcal{R}}_\emptyset\,\overline{t}$ if $s\,\mathcal{R}\,t$, and for each $E_i \in Ef_Q$, $\mathfrak{D}_i\,\widehat{\mathcal{R}}_{Q'}\,\mathfrak{T}_i$ implies $(\sum_{i\in I} E_i \boxtimes \mathfrak{D}_i)\,\widehat{\mathcal{R}}_{Q\uplus Q'}\,(\sum_{i\in I} E_i \boxtimes \mathfrak{T}_i)$.*

Note that $\widehat{\mathcal{R}}_\emptyset$ is the usual probabilistic lifting of [19], and we denote it as $\mathring{\mathcal{R}}$. In the following we often omit Q when clear from the context. We recover the following property, known as decomposability, roughly stating that two distributions are paired by the lifting of a relation when they can be decomposed in such a way that they associate related states with the same effects.

▶ **Lemma 13.** *For all $\mathcal{R}$, $\mathfrak{D}\,\widehat{\mathcal{R}}_Q\,\mathfrak{T}$ iff there exist a set of indices I and a set of effects $\{E_i \in Ef_Q\}_{i\in I}$ such that $\mathfrak{D} = \{x_i \rhd E_i\}_{i\in I}$, $\mathfrak{T} = \{y_i \rhd E_i\}_{i\in I}$, and $x_i\,\mathcal{R}\,y_i$ for any $i \in I$.*

3.2 Effect Transition Systems and their Bisimilarity

To model quantum systems and protocols we introduce effect labelled transition systems (eLTSs). Then we investigate different notions of bisimilarity.

▶ **Definition 14.** *An eLTS over Ef_Q is a triple $(S, Act, \to)$ where S is a set of states, Act is a set of labels, and $\to \subseteq S \times Act \times \mathcal{Q}_Q S$ is a transition relation.*

Hereafter, we assume a set of qubits Q and an eLTS $(S, Act, \to)$ over Ef_Q, and we write $s \xrightarrow{\mu} \mathfrak{D}$ for $(s, \mu, \mathfrak{D}) \in \to$.

We instantiate two distinct definitions of semantic equivalence on quantum systems: *Aczel-Mendler* and *Larsen-Skou* bisimilarities [33]. They are known to coincide on classical probabilistic processes [19]. Notably, they do not in the quantum case.

▶ **Definition 15.** *A symmetric relation $\mathcal{R} \subseteq S \times S$ is an* AM-bisimulation *if for any $s\,\mathcal{R}\,t$*

if $s \xrightarrow{\mu} \mathfrak{D}$ then $t \xrightarrow{\mu} \mathfrak{T}$ for some $\mathfrak{T}$ such that $\mathfrak{D}\,\widehat{\mathcal{R}}_Q\,\mathfrak{T}$

Let AM-bisimilarity *$\sim_{am}$ be the largest AM-bisimulation.*

▶ **Example 16.** Consider the eLTS in Figure 1a with states $\{s_1, s_2, s_3, s_4, s_5\}$ and transitions $s_1 \xrightarrow{\alpha} \mathfrak{D} = \{s_4 \rhd |0\rangle\langle 0|, s_5 \rhd |1\rangle\langle 1|\}$, $s_2 \xrightarrow{\alpha} \mathfrak{G} = \{s_4 \rhd \mathbb{I}\}$, $s_3 \xrightarrow{\alpha} \mathfrak{T} = \{s_4 \rhd |+\rangle\langle +|, s_5 \rhd |-\rangle\langle -|\}$. Note that s_4 and s_5 are deadlock states, hence $s_4 \sim_{am} s_5$. Moreover, $s_1 \sim_{am} s_2 \sim_{am} s_3$, because $|0\rangle\langle 0| + |1\rangle\langle 1| = I = |+\rangle\langle +| + |-\rangle\langle -|$, and hence

$$\mathfrak{D} \mathrel{\widehat{\sim}_{am}} \{s_4 \rhd |0\rangle\langle 0|, s_4 \rhd |1\rangle\langle 1|\} = \mathfrak{G} = \{s_4 \rhd |+\rangle\langle +|, s_4 \rhd |-\rangle\langle -|\} \mathrel{\widehat{\sim}_{am}} \mathfrak{T}.$$

Still, $s_1 \not\sim_{am} s_3$, as we cannot write $\mathfrak{D}$ and $\mathfrak{T}$ with the same effects as required by Lemma 13.

This example, inspired by [32], proves that $\sim_{am}$ is not transitive. We thus generalize *Larsen-Skou bisimilarity* [26] (named kernel bisimilarity in [33]) to the quantum case.

▶ **Definition 17.** *An equivalence relation $\mathcal{R} \subseteq S \times S$ is an* LS-bisimulation *if for any $s \mathcal{R} t$*

if $s \xrightarrow{\mu} \mathfrak{D}$ then $t \xrightarrow{\mu} \mathfrak{T}$ for some $\mathfrak{T}$ such that $\forall C \in S/_{\mathcal{R}} \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x)$

with $S/_{\mathcal{R}}$ the equivalence classes of S. Let LS-bisimilarity $\sim_{ls}$ *be the largest LS-bisimulation.*

We show that $\sim_{ls}$ behaves differently from $\sim_{am}$, and indeed it is strictly coarser.

▶ **Example 18.** Consider Example 16. We can see that $s_1 \sim_{ls} s_3$ as both $\mathfrak{D}$ and $\mathfrak{T}$ associate the equivalence class $\{s_4, s_5\}$ with the effect $\mathbb{I}$.

▶ **Theorem 19.** *For any eLTS over Ef_Q with states S, $\sim_{am} \subseteq \sim_{ls}$. Moreover, $\sim_{am} = \sim_{ls}$ if $Q = \emptyset$, and $\sim_{am} \subsetneq \sim_{ls}$ if Q is of dimension at least 2 and S of cardinality at least 4.*

LS-bisimilarity is also trivially an equivalence relation. In the following we discuss its adequacy as quantum semantic equivalence.

Our ground truth is that bisimilar processes must exhibit the same probabilistic behaviour, as it is the only observable property of quantum systems. We therefore define a parameterized version of probabilistic bisimilarity for eLTSs, stating that equivalent states should express the same probabilistic behaviour when instantiated with any possible quantum state. More precisely, for each ρ, we define a ρ-bisimilarity equating states that are probabilistically bisimilar when each effect distribution is instantiated with ρ to obtain a probability distribution.

▶ **Definition 20.** *Given $\rho \in DM_Q$, a symmetric relation $\mathcal{R} \subseteq S \times S$ is a* ρ-bisimulation *if for any $s \mathcal{R} t$*

if $s \xrightarrow{\mu} \mathfrak{D}$ then $t \xrightarrow{\mu} \mathfrak{T}$ for some $\mathfrak{T}$ such that $\mathfrak{D}{\downarrow_\rho} \mathrel{\mathring{\mathcal{R}}} \mathfrak{T}{\downarrow_\rho}$

Let ρ-bisimilarity $\sim_\rho$ *be the largest ρ-bisimulation. We define* probabilistic behavioural equivalence $\simeq_{pbe}$ *as the relation pairing states that are indistinguishable when every possible quantum state is considered, i.e. $\simeq_{pbe} = \bigcap_{\rho \in DM_Q} \sim_\rho$.*

In other words, an adversary trying to disprove $s \simeq_{pbe} t$ can test their probabilistic behaviour on any arbitrary input state ρ, looking for one such that $s \not\sim_\rho t$. One could hypothesize an even stronger adversary, with the faculty of choosing a different input state at each step of the computation, not just once at the beginning as for $\simeq_{pbe}$. We formalize this notion as *locally-parameterized probabilistic bisimilarity*, and we investigate how $\sim_{ls}$ relates with both these behavioural equivalences.

▶ **Definition 21.** *A symmetric relation $\mathcal{R} \subseteq S \times S$ is a* lpp-bisimulation *if for any $s\,\mathcal{R}\,t$*

if $s \xrightarrow{\mu} \mathfrak{D}$ then $t \xrightarrow{\mu} \mathfrak{T}$ for some $\mathfrak{T}$ such that $\mathfrak{D}{\downarrow_\rho}\ \mathring{\mathcal{R}}\ \mathfrak{T}{\downarrow_\rho}$ for any $\rho \in DM_Q$

Let lpp-bisimilarity $\sim_{lpp}$ *be the largest lpp-bisimulation.*

We exemplify the difference between $\simeq_{pbe}$ and $\sim_{lpp}$ below.

▶ **Example 22.** Consider the eLTS in Figure 1b, where s_5 and s_6 are immediately distinguishable as they perform different visible actions. To show that $s_1 \not\sim_{lpp} s_2$ it suffices to choose $|0\rangle\langle 0|$ for their first reduction and $|+\rangle\langle +|$ for the second one. Formally, since $\mathfrak{D}{\downarrow_{|0\rangle\langle 0|}} = \overline{s_3}$ and $\mathfrak{T}{\downarrow_{|0\rangle\langle 0|}} = \overline{s_4}$, we must have that $s_3 \sim_{lpp} s_4$. But $\mathfrak{G}{\downarrow_{|+\rangle\langle +|}} = \overline{s_5}$ and $\mathfrak{R}{\downarrow_{|+\rangle\langle +|}} = \overline{s_6}$. Thus, $s_3 \sim_{lpp} s_4$ requires $s_5 \sim_{lpp} s_6$, which does not hold.

Finally, note that neither $\sim_{|0\rangle\langle 0|}$ nor $\sim_{|+\rangle\langle +|}$ are capable of distinguishing s_1 and s_2, as indeed $\mathfrak{G}{\downarrow_{|0\rangle\langle 0|}} = \mathfrak{R}{\downarrow_{|0\rangle\langle 0|}}$ and $\mathfrak{D}{\downarrow_{|+\rangle\langle +|}} = \mathfrak{T}{\downarrow_{|+\rangle\langle +|}}$.

Using Theorem 4, we prove that $\sim_{ls}$ is adequate for characterizing $\sim_{lpp}$.

▶ **Theorem 23.** *For any $s, t \in S$, $s \sim_{ls} t$ if and only if $s \sim_{lpp} t$.*

Quite surprisingly, for finite eLTSs the two relations $\sim_{lpp}$ and $\simeq_{pbe}$ coincide.

▶ **Theorem 24.** *For any $s, t \in S$, $s \sim_{ls} t$ implies $s \simeq_{pbe} t$. Moreover, if S is finitely dimensional, then $s \simeq_{pbe} t$ implies $s \sim_{ls} t$.*

The interesting case is for $\simeq_{pbe} \subseteq \sim_{ls}$, where we consider the (finite) set of effects $\mathbb{E}$ that may appear in the eLTS, and we build a density operator $\rho_{\mathbb{E}}$ that distinguishes all the effects in $\mathbb{E}$. Roughly, $\sim_\rho$ requires associating the same probability to all the equivalence classes of states, but this can only be the case when the associated effects are the same for $\rho = \rho_{\mathbb{E}}$. Indeed, a single quantum state is sufficient for distinguishing s_1 and s_2 of Example 22.

▶ **Example 25.** Consider Example 22, and let $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$. Then $s_1 \not\sim_\rho s_2$ (and hence $s_1 \not\simeq_{pbe} s_2$). Note that $\mathfrak{D}{\downarrow_\rho} = \overline{s_3}\ {}_{\frac{3}{4}}\!\oplus \overline{s_4}$ and $\mathfrak{T}{\downarrow_\rho} = \overline{s_3}\ {}_{\frac{1}{4}}\!\oplus \overline{s_4}$. For s_1 to be ρ-bisimilar to s_2, it must be that $s_3 \sim_\rho s_4$, which is false since $\mathfrak{G}{\downarrow_\rho} = \overline{s_5}\ {}_{\frac{3}{4}}\!\oplus \overline{s_6}$ and $\mathfrak{R}{\downarrow_\rho} = \overline{s_5}\ {}_{\frac{1}{4}}\!\oplus \overline{s_6}$.

We thus have shown that two bisimilar processes behave the same under any possible quantum input. Nonetheless, LS-bisimilarity is still decidable in an efficient way, thanks to the finite representation of effects. The partition refinement algorithm proposed in [22], for example, could promptly be adapted to our eLTSs. More in detail, that algorithm is parametric with respect to the *functor* used to specify the visible labels and the weights of a generic transition system, which in the case of eLTSs are Act and the effects in $\mathbb{C}^{d\times d}$.

We conclude the section by introducing a *partial evaluation* operator relating eLTSs over different sets of qubits, namely instantiating some of the expected input qubits of the former to some specific state.

▶ **Definition 26.** *Given an eLTS $\mathbb{S} = (S, Act, \to_1)$ over Ef_Q and $\rho \in DM_{Q'}$, with $Q' \subseteq Q$, the partial evaluation of $\mathbb{S}$ with ρ is the eLTS over $Ef_{Q\setminus Q'}$ defined as $(S', Act, \to)$, where $S' = \{s|_\rho \mid s \in S\}$ and $\to$ is the smallest relation satisfying the following rule.*

$$\frac{s \xrightarrow{\mu}_1 \{s_i \rhd E_i\}_{i\in I}}{s|_\rho \xrightarrow{\mu} \{s_i|_\rho \rhd \mathrm{tr}_{Q'}(E_i(\rho \boxtimes \mathbb{I}_{Q\setminus Q'}))\}_{i\in I}}\ \textsc{PEval}$$

▶ **Example 27.** Figure 2 shows an eLTS over two qubits and its partial evaluation (of the first qubit) with $\rho = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|1\rangle\langle 1|$.

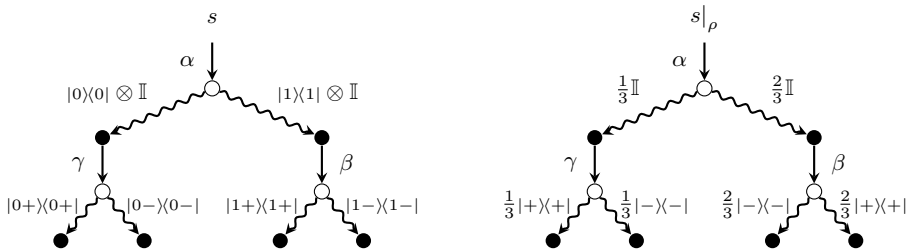


Figure 2 Partial evaluation of the first qubit of the eLTS on the left with $\rho = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|1\rangle\langle 1|$.

LS-bisimilarity is preserved by partial evaluation.

▶ **Theorem 28.** *If $s \sim_{ls} t$ then $s|_\rho \sim_{ls} t|_\rho$.*

For ρ large enough, the partial evaluation returns a pLTS obtained by applying the same quantum input to each effect distribution of the eLTS. Hence, $s|_\rho \sim_{ls} t|_\rho$ corresponds to verifying $s \sim_\rho t$, and the following is a corollary of Theorem 24.

▶ **Corollary 29.** *Given a finite eLTS $(S, Act, \to)$ over Ef_Q and $s, t \in S$, if for any $\rho \in DM_Q$ we have $s|_\rho \sim_{ls} t|_\rho$, then $s \sim_{ls} t$.*

Having found that $\sim_{ls}$ satisfies all our desiderata for a quantum behavioural equivalence, we will denote it simply as $\sim$ for the rest of the paper.

4 Modelling a Minimal Process Algebra with eLTSs

We explore how eLTSs can model concurrent communicating quantum systems by considering a *minimal Quantum Process Algebra (mQPA)* featuring non-deterministic and parallel composition of processes, synchronization, restriction, measurements and application of unitaries. For synchronization, we assume that the set of actions Act contains a distinguished element τ, and that every other label $\alpha \in Act$ has in inverse $\overline{\alpha}$ that is involutive, i.e. such that $\overline{\overline{\alpha}} = \alpha$. We equip our algebra with two distinct semantics: a standard *Schrödinger* stateful pLTS semantics that depends on the quantum input, and a *Heisenberg* eLTS semantics that does not. Both are based on configurations, pairing the processes with superoperators in the latter, and density operators in the former, as it is common in the literature [8, 9, 7]. We prove that the two coincide: we can use bisimilarity in the Heisenberg eLTS to prove probabilistic bisimilarity in all the Schrödinger pLTSs.

▶ **Definition 30.** *An mQPA process P is defined below, with $\mu \in Act$ an action and $\sum_i E_i = \mathbb{I}$.*

$$P ::= \mathbf{0} \mid P + P \mid P \parallel P \mid P \setminus \alpha \mid \mu.([E_i]P_i)_{i \in I} \mid U; P$$

As usual, $\mathbf{0}$ stands for a deadlock process, and the meaning of parallel, non-deterministic sum and restriction is as expected. A prefix $\mu.([E_i]P_i)_{i \in I}$ represents an action μ followed by a destructive measurement over the qubits of E_i, whose outcome controls the evolution of the process. Finally, $U; P$ behaves as P would over a state that has been modified by U. Recall that unitaries and effects symbols come with the set of qubits they act on. Moreover, we assume such sets disjoint when needed (enforced e.g. by a type system [7]). More in detail, the sets of qubits used in (unitaries and measurements of) the parallel processes P and R of $P \parallel R$ must be disjoint, and the qubits measured by E_i in $\mu.([E_i]P_i)$ cannot be used by P_i. On the same line, we let Q_P be the smallest set containing the qubits used in the effects and unitaries of P. Finally, we often write $\mu.P$ in place of $\mu.([1]P)$, and μ for the process $\mu.\mathbf{0}$.

$$\frac{\rho_i = \mathcal{M}_{E_i}(\rho)}{\langle \rho, \mu.([E_i]s_i)_{i\in I}\rangle \xrightarrow{\mu} \{\langle \rho_i, s_i\rangle \rhd \mathrm{tr}(\rho_i)\}_{i\in I}}\ \textsc{SPre} \qquad \frac{\langle \mathcal{U}(\rho), s\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \rho, U; s\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{SU}$$

$$\frac{\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \rho_i, s_i\rangle \rhd p_i\}_{i\in I} \quad \mu \neq \alpha \quad \mu \neq \overline{\alpha}}{\langle \rho, s \setminus \alpha\rangle \xrightarrow{\mu} \{\langle \rho_i, s_i \setminus \alpha\rangle \rhd p_i\}_{i\in I}}\ \textsc{SRes}$$

$$\frac{\langle \rho, s\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \rho, s + t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{SSumL} \qquad \frac{\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \rho_i, s_i\rangle \rhd p_i\}_{i\in I}}{\langle \rho, s \parallel t\rangle \xrightarrow{\mu} \{\langle \rho_i, s_i \parallel t\rangle \rhd p_i\}_{i\in I}}\ \textsc{SParL}$$

$$\frac{\langle \rho, t\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \rho, s + t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{SSumR} \qquad \frac{\langle \rho, t\rangle \xrightarrow{\mu} \{\langle \rho_j, t_j\rangle \rhd p_j\}_{j\in J}}{\langle \rho, s \parallel t\rangle \xrightarrow{\mu} \{\langle \rho_j, s \parallel t_j\rangle \rhd p_j\}_{j\in J}}\ \textsc{SParR}$$

$$\frac{\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \rho_i, s_i\rangle \rhd p_i\}_{i\in I} \quad \langle \rho_i, t\rangle \xrightarrow{\overline{\mu}} \{\langle \rho_j, t_j\rangle \rhd p_j\}_{j\in J_i}}{\langle \rho, s \parallel t\rangle \xrightarrow{\tau} \{\langle \rho_j, s_i \parallel t_j\rangle \rhd p_j\}_{(i,j)\in I\times J_i}}\ \textsc{SSynL}$$

$$\frac{\langle \rho, t\rangle \xrightarrow{\mu} \{\langle \rho_i, t_i\rangle \rhd p_i\}_{i\in I} \quad \langle \rho_i, s\rangle \xrightarrow{\overline{\mu}} \{\langle \rho_{ij}, s_j\rangle \rhd p_{ij}\}_{j\in J}}{\langle \rho, s \parallel t\rangle \xrightarrow{\tau} \{\langle \rho_{ij}, s_i \parallel t_j\rangle \rhd p_{ij}\}_{(i,j)\in I\times J}}\ \textsc{SSyncR}$$

(a) Rules for Schrödinger stateful semantics.

$$\frac{}{\langle \mathcal{E}, \mu.([E_i]s_i)_{i\in I}\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i} \circ \mathcal{E}, s_i\rangle \rhd \mathcal{Z}(E_i \boxtimes \mathbb{I})\}_{i\in I}}\ \textsc{HPre} \qquad \frac{\langle \mathcal{U} \circ \mathcal{E}, s\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \mathcal{E}, U; s\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{HU}$$

$$\frac{\langle \mathcal{E}, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle \rhd E_i\}_{i\in I} \quad \mu \neq \alpha \quad \mu \neq \overline{\alpha}}{\langle \mathcal{E}, s \setminus \alpha\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i \setminus \alpha\rangle \rhd E_i\}_{i\in I}}\ \textsc{HRes}$$

$$\frac{\langle \mathcal{E}, s\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \mathcal{E}, s + t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{HSumL} \qquad \frac{\langle \mathcal{E}, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle \rhd E_i\}_{i\in I}}{\langle \mathcal{E}, s \parallel t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i \parallel t\rangle \rhd E_i\}_{i\in I}}\ \textsc{HParL}$$

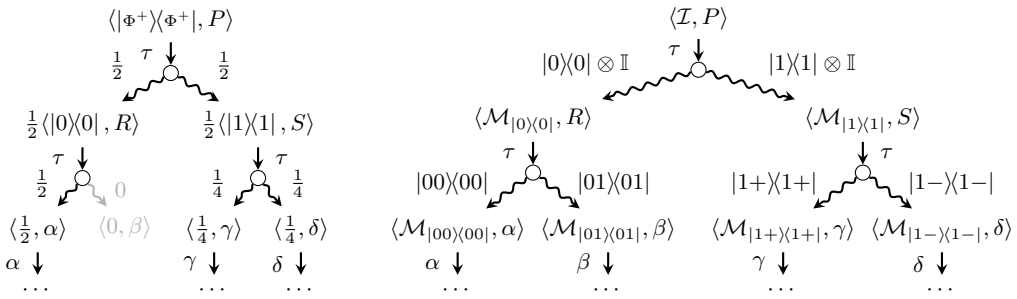
$$\frac{\langle \mathcal{E}, t\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \mathcal{E}, s + t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{HSumR} \qquad \frac{\langle \mathcal{E}, t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_j, s_j\rangle \rhd E_j\}_{j\in J}}{\langle \mathcal{E}, s \parallel t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_j, s \parallel t_j\rangle \rhd E_j\}_{j\in J}}\ \textsc{HParR}$$

$$\frac{\langle \mathcal{E}, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle \rhd E_i)\}_{i\in I} \quad \langle \mathcal{E}_i, t\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_j, t_j\rangle \rhd E_j\}_{j\in J_i}}{\langle \mathcal{E}, s \parallel t\rangle \xrightarrow{\tau} \{\langle \mathcal{E}_j, s_i \parallel t_j\rangle \rhd E_j\}_{(i,j)\in I\times J_i}}\ \textsc{HSyncL}$$

$$\frac{\langle \mathcal{E}, t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_j, t_j\rangle \rhd E_J)\}_{j\in J} \quad \langle \mathcal{E}_j, s\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_i, s_i\rangle \rhd E_i\}_{i\in I_j}}{\langle \mathcal{E}, s \parallel t\rangle \xrightarrow{\tau} \{\langle \mathcal{E}_i, s_i \parallel t_j\rangle \rhd E_i\}_{(j,i)\in J\times I_j}}\ \textsc{HSyncR}$$

(b) Rules for Heisenberg stateless semantics.

Figure 3 Rules for stateful and stateless semantics of mQPA.



(a) Schrödinger semantics of P. **(b)** Heisenberg semantics of P.

Figure 4 Our two semantics for the process P of Example 32.

We consider an operational, stateful semantics in the style of [7, 9, 12] for mQPA given in terms of a pLTS, where each state is the pairing of a density operator and a process. Being state-based, we name this Schrödinger semantics.

▶ **Definition 31.** *The Schrödinger semantics of mQPA is given by a pLTS whose states are pairs $\langle \rho, P\rangle$ for P mQPA process and $\rho \in DM_{Q'}$ density operator with $Q' \supseteq Q_P$, and where the transition is the smallest relation satisfying the rules in Figure 3a.*

The SPre rule updates the quantum state through the destructive measurement operator $\mathcal{M}_{E_i} : DM_Q \to DM_{Q'}$ associated to the effect $E_i \in Ef_{Q\setminus Q'}$ defined by $\mathcal{M}_{E_i}(\rho) = \mathrm{tr}_{Q\setminus Q'}((\sqrt{E_i} \boxtimes \mathbb{I}_{Q'})\rho(\sqrt{E_i} \boxtimes \mathbb{I}_{Q'}))$. Given the unitary U acting on qubits Q_U, the SU rule updates the state with the superoperator $\mathcal{U} : DM_Q \to DM_Q$, defined as $\mathcal{U}(\rho) = (U \boxtimes \mathbb{I}_{Q\setminus Q_U})\rho(U^\dagger \boxtimes \mathbb{I}_{Q\setminus Q_U})$.

Note that the resulting effect distribution is always a probability distribution, obtained by tracing the resulting density operator. We remark that SSyncL and SSyncR only differ in the order of the application of measurements between the two branches of the parallel operator, as both the orderings are possible.

▶ **Example 32.** Consider a process $P = \tau.([|0\rangle\langle 0|]R, [|1\rangle\langle 1|]S)$ with $R = \tau.([|0\rangle\langle 0|]\alpha, [|1\rangle\langle 1|]\beta)$ and $S = H;\tau.([|0\rangle\langle 0|]\gamma, [|1\rangle\langle 1|]\delta)$. First, P measures a qubit q_1 in the computational basis and then measures a qubit q_2 either in the computational or in the Hadamard basis. The stateful semantics of $\langle |\Phi^+\rangle\langle\Phi^+|, P\rangle$ is given in Figure 4a. Notice that measurements are destructive and are always prefixed by an action (which is not necessarily a τ as in [9, 7]).

For any process P, the stateful semantics results in infinitely many pLTSs according to the input quantum state ρ. We seek an alternative stateless characterization, hence adequate for algorithmic verification. We therefore give a new semantics for mQPA processes in terms of eLTSs. We name this Heisenberg semantics, because its focus is on the effects used as weights, rather than on the quantum state. Moreover, it is a symbolic semantics, as it is independent of the input state.

▶ **Definition 33.** *The Heisenberg semantics of mQPA with respect to a chosen set Q of qubits is given by an eLTS over Ef_Q whose states are pairs $\langle \mathcal{E}, P\rangle$ for P mQPA process and $\mathcal{E} \in DM_Q \to DM_{Q'}$ superoperator with $Q \supseteq Q' \supseteq Q_P$, and where the transition is the smallest relation satisfying the rules in Figure 3b.*

The Heisenberg semantics of a process P is the eLTS over Ef_{Q_P} rooted in $\langle \mathcal{I}, P\rangle$. The superoperator $\mathcal{E}$ in the Heisenberg configuration $\langle \mathcal{E}, P\rangle$ records the performed measurements and unitaries. According to that, the weights of the subsequent effect distributions must be

updated through the corresponding dual superoperator $\mathcal{J}$. In the HPRE rule, the superoperator $\mathcal{E} : DM_Q \to DM_{Q'}$ is updated by composition with the measurement superoperator associated to the effect $E_i \in Ef_{Q_m}$, $\mathcal{M}_{E_i} : DM_{Q'} \to DM_{Q' \setminus Q_m}$, where $Q_m \subseteq Q'$ are the measured qubits. The weight resulting from the measurement is $E_i \boxtimes \mathbb{I}$ with $\mathbb{I} \in Ef_{Q' \setminus Q_m}$ meaning that the qubits that are not measured are left unchanged. Finally, the effect is updated via the dual superoperator $\mathcal{J}$ representing the previously applied transformations. All the other rules mirror the Schrödinger semantics.

▶ **Example 34.** Consider the process P of Example 32. Figure 4b shows its Heisenberg semantics. Inside the lowest configurations, we have $\mathcal{M}_{|00\rangle\langle 00|}$, obtained by composing $\mathcal{M}_{|0\rangle\langle 0|}$ over the first qubit with $\mathcal{M}_{|0\rangle\langle 0|}$ over the second qubit, and similarly $\mathcal{M}_{|1+\rangle\langle 1+|} = \mathcal{M}_{|0\rangle\langle 0|} \circ \mathcal{H} \circ \mathcal{M}_{|1\rangle\langle 1|}$.

In order to fix an input state $\rho \in DM_{Q_P}$, and thus instantiate the semantics of the process P, we can use the partial evaluation $\cdot|_\rho$ in Definition 26. Since ρ defines a value for all the qubits used by P, this is a full evaluation: the resulting eLTS is indeed a pLTS.

▶ **Example 35.** Consider the process P of Example 32 and $\rho = |\Phi^+\rangle\langle\Phi^+|$. Notice that $\langle \mathcal{I}, P\rangle|_\rho$, with $\langle \mathcal{I}, P\rangle$ as in Figure 4b, is a pLTS isomorphic to the Schrödinger semantics $\langle \rho, P\rangle$ in Figure 4a. The labels coincide since they are syntax-driven. Furthermore, the weights are identical, since the probabilities of the Schrödinger semantics are exactly the result of applying ρ to the effects in the Heisenberg eLTS.

This example hints at a connection between the two semantics, which is to be expected given the duality between effects and states in quantum theory. Indeed, the eLTSs produced by instantiating the Heisenberg semantics have exactly the same transitions of the Schrödinger semantics, thus the following holds.

▶ **Theorem 36.** *For any process P and $\rho \in DM_{Q_P}$, $\langle \mathcal{I}, P\rangle|_\rho \sim \langle \rho, P\rangle$.*

It follows that we can verify whether two processes are bisimilar for any input just by looking at their Heisenberg semantics.

▶ **Corollary 37.** *Given two processes P and R, $\langle \mathcal{I}, P\rangle \sim \langle \mathcal{I}, R\rangle$ if and only if $\langle \rho, P\rangle \sim \langle \rho, R\rangle$ for any $\rho \in DM_{Q_P}$.*

We conclude with a real-world example: the well-known teleportation protocol [3].

▶ **Example 38.** Alice (**A**) and Bob (**B**) each have a qubit of q_2, q_3, and **A** wants to send its additional qubit q_1 to **B** without a quantum channel. The agents just apply unitaries and measurements on their qubits locally, and synchronize over labels that represent the result of measurements. The protocol is encoded as the following mQPA process **Tel**.

$$\begin{aligned}
\mathbf{Tel} &\coloneqq (\mathbf{A} \parallel \mathbf{B}) \setminus \alpha, \beta, \gamma, \delta \\
\mathbf{A} &\coloneqq \mathit{CNOT}_{q_1 q_2}; H_{q_1} \boxtimes \mathbb{I}_{q_2}; \tau.([|00\rangle\langle 00|]\alpha, [|01\rangle\langle 01|]\beta, [|10\rangle\langle 10|]\gamma, [|11\rangle\langle 11|]\delta) \\
\mathbf{B} &\coloneqq \overline{\alpha}.\mathbf{B}' \;+\; \overline{\beta}.X; \mathbf{B}' \;+\; \overline{\gamma}.Z; \mathbf{B}' \;+\; \overline{\delta}.Z; X; \mathbf{B}'
\end{aligned}$$

where $\mathbf{B}'$ is the unspecified continuation of **B** with q_3.

Then, if q_2 and q_3 are in state $|\Phi^+\rangle\langle\Phi^+|$, as prescribed by the protocol, **Tel** is indistinguishable to $\mathbf{B}'$ acting on q_1 instead of q_3: $\langle \mathcal{I}, \mathbf{Tel}\rangle|_{|\Phi^+\rangle\langle\Phi^+|} \sim \langle \mathcal{I}, \tau.\tau.\mathbf{B}'[q_3/q_1]\rangle$.

5 Related Works

In our work we follow a foundational approach to quantum bisimilarity. We employ effect distributions (a finite non-normalized version of positive operator-valued measures, POVMs [30]) as a generalization of sub-probability distributions, finding them well-suited to model the observable behaviour of quantum systems. Our notion generalizes the quantum monad of [1], which is based on projectors, and it instantiates the abstract "effect algebra monad" of [21]. More in depth, the author in [21] proposes effects monoids, i.e. effect algebras with multiplication, and use them as weights of distributions. Our effects do have tensoring as a multiplication operator, but it does not form a proper effect monoid since it changes the effects dimensions. These works come from the fields of quantum complexity and quantum logic. We apply similar concepts to quantum protocol semantics, introducing eLTSs and studying their composition and their behavioural equivalences.

Our eLTSs can be seen as a labelled, non-deterministic version of the effect-valued Quantum Markov chains of [16], where tensor product is used instead of sequential effect composition. The most general model of "quantum transition system" is the one of [32, 27], where the weights are superoperators instead of effects, to capture also non-destructive measurements and qubit initialization. The author of [32] introduces two different notions of bisimilarity, which we recover in our minimal, effect-based setting as AM and LS bisimilarity. However, none of these works feature non-determinism, nor do they apply the proposed coalgebraic model to process calculi suitable for expressing quantum protocols.

In the literature the semantics of quantum processes is usually described via pLTSs and probabilistic bisimilarity [24, 10, 8, 9, 7]. Despite their differences, these works all define a pLTS made of configurations, i.e. pairs of quantum values and syntactic processes, and they require bisimilar systems to exhibit the same probabilistic behaviour and observable quantum values. Many of the existing works have to tweak the natural definition of probabilistic bisimilarity in an *ad hoc* manner, in order to capture the peculiar observable properties of quantum values. We instead introduce purely quantum LTSs, and we manipulate quantum values only through effects, which represent their observable probabilistic behaviour. Moreover, in the previous proposals, verifying the equivalence of two processes requires instantiating them with each possible quantum input, impeding algorithmic verification. Using effects, we describe the "symbolic" semantics of protocols, abstracting away from the input.

Most similar to our work is [11], which introduces superoperator-valued quantum distributions, analogous to the ones in [17, 32, 27]. This allows modelling the more expressive non-destructive measurements and quantum communication, but their bisimilarity does not respect the observational properties prescribed by quantum theory [23, 7, 13]. For the operational semantics of their language, they employ configurations of superoperators and processes (as in our Heisenberg semantics), and they build a superoperator-weighted LTS. The bisimilarity that they propose is equivalent to the one in [10], and requires bisimilar configurations with the same weights, leading to a form of AM-bisimilarity finer than of our LS-bisimilarity. For example, it discriminates the following precesses (in mQPA syntax).

▶ **Example 39.** Let $P = \tau.([|0\rangle\langle 0|]R, [|1\rangle\langle 1|]R')$ and $Q = \tau.([|+\rangle\langle +|]R, [|-\rangle\langle -|]R')$ with R and R' two deadlock processes that maintain the ownership of the measured qubit (recall that [11] considers non-destructive measurements), thus making it unobservable. In other words, P and Q perform some local measurement on their qubit, without leaking any classical information to an external observer. Nonetheless, P and Q are not bisimilar for the symbolic/open bisimilarity of [11, 10], as can be seen studying the ground behaviour of $\langle \Phi^+, P\rangle$ and $\langle \Phi^+, Q\rangle$. These processes are bisimilar in our proposal, as well as in other recent works [23, 9, 7].

The bisimilarity of [10] has been relaxed in [13, 9] to match the prescriptions of quantum theory, but no symbolic version of this coarser bisimilarity has been proposed.

6 Conclusions and future works

We proposed effect labelled transition systems (eLTSs), a new operational model that generalizes the probabilistic ones and is suitable for modeling quantum concurrent systems. We investigated bisimilarity, adapting two equivalent definitions of probabilistic bisimilarity to the quantum case, namely Aczel-Mendler and Larsen-Skou bisimilarity. Despite coinciding for classical systems, they disagree on quantum processes, and only the latter is guaranteed to be an equivalence relation. Then, we proved the adequacy of the Larsen-Skou bisimilarity, showing it correct and complete with respect to the observable probabilistic behaviour prescribed by quantum theory.

This model allows for a purely quantum-based semantics of quantum protocols, with the advantage of providing an algorithmically verifiable equivalence over processes. Indeed, eLTSs can be easily defined in a coalgebraic fashion, allowing e.g. to resort to the general algorithm for partition refinement of [22] for proving Larsen-Skou bisimilarity.

We assessed our approach in a process calculus with minimal features, like destructive measurements, unitaries, synchronization and non-determinism. In the standard probabilistic approach to quantum process calculi [24, 7, 8, 10, 9, 6], processes must be compared with respect to every possible input quantum state, thus considering a continuously infinite set of cases. We instead equipped our calculus with a stateless eLTS semantics, and proved that it is consistent with the natural stateful semantics: two processes are bisimilar in the eLTS if they are indistinguishable on every input quantum state.

As a future work, we plan to investigate quantum extensions of Hennessy-Milner logic for characterizing Larsen-Skou bisimilarity. Moreover, we aim to enrich our process calculus with quantum value passing, and to study its stateless semantics using superoperator-weighted models, like the one of [11].

References

1 Samson Abramsky, Rui Soares Barbosa, Nadish de Silva, and Octavio Zapata. The quantum monad on relational structures. In Kim G. Larsen, Hans L. Bodlaender, and Jean-François Raskin, editors, *MFCS 2017*, volume 83 of *LIPIcs*, pages 35:1–35:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPICS.MFCS.2017.35.

2 Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. doi:10.1016/j.tcs.2014.05.025.

3 Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993. doi:10.1103/PhysRevLett.70.1895.

4 Filippo Bonchi, Alexandra Silva, and Ana Sokolova. The power of convex algebras. In Roland Meyer, Uwe Nestmann, and Marc Herbstritt, editors, *CONCUR 2017*, volume 85 of *LIPIcs*, pages 23:1–23:18. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPICS.CONCUR.2017.23.

5 Marcello Caleffi, Angela Sara Cacciapuoti, and Giuseppe Bianchi. Quantum internet: from communication to distributed computing! In Jón Atli Benediktsson and Falko Dressler, editors, *NANOCOM 2018*, pages 3:1–3:4. ACM, 2018. doi:10.1145/3233188.3233224.

6 Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. Quantum bisimilarity via barbs and contexts: Curbing the power of non-deterministic observers (extended version). *CoRR*, abs/2311.06116, 2023. doi:10.48550/arXiv.2311.06116.

7 Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. Quantum bisimilarity via barbs and contexts: Curbing the power of non-deterministic observers. *Proceedings of the ACM on Programming Languages*, 8(POPL):43:1269–43:1297, 2024. doi:10.1145/3632885.

8 Timothy A. S. Davidson. *Formal Verification Techniques Using Quantum Process Calculus*. PhD thesis, University of Warwick, 2012.

9 Yuxin Deng. Bisimulations for probabilistic and quantum processes. In Sven Schewe and Lijun Zhang, editors, *CONCUR 2018*, volume 118 of *LIPIcs*, pages 2:1–2:14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPIcs.CONCUR.2018.2.

10 Yuxin Deng and Yuan Feng. Open bisimulation for quantum processes. In Jos C. M. Baeten, Thomas Ball, and Frank S. de Boer, editors, *TCS 2012*, volume 7604 of *LNCS*, pages 119–133. Springer, 2012. doi:10.1007/978-3-642-33475-7_9.

11 Yuan Feng, Yuxin Deng, and Mingsheng Ying. Symbolic bisimulation for quantum processes. *ACM Transactions on Computational Logic*, 15(2):14:1–14:32, 2014. doi:10.1145/2579818.

12 Yuan Feng, Runyao Duan, and Mingsheng Ying. Bisimulation for quantum processes. *ACM Transactions on Programming Languages and Systems*, 34(4):17:1–17:43, 2012. doi:10.1145/2400676.2400680.

13 Yuan Feng and Mingsheng Ying. Toward automatic verification of quantum cryptographic protocols. In Luca Aceto and David de Frutos-Escrig, editors, *CONCUR 2015*, volume 42 of *LIPIcs*, pages 441–455. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2015. doi:10.4230/LIPIcs.CONCUR.2015.441.

14 Fei Gao, SuJuan Qin, Wei Huang, and QiaoYan Wen. Quantum private query: A new kind of practical quantum cryptographic protocol. *Science China Physics, Mechanics & Astronomy*, 62(7):70301, 2019. doi:10.1007/s11433-018-9324-6.

15 Simon J. Gay and Rajagopal Nagarajan. Communicating quantum processes. In Jens Palsberg and Martín Abadi, editors, *POPL 2005*, pages 145–157. ACM, 2005. doi:10.1145/1040305.1040318.

16 Stanley Gudder. Quantum Markov chains. *Journal of Mathematical Physics*, 49(7):072105, 2008. doi:10.1063/1.2953952.

17 Ichiro Hasuo and Naohiko Hoshino. Semantics of higher-order quantum computation via geometry of interaction. In *LICS 2011*, pages 237–246. IEEE Computer Society, 2011. doi:10.1109/LICS.2011.26.

18 Teiko Heinosaari and Mário Ziman. *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement*. Cambridge University Press, 2011.

19 Matthew Hennessy. Exploring probabilistic bisimulations, part I. *Formal Aspects of Computing*, 24(4-6):749–768, 2012. doi:10.1007/s00165-012-0242-7.

20 Matthew Hennessy and Huimin Lin. Symbolic bisimulations. *Theoretical Computer Science*, 138(2):353–389, 1995. doi:10.1016/0304-3975(94)00172-F.

21 Bart Jacobs. Probabilities, distribution monads, and convex categories. *Theoretical Computer Science*, 412(28):3323–3336, June 2011. doi:10.1016/j.tcs.2011.04.005.

22 Jules Jacobs and Thorsten Wißmann. Fast coalgebraic bisimilarity minimization. *Proceedings of the ACM on Programming Languages*, 7(POPL):52:1514–52:1541, 2023. doi:10.1145/3571245.

23 Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano, and Hideki Sakurada. Application of a process calculus to security proofs of quantum protocols. In Hamid R. Arabnia, George A. Gravvanis, and Ashu M. G. Solo, editors, *FCS 2012*, pages 141–147. CSREA Press, 2012.

24 Marie Lalire. Relations among quantum processes: Bisimilarity and congruence. *Mathematical Structures in Computer Science*, 16(3):407–428, 2006. doi:10.1017/S096012950600524X.

25 Marie Lalire and Philippe Jorrand. A process algebraic approach to concurrent and distributed quantum computation: Operational semantics. *CoRR*, quant-ph/0407005, 2004. `arXiv:quant-ph/0407005`.

26 Kim G. Larsen and Arne Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, 1991. `doi:10.1016/0890-5401(91)90030-6`.

27 Ai Liu and Meng Sun. A coalgebraic semantics framework for quantum systems. In Yamine Aït Ameur and Shengchao Qin, editors, *ICFEM 2019*, volume 11852 of *LNCS*, pages 387–402. Springer, 2019. `doi:10.1007/978-3-030-32409-4_24`.

28 Gui-lu Long, Fu-guo Deng, Chuan Wang, Xi-Han Li, Kai Wen, and Wan-Ying Wang. Quantum secure direct communication and deterministic secure quantum communication. *Frontiers of Physics in China*, 2(3):251–272, 2007. `doi:10.1007/s11467-007-0050-3`.

29 Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406, 2001. `doi:10.1145/382780.382781`.

30 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

31 Ali Ibnun Nurhadi and Nana Rachmana Syambas. Quantum key distribution (QKD) protocols: A survey. In *ICWT 2018*, pages 1–5. IEEE, 2018. `doi:10.1109/ICWT.2018.8527822`.

32 Hiroshi Ogawa. Coalgebraic approach to equivalences of quantum systems. Master's thesis, University of Tokyo, 2014.

33 Sam Staton. Relating coalgebraic notions of bisimulation. *Logical Methods in Computer Science*, 7(1), 2011. `doi:10.2168/LMCS-7(1:13)2011`.

34 Yong Wang. Probabilistic process algebra to unifying quantum and classical computing in closed systems. *International Journal of Theoretical Physics*, 58(10):3436–3509, 2019. `doi:10.1007/s10773-019-04216-2`.

35 Peiying Zhang, Ning Chen, Shigen Shen, Shui Yu, Sheng Wu, and Neeraj Kumar. Future quantum communications and networking: A review and vision. *IEEE Wireless Communications*, 31(1):141–148, 2024. `doi:10.1109/MWC.012.2200295`.

A Proofs of Section 3

▶ **Proposition 40.** *Let E_1 and E_2 be two effects. If $E_1 + E_2 = |\psi\rangle\langle\psi|$ then $E_i = p_i\,|\psi\rangle\langle\psi|$ for some p_i, $i = 1, 2$. If $E_1 \,{}_p\!\oplus\, E_2 = |\psi\rangle\langle\psi|$ then $E_i = |\psi\rangle\langle\psi|$ for $i = 1, 2$.*

▶ **Theorem 4.** *Effect distributions correspond to all and only the parameterized sub-probability distributions that are convex and have an "overall" finite support.*

$$\mathcal{Q}_Q \cong \left\{ \mathfrak{D}{\downarrow_\_} \in (\mathcal{D}X)^{DM_Q} \;\middle|\; \mathfrak{D}{\downarrow_{\rho \,{}_p\!\oplus\, \sigma}} = (\mathfrak{D}{\downarrow_\rho}) \,{}_p\!\oplus\, (\mathfrak{D}{\downarrow_\sigma}) \text{ and } \bigcup_{\rho \in DM_Q} \mathrm{supp}(\mathfrak{D}{\downarrow_\rho}) \text{ is finite} \right\}$$

Proof. Let d be the dimension of $\mathcal{H}_Q$. Recall that $(Ef_d, 0_d, +)$ is a Partial Commutative Monoid (PCM) [21]. Each PCM has a partial order, defined as $a \preceq b$ if and only if $\exists c. a + c = b$. In the case of Ef_d, $\preceq$ is the Löwner order $\sqsubseteq$. We employ a known result in quantum theory [18]: Ef_d is isomorphic to $\mathbf{Conv}(DM_d, [0, 1])$. Moreover, $\mathbf{Conv}(DM_d, [0, 1])$ forms a PCM, where the monoid identity is $\lambda\rho.0$ and the summation of functions is defined pointwise. Since the isomorphism between Ef_d and $\mathbf{Conv}(DM_d, [0, 1])$ is a PCM isomorphism, it follows that

$$\mathcal{Q}_d \cong \left\{ \mathfrak{D} : X \to DM_d \to [0, 1] \;\middle|\; \begin{array}{l} \forall x\ \mathfrak{D}(x) \text{ is convex, } \mathrm{supp}(\mathfrak{D}) \text{ is finite} \\ \sum_{x \in \mathrm{supp}(\mathfrak{D})} \mathfrak{D}(x) \preceq \lambda\rho.1 \end{array} \right\}$$

where $\mathrm{supp}(\mathfrak{D})$ is defined as $\{x \in X \mid \mathfrak{D}(x) \neq \lambda\rho.0\}$ and $\preceq$ is the pointwise ordering between functions. The theorem follows by proving that the set above is isomorphic to

$$\left\{ \mathfrak{D}{\downarrow_{\_}} : DM_d \to X \to [0,1] \;\middle|\; \begin{array}{l} \mathfrak{D}{\downarrow_{\_}} \text{ is convex, } \bigcup_\rho \mathrm{supp}(\mathfrak{D}{\downarrow_\rho}) \text{ is finite} \\ \forall \rho \sum_{x \in \mathrm{supp}(\mathfrak{D}{\downarrow_\rho})} \mathfrak{D}{\downarrow_\rho}(x) \leq 1 \end{array} \right\}$$

To prove this isomorphism, we provide an invertible function $f(\mathfrak{D}) = \lambda\rho.\lambda x.\mathfrak{D}(x)(\rho)$ that preserves and reflects the three properties we are interested in. For convexity, we have that

$$\begin{aligned} \forall x\ \mathfrak{D}(x) \text{ is convex} &\Leftrightarrow \forall x\ \mathfrak{D}(x)(\rho\ {}_p\!\oplus \sigma) = (\mathfrak{D}(x)(\rho))\ {}_p\!\oplus (\mathfrak{D}(x)(\sigma)) \\ &\Leftrightarrow \forall x\ f(\mathfrak{D})(\rho\ {}_p\!\oplus \sigma)(x) = (f(\mathfrak{D})(\rho)(x))\ {}_p\!\oplus (f(\mathfrak{D})(\sigma)(x)) \\ &\Leftrightarrow f(\mathfrak{D})(\rho\ {}_p\!\oplus \sigma) = f(\mathfrak{D})(\rho)\ {}_p\!\oplus f(\mathfrak{D})(\sigma) \Leftrightarrow f(\mathfrak{D}) \text{ is convex} \end{aligned}$$

For the finite support, we have that

$$\begin{aligned} \mathrm{supp}(\mathfrak{D}) &= \{x \in X \mid \mathfrak{D}(x) \neq \lambda\rho.0\} = \{x \in X \mid \exists \rho.\mathfrak{D}(x)(\rho) \neq 0\} \\ &= \bigcup\nolimits_\rho \{x \in X \mid \mathfrak{D}(x)(\rho) \neq 0\} = \bigcup\nolimits_\rho \mathrm{supp}(f(\mathfrak{D})) \end{aligned}$$

For the sum over the support, we have that

$$\begin{aligned} \sum_{x \in \mathrm{supp}(\mathfrak{D})} \mathfrak{D}(x) \preceq \lambda\rho.1 \;&\Leftrightarrow \forall \rho. \sum_{x \in \mathrm{supp}(\mathfrak{D})} \mathfrak{D}(x)(\rho) \leq 1 \Leftrightarrow \forall \rho. \sum_{\substack{x \in \mathrm{supp}(\mathfrak{D}) \\ \mathfrak{D}(x)(\rho) \neq 0}} \mathfrak{D}(x)(\rho) \leq 1 \\ &\Leftrightarrow \forall \rho. \sum_{\mathrm{supp}(f(\mathfrak{D})\rho)} \mathfrak{D}(x)(\rho) \leq 1 \Leftrightarrow \forall \rho. \sum_{\mathrm{supp}(f(\mathfrak{D})\rho)} f(\mathfrak{D})(\rho)(x) \leq 1 \end{aligned}$$

◀

▶ **Lemma 41.** *Let $\{s_\alpha, s_\beta, s_\gamma, s_\delta\} \subseteq X$, and let $\mathfrak{D} \in \mathcal{Q}_Q X$ be defined as $\mathfrak{D} = \{s_\alpha \rhd |\Phi^+\rangle\langle\Phi^+|, s_\beta \rhd |\Phi^-\rangle\langle\Phi^-|, s_\gamma \rhd |\Psi^+\rangle\langle\Psi^+|, s_\delta \rhd |\Psi^-\rangle\langle\Psi^-|\}$, where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. There is no $\mathfrak{T} \in \mathcal{Q}_Q^{\boxplus} X$ and subsets $X_\alpha, X_\beta, X_\gamma, X_\delta$ of X such that $\sum_{x \in X_y} \mathfrak{T}(x) = \mathfrak{D}(s_y)$ for $y \in \{\alpha, \beta, \gamma, \delta\}$.*

Proof. We proceed by induction on the number of application of $\boxplus$. No point distribution can verify this, hence the base case is trivial. Assume $\mathfrak{T}_1$ and $\mathfrak{T}_2$ can be defined by using $\boxplus$ n times starting from point distributions, and let $\mathfrak{T} = \mathfrak{T}_1\ {}_E\!\boxplus \mathfrak{T}_2$. We proceed by cases on the dimension d of the Hilbert space of the effect E. If $d = 1$, then $E = p$ for some p and

$$\sum_{x \in X_y} p \cdot \mathfrak{T}_1(x) + (1-p) \cdot \mathfrak{T}_2(x) = p \cdot \sum_{x \in X_y} \mathfrak{T}_1(x) + (1-p) \cdot \sum_{x \in X_y} \mathfrak{T}_2(x) = \mathfrak{D}(s_y).$$

If p is 0 or 1, then $\mathfrak{T} = \mathfrak{T}_1$ or $\mathfrak{T}_2$, and the result directly follows from induction hypothesis. Otherwise, since $\mathfrak{D}(s_y)$ is of the form $|\psi\rangle\langle\psi|$ for each y, by Proposition 40 both $\sum_{x \in X_y} \mathfrak{T}_1(x)$ and $\sum_{x \in X_y} \mathfrak{T}_2(x)$ are equal to $\mathfrak{D}(s_y)$.

Consider now the case $d = 2$, then $\mathfrak{T}_1$, $\mathfrak{T}_2$ must be of dimension 2, and it must be that

$$\sum_{x \in X_\alpha} E \boxtimes \mathfrak{T}_1(x) + (\mathbb{I} - E) \boxtimes \mathfrak{T}_2(x) = E \boxtimes \sum_{x \in X_y} \mathfrak{T}_1(x) + (\mathbb{I} - E) \boxtimes \sum_{x \in X_y} \mathfrak{T}_2(x) = \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|.$$

By Proposition 40, $E \boxtimes \sum_{x \in X_y} \mathfrak{T}_1(x)$ must be equal to $p \cdot |\Phi^+\rangle\langle\Phi^+|$ for some p. But then, $\frac{1}{p} E \boxtimes \sum_{x \in X_y} \mathfrak{T}_1(x) = |\Phi^+\rangle\langle\Phi^+|$ contradicting the inseparability of $|\Phi^+\rangle\langle\Phi^+|$.

The dimension d cannot be 3 since $\mathfrak{D}$ is of dimension 4.

If $d = 4$, then $\mathfrak{T}_1$ and $\mathfrak{T}_2$ can only be of dimension 1, and the effects in $\mathfrak{D}$ must be all expressible as pE or $p(\mathbb{I} - E)$ for some probability p, but this is not the case.

Finally, note that d cannot be greater than 4, because $\mathcal{H}_Q$ is of dimension 4. ◀

▶ **Theorem 11.** *If $|X| \geq 4$ and $|Q| \geq 2$, with $|\cdot|$ the cardinality, then $\mathcal{Q}_Q^{\boxplus} X \neq \mathcal{Q}_Q X$.*

Proof. For $|Q| = 2$, i.e. $\mathcal{H}_Q$ of dimension 4, it is sufficient to note that this equivalence would contradict Lemma 41. This trivially generalizes to higher dimensional Hilbert spaces. ◀

▶ **Lemma 13.** *For all $\mathcal{R}$, $\mathfrak{D}\,\widehat{\mathcal{R}}_Q\,\mathfrak{T}$ iff there exist a set of indices I and a set of effects $\{E_i \in Ef_Q\}_{i\in I}$ such that $\mathfrak{D} = \{x_i \rhd E_i\}_{i\in I}$, $\mathfrak{T} = \{y_i \rhd E_i\}_{i\in I}$, and $x_i\,\mathcal{R}\,y_i$ for any $i \in I$.*

Proof. ($\Leftarrow$) Suppose there is a finite index set I such that (1) $\mathfrak{D} = \{s_i \rhd E_i\}_{i\in I}$, (2) $\mathfrak{T} = \{t_i \rhd E_i\}_{i\in I}$ and (3) $s_i\,\mathcal{R}\,t_i$ for each $i \in I$. By (3) and by definition, it follows that $\overline{s}_i\ \widehat{\mathcal{R}_\emptyset}\ \overline{t}_i$ for each $i \in I$. Then, by Definition 12, $\mathfrak{D} = (\sum_{i\in I} E_i \boxtimes \overline{s_i})\widehat{\mathcal{R}}_Q(\sum_{i\in I} E_i \boxtimes \overline{t_i}) = \mathfrak{T}$.

($\Rightarrow$) By induction on the rules for $\widehat{\mathcal{R}}_Q$. For the first rule, assume $s\ \mathcal{R}\ t$ and $\overline{s}\ \widehat{\mathcal{R}}_\emptyset\ \overline{t}$, then $\overline{s} = \{s \rhd 1\}$ and $\overline{t} = \{t \rhd 1\}$. For the second rule, assume $\mathfrak{D}_i\ \widehat{\mathcal{R}}_Q\ \mathfrak{T}_i$. Then by induction hypothesis, for any $i \in I$, it holds that $\mathfrak{D}_i = \{s_{i,j} \rhd E_{i,j}\}_{j\in i_i}$ and $\mathfrak{T}_i = \{t_{i,j} \rhd E_{i,j}\}_{j\in i_i}$, with $s_{i,j}\ \mathcal{R}\ t_{i,j}$. Hence it is true that $\sum_{i\in I} E_i \boxtimes \mathfrak{D}_i = \{s_{i,j} \rhd E_i \boxtimes E_{i,j}\}_{i\in I, j\in i_i}$ and $\sum_{i\in I} E_i \boxtimes \mathfrak{T}_i = \{t_{i,j} \rhd E_i \boxtimes E_{i,j}\}_{i\in I, j\in i_i}$, thus the result follows by definition. ◀

▶ **Theorem 19.** *For any eLTS over Ef_Q with states S, $\sim_{am} \subseteq \sim_{ls}$. Moreover, $\sim_{am} = \sim_{ls}$ if $Q = \emptyset$, and $\sim_{am} \subsetneq \sim_{ls}$ if Q is of dimension at least 2 and S of cardinality at least 4.*

Proof. For $\subseteq$ it is sufficient to show that $\mathfrak{D}\,\widehat{\mathcal{R}}\,\mathfrak{T}$ requires $\mathfrak{D}$ and $\mathfrak{T}$ to assign the same effect to each class in $S/_{\mathcal{R}}$, by Lemma 13. The equality $\sim_{am} = \sim_{ls}$ in eLTSs of dimension one is a classical for pLTSs [19]. Then it suffices to consider Example 18. ◀

▶ **Theorem 23.** *For any $s, t \in S$, $s \sim_{ls} t$ if and only if $s \sim_{lpp} t$.*

Proof. It is easy to show that $\sim_{ls}$ is a lpp-bisimulation and that $\sim_{lpp}$ is a ls-bisimulation. For the first direction, take $s \sim_{ls} t$ and suppose that $s \xrightarrow{\mu} \mathfrak{D}$, then there exists $t \xrightarrow{\mu} \mathfrak{T}$ such that $\forall C \in S/_{\sim_{ls}}\ \mathfrak{D}(C) = \mathfrak{T}(C)$, where $\mathfrak{D}(C) = \sum_{x\in C} \mathfrak{D}(x)$, and similarly for $\mathfrak{T}$. In other words, we know that $\mathfrak{D}$ and $\mathfrak{T}$ are identical when considered as effect distributions on the set of equivalence classes. Thus, applying Theorem 4, we know that $\mathfrak{D}{\downarrow_\_} = \mathfrak{T}{\downarrow_\_}$, i.e. that for any ρ they give the same probability distribution on equivalence classes, as required by the definition of lpp-bisimulation.

The other direction is identical, employing the isomorphism of Theorem 4 ◀

▶ **Lemma 42.** *Given a set of effects $\mathbb{E}$ of a fixed dimension, there exists a state ρ such that $\forall i, j \in \mathbb{E}.\ tr(E_i\rho_{\mathbb{E}}) = tr(E_j\rho_{\mathbb{E}})$ iff $i = j$.*

Proof. Note that for any pair of distinct effects E_i, E_j there is a state $\rho_{i,j}$ such that $tr(E_i\rho_{i,j}) \neq tr(E_j\rho_{i,j})$. Let $p^k_{i,j} = tr(E_k\rho_{i,j})$. Note also that $\{p^k_{i,j}\}_{i,j,k}$ is in the algebraic closure of $\mathbb{Q} \cup T$ with T a finite set of transcendental numbers.

Let $q_{i,j}$ be transcendental numbers not in T such that for each i, j, $q_{i,j}$ is not in the algebraic closure of $\mathbb{Q} \cup T \cup \{q_{a,b} \mid a \neq i \text{ or } b \neq j\}$ (there are enough transcendental numbers, otherwise we could prove $\mathbb{R}$ to be denumerable). We let q' be defined as $(1 - \sum_{i,j} q_{i,j})$, and we use it to scale the $q_{i,j}$ to the weights of a full probability distribution, letting $x_{i,j} = q_{i,j}q'$.

We let $\rho_{\mathbb{E}} = \sum_{i,j} x_{i,j}\rho_{i,j}$ and prove by refutation that it distinguishes all the effects in $\mathbb{E}$. Assume that $tr(E_a\rho_{\mathbb{E}}) = tr(E_b\rho_{\mathbb{E}})$ for some indices $a \neq b$. We observe that for $k \in \{a, b\}$

$$tr(E_k\rho_{\mathbb{E}}) = \sum_{i,j} x_{i,j} tr(E_k\rho_{i,j}) = \sum_{i,j} x_{i,j} p^k_{i,j} = q' \sum_{i,j} q_{i,j} p^k_{i,j}.$$

Hence, we can rewrite our assumption as $\sum_{i,j} q_{i,j} p^a_{i,j} = \sum_{i,j} q_{i,j} p^b_{i,j}$. Note that for each pair of indices c and d we can rewrite the formula above as

$$q_{c,d}(p^a_{c,d} - p^b_{c,d}) = \sum_{i,j\neq c,d} q_{i,j} p^b_{i,j} - \sum_{i,j\neq c,d} q_{i,j} p^a_{i,j}$$

If for some c or d, $p^a_{c,d} - p^b_{c,d}$ is not zero, then we can divide both sides for $p^a_{c,d} - p^b_{c,d}$, proving that $q_{c,d}$ is indeed in the algebraic closure of $\mathbb{Q} \cup T \cup \{q_{e,f} \mid e \neq c \text{ or } f \neq d\}$. Since this would contradict our hypothesis, we must assume that $p^a_{c,d} - p^b_{c,d} = 0$ for any choice of c and d, but this is a contradiction with the definition of $p^k_{i,j}$, since $p^a_{a,b} \neq p^b_{a,b}$ by construction. ◀

▶ **Theorem 24.** *For any $s, t \in S$, $s \sim_{ls} t$ implies $s \simeq_{pbe} t$. Moreover, if S is finitely dimensional, then $s \simeq_{pbe} t$ implies $s \sim_{ls} t$.*

Proof. By Theorem 23, for proving $\sim_{ls} \subseteq \simeq_{pbe}$ it suffices to show that $\sim_{lpp} \subseteq \simeq_{pbe}$, which holds by definition.

For $\simeq_{pbe} \subseteq \sim_{ls}$, let n be the cardinality of S, and consider the set of effects that appears in the eLTS $\mathbb{E}^0 = \{E \mid \exists s, s' \in S, \mu \in Act. s \xrightarrow{\mu} \mathfrak{D} \text{ and } \mathfrak{D}(s') = E\}$. We let $\mathbb{E}$ be the set of the effects obtained by summing up to n effects in $\mathbb{E}^0$, i.e. effects that are possibly associated with some equivalence class. By Lemma 42, there is a quantum state $\rho_{\mathbb{E}}$ such that $\forall E_i, E_j \in \mathbb{E}. tr(E_i \rho_{\mathbb{E}}) = tr(E_j \rho_{\mathbb{E}})$ iff $E_i = E_j$. Note that $\simeq_{pbe} \subseteq \sim_{\rho_{\mathbb{E}}}$ by definition of $\simeq_{pbe}$. Note also that by proving $\sim_{\rho_{\mathbb{E}}} \subseteq \sim_{ls}$ we would get the thesis by transitivity.

We will prove that $\sim_{\rho_{\mathbb{E}}}$ is a LS-bisimulation. Assume $s \sim_{\rho_{\mathbb{E}}} t$, and that $s \xrightarrow{\mu} \mathfrak{D}$, then $t \xrightarrow{\mu} \mathfrak{T}$ with $\mathfrak{D}{\downarrow_{\rho_{\mathbb{E}}}} \widehat{\sim_{\rho_{\mathbb{E}}}}_1 \mathfrak{T}{\downarrow_{\rho_{\mathbb{E}}}}$. Note that, since LS and AM-bisimilarity coincides in the probabilistic case, the relation above implies that $\forall C \in S/_{\sim_{\rho_{\mathbb{E}}}}. \sum_{x \in C} \mathfrak{D}{\downarrow_{\rho_{\mathbb{E}}}}(x) = \sum_{x \in C} \mathfrak{T}{\downarrow_{\rho_{\mathbb{E}}}}(x)$.

We now have to prove that $\forall C \in S/_{\sim_{\rho_{\mathbb{E}}}}. \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x)$. Assume by refutation that there is a C such that the condition does not hold. Then it suffices to note that

$$\sum_{x \in C} \mathfrak{D}{\downarrow_{\rho_{\mathbb{E}}}}(x) = \sum_{x \in C} \mathrm{tr}(\mathfrak{D}(x)\rho_{\mathbb{E}}) = \mathrm{tr}\left(\left(\sum_{x \in C} \mathfrak{D}(x)\right)\rho_{\mathbb{E}}\right)$$
$$\sum_{x \in C} \mathfrak{T}{\downarrow_{\rho_{\mathbb{E}}}}(x) = \sum_{x \in C} \mathrm{tr}(\mathfrak{T}(x)\rho_{\mathbb{E}}) = \mathrm{tr}\left(\left(\sum_{x \in C} \mathfrak{T}(x)\right)\rho_{\mathbb{E}}\right)$$

Since $\sum_{x \in C} \mathfrak{D}(x)$ and $\sum_{x \in C} \mathfrak{T}(x)$ are both effects in $\mathbb{E}$, we have that $tr((\sum_{x \in C} \mathfrak{D}(x))\rho_{\mathbb{E}}) = tr((\sum_{x \in C} \mathfrak{T}(x))\rho_{\mathbb{E}})$ implies $\sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x)$ contradicting our assumption. ◀

In the following we write $\mathfrak{D}|_\rho$ for $\{s_i|_\rho \rhd \mathrm{tr}_{Q'}(E_i(\rho \boxtimes \mathbb{I}_{Q \setminus Q'}))\}_{i \in I}$ with $\mathfrak{D} = \{s_i \rhd E_i\}_{i \in I}$.

▶ **Theorem 28.** *If $s \sim_{ls} t$ then $s|_\rho \sim_{ls} t|_\rho$.*

Proof. We prove $\mathcal{R} = \{(s|_\rho, t|_\rho) \mid s \sim_{ls} t\}$ to be a ls-bisimulation. Take $(s|_\rho, t|_\rho) \in \mathcal{R}$, and assume $s|_\rho$ performs a reduction, then, by PEVAL it must be that $s \xrightarrow{\mu} \mathfrak{D}$. Since $s \sim_{ls} t$, there exists $\mathfrak{T}$ such that $t \xrightarrow{\mu} \mathfrak{T}$ and $\forall C \in S/_{\sim_{ls}} \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x)$. Moreover, $t|_\rho \xrightarrow{\mu} \mathfrak{T}|_\rho$ by PEVAL. We are left with proving that $\forall C \in S/_{\mathcal{R}} \sum_{x \in C} \mathfrak{D}(x)|_\rho = \sum_{x \in C} \mathfrak{T}(x)|_\rho$. Note that, by definition of $\mathcal{R}$ $C \in S/_{\sim_{ls}}$ if and only if $\{x|_\rho \mid x \in C\} \in S/_{\mathcal{R}}$. Therefore, we can rewrite our condition as $\forall C \in S/_{\sim_{ls}} \sum_{x \in C} \mathfrak{D}(x|_\rho)\big|_\rho = \sum_{x \in C} \mathfrak{T}(x|_\rho)\big|_\rho$, which clearly derives from $\forall C \in S/_{\sim_{ls}} \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x)$, by definition of $\mathfrak{D}|_\rho$. ◀

▶ **Lemma 43.** *For any eLTS $(S, Act, \to)$ over Ef_Q and state $\rho \in DM_Q$, given a relation $\mathcal{R} \subseteq S \times S$ we have that $\mathcal{R}$ is a ρ-bisimulation if and only if $\mathcal{R}|_\rho$ is a bisimulation, where $\mathcal{R}|_\rho$ is defined as $s|_\rho \mathcal{R}|_\rho t|_\rho$ if and only if $s \mathcal{R} t$.*

Proof. Note that for any two distribution $\mathfrak{D}, \mathfrak{T}$, it holds $\mathfrak{D}{\downarrow_\rho} \mathring{\mathcal{R}} \mathfrak{T}{\downarrow_\rho}$ iff $\mathfrak{D}|_\rho \mathring{\mathcal{R}}|_\rho \mathfrak{T}|_\rho$ since $\mathfrak{D}{\downarrow_\rho}$ and $\mathfrak{D}|_\rho$ assign the same probability to same elements, modulo the $|_\rho$ renaming.

We must now prove that $\mathcal{R}|_\rho$ is a bisimulation. Suppose $s|_\rho \mathcal{R}|_\rho t|_\rho$, then if $s|_\rho \xrightarrow{\mu} \mathfrak{D}|_\rho$ it must be $s \xrightarrow{\mu} \mathfrak{D}$. As t is ρ-bisimilar, we know that $t \xrightarrow{\mu} \mathfrak{T}$ and $\mathfrak{D}{\downarrow_\rho} \mathring{\mathcal{R}} \mathfrak{T}{\downarrow_\rho}$, because, since they are probability distributions, the equivalence class condition of ρ bisimilarity is equivalent to the relational lifting. Thus we get $\mathfrak{D}|_\rho \widehat{\mathcal{R}|_\rho} \mathfrak{T}|_\rho$, showing that $\mathcal{R}|_\rho$ is a bisimulation. ◀

▶ **Corollary 29.** *Given a finite eLTS $(S, Act, \to)$ over Ef_Q and $s, t \in S$, if for any $\rho \in DM_Q$ we have $s|_\rho \sim_{ls} t|_\rho$, then $s \sim_{ls} t$.*

Proof. Take $\mathcal{R} = \{(x, y) \mid x|_\rho \sim_{ls} y|_\rho\}$. The relation $\mathcal{R}|_\rho$ is a bisimulation since if $x|_\rho \xrightarrow{\mu} \mathfrak{D}|_\rho$ we have $y|_\rho \xrightarrow{\mu} \mathfrak{T}|_\rho$, and $\mathfrak{D}|_\rho, \mathfrak{T}|_\rho$ are not only in $\overset{\circ}{\sim}_{ls}$, but also in $\overset{\circ}{\mathcal{R}}|_\rho$. By Lemma 43 $\mathcal{R}$ is a ρ-bisimulation, and s, t are ρ-bisimilar for any ρ. Thus by Theorem 24 they are bisimilar. ◀

B Proofs of Section 4

Recall that we write $\sim$ for the LS-bisimilarity $\sim_{ls}$.

▶ **Lemma 44.** *Consider a Ef_Q eLTS and $\mathcal{E} : DM_Q \to DM_{Q'}$ with $Q' \subseteq Q$. For any s, if $\langle \mathcal{E}, s\rangle \xrightarrow{\mu} \mathfrak{D}$, then there are states s_i and superoperators $\mathcal{E}_i : DM_Q \to DM_{Q''}$ with $Q'' \subseteq Q'$ such that $\mathfrak{D} = \{\langle \mathcal{E}_i, s_i\rangle \rhd \mathcal{I}_i(\mathbb{I}_{Q''})\}$. Moreover, for all $\rho \in DM_Q$, $\langle \mathcal{E}(\rho), s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd tr(\mathcal{E}_i(\rho))\}$.*

Proof. By induction on the rules of the Heisenberg semantics.

(case HPre) Consider the transition $\langle \mathcal{E}, \mu.([E_i]s_i)_{i\in I}\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i} \circ \mathcal{E}, s_i\rangle \rhd \mathcal{I}(E_i \boxtimes \mathbb{I}_{Q\setminus Q'})\}_{i\in I}$. Let $\mathcal{E}_i = \mathcal{M}_{E_i} \circ \mathcal{E}$. The first point follows from duality, $\mathcal{E}_i$ is $\mathcal{I}_i(F) = \mathcal{I} \circ (E_i \boxtimes F)$. For the second point, take any ρ, and apply the SPre rule: $\langle \mathcal{E}(\rho), \mu.([E_i]s_i)_{i\in I}\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\mathcal{E}(\rho)), s_i\rangle \rhd \mathrm{tr}(\mathcal{M}_{E_i}(\mathcal{E}(\rho)))\}_{i\in I}$. The result holds by definition since $\mathcal{E}_i = \mathcal{M}_{E_i} \circ \mathcal{E}$.

(case HU) Consider the transition $\langle \mathcal{E}, U; s\rangle \xrightarrow{\mu} \mathfrak{D}$. By induction hypothesis, $\langle \mathcal{U} \circ \mathcal{E}, s\rangle \xrightarrow{\mu} \mathfrak{D}$ and $\mathfrak{D} = \{\langle \mathcal{E}_i, s_i\rangle \rhd \mathcal{I}_i(\mathbb{I}_{Q''})\}$, trivially proving the first point. By induction hypothesis, it also holds that for any ρ, $\langle (\mathcal{U} \circ \mathcal{E})(\rho), s\rangle \xrightarrow{\mu} \mathfrak{T} = \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd tr(\mathcal{E}_i(\rho))\}$. Then, the result holds by considering the rule SU: $\langle \mathcal{E}(\rho), U; s\rangle \xrightarrow{\mu} \mathfrak{T}$.

(case HSyncL) Consider the transition $\langle \mathcal{E}, r \parallel t\rangle \xrightarrow{\tau} \{\langle \mathcal{E}_j, r_k \parallel t_j\rangle \rhd E_j\}_{(k,j)\in K\times J_k}$. By induction hypothesis, we know that

$$\langle \mathcal{E}, r\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_k, r_k\rangle \rhd \mathcal{I}_k(\mathbb{I})\}_{k\in K} \Rightarrow \forall \rho.\langle \mathcal{E}(\rho), r\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_k(\rho), r_k\rangle \rhd p_k\}_{k\in K}$$
$$\langle \mathcal{E}_k, t\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_j, t_j\rangle \rhd \mathcal{I}_j(\mathbb{I})\}_{j\in J_k} \Rightarrow \forall \rho.\langle \mathcal{E}_k(\rho), t\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_j(\rho), t_j\rangle \rhd tr(\mathcal{E}_j(\rho))\}_{j\in J_k}$$

since $E_j = \mathcal{I}_j(\mathbb{I})$, $I = K \times J_k$, $s_i = r_k \parallel t_j$, $\mathcal{E}_i = \mathcal{E}_j$, the first point holds by definition. Take any ρ, and apply SSyncL. Then $\langle \mathcal{E}(\rho), r \parallel t\rangle \xrightarrow{\tau} \{\langle \mathcal{E}_j(\rho), r_k \parallel t_j\rangle \rhd tr(\mathcal{E}_j(\rho))\}_{(k,j)\in K\times J_k}$, thus proving the second point. All the other cases follow by induction. ◀

▶ **Lemma 45.** *Let $\mathcal{E} : DM_Q \to DM_{Q'}$ with $Q' \subseteq Q$. For any s and any $\rho \in DM_Q$, if $\langle \mathcal{E}(\rho), s\rangle \xrightarrow{\mu} \mathfrak{D}$, then there exists states s_i and superoperators $\mathcal{E}_i : DM_Q \to DM_{Q''}$ with $Q'' \subseteq Q'$ such that $\mathfrak{D} = \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd tr(\mathcal{E}_i(\rho))\}$. Moreover, there exists a transition $\langle \mathcal{E}, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle \rhd \mathcal{I}_i(\mathbb{I}_{Q''})\}$.*

Proof. We proceed by induction on the rules of the Schrödinger semantics.

(case SPre) Consider $\langle \mathcal{E}(\rho), \mu.([E_i]s_i)_{i\in I}\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\mathcal{E}(\rho)), s_i\rangle \rhd \mathrm{tr}(\mathcal{M}_{E_i}(\mathcal{E}(\rho)))\}_{i\in I}$. Then $\mathcal{E}_i = \mathcal{M}_{E_i} \circ \mathcal{E}$. Furthermore, by rule HPre $\langle \mathcal{E}, \mu.([E_i]s_i)_{i\in I}\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i} \circ \mathcal{E}, s_i\rangle \rhd \mathcal{I}(E_i \boxtimes \mathbb{I}_{Q\setminus Q'})\}_{i\in I}$, with $\mathcal{I}_i(F) = \mathcal{I} \circ (E_i \boxtimes F)$ being the dual of $\mathcal{E}_i$.

(case SU) Consider the transition $\langle \mathcal{E}(\rho), U; s\rangle \xrightarrow{\mu} \mathfrak{T}$. Then, by induction hypothesis, $\langle \mathcal{U}(\mathcal{E}(\rho)), s\rangle \xrightarrow{\mu} \mathfrak{T} = \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd tr(\mathcal{E}_i(\rho))\}$, and $\langle \mathcal{U} \circ \mathcal{E}, s\rangle \xrightarrow{\mu} \mathfrak{D} = \{\langle \mathcal{E}_i, s_i\rangle \rhd \mathcal{I}_i(\mathbb{I}_{Q''})\}$. Then, the result holds by considering the rule HU, granting that $\langle \mathcal{E}, U; s\rangle \xrightarrow{\mu} \mathfrak{D}$.

(case SSyncL) Consider the transition $\langle \mathcal{E}(\rho), r \parallel t\rangle \xrightarrow{\tau} \{\langle \rho_j, r_k \parallel t_j\rangle \rhd p_j\}_{(k,j)\in K\times J_k}$. By induction hypothesis, the required premises hold, and they have the following form and that

$$\langle \mathcal{E}(\rho), r\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_k(\rho), r_k\rangle \rhd p_k\}_{k\in K} \Rightarrow \langle \mathcal{E}, r\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_k, r_k\rangle \rhd \mathcal{Z}_k(\mathbb{I})\}_{k\in K}$$
$$\langle \mathcal{E}_k(\rho), t\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_j(\rho), t_j\rangle \rhd tr(\mathcal{E}_j(\rho))\}_{j\in J_k} \Rightarrow \langle \mathcal{E}_k, t\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_j, t_j\rangle \rhd \mathcal{Z}_j(\mathbb{I})\}_{j\in J_k}$$

where $\rho_j = \mathcal{E}_j(\rho)$ and $p_j = tr(\mathcal{E}_j(\rho))$. The first point holds by definition. Take HSyncL. Then $\langle \mathcal{E}, r \parallel t\rangle \xrightarrow{\tau} \{\langle \mathcal{E}_j, r_k \parallel t_j\rangle \rhd \mathcal{Z}_j(\mathbb{I})\}_{(k,j)\in K\times J_k}$, thus proving the second point. All the other cases follows by induction. ◀

▶ **Theorem 36.** *For any process P and $\rho \in DM_{Q_P}$, $\langle \mathcal{I}, P\rangle|_\rho \sim \langle \rho, P\rangle$.*

Proof. Take $\mathcal{R} = \{(\langle \mathcal{E}, R\rangle|_\rho, \langle \mathcal{E}(\rho), R\rangle) \mid Q \text{ is a process, and } \mathcal{E} : Ef_{Q_P} \to Ef_Q, Q \supseteq Q_R\}$ Take a pair $(\langle \mathcal{E}, R\rangle|_\rho, \langle \mathcal{E}(\rho), R\rangle)$ and assume that $\langle \mathcal{E}, R\rangle|_\rho \xrightarrow{\mu} \mathfrak{D}$. Then, by definition of $\cdot|_\rho$ and Lemma 44, we have $\langle \mathcal{E}, R\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle \rhd \mathcal{Z}_i(\mathbb{I})\}_{i\in I}$ and $\mathfrak{D} = \{\langle \mathcal{E}_i, s_i\rangle|_\rho \rhd tr((\mathcal{Z}_i(\mathbb{I}))\rho)\}_{i\in I}$. Moreover, by Lemma 44, $\langle \mathcal{E}(\rho), R\rangle \xrightarrow{\mu} \mathfrak{T} = \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd tr(\mathcal{E}_i(\rho))\}_{i\in I}$. Note that $\mathfrak{D} \mathrel{\mathring{\mathcal{R}}} \mathfrak{T}$ since $\langle \mathcal{E}_i, s_i\rangle|_\rho \mathcal{R} \langle \mathcal{E}_i(\rho), s_i\rangle$ and $tr((\mathcal{Z}_i(\mathbb{I}))\rho) = tr(\mathbb{I}(\mathcal{E}_i(\rho))) = tr(\mathcal{E}_i(\rho))$. The other direction is symmetric thanks to Lemma 45. ◀

▶ **Corollary 37.** *Given two processes P and R, $\langle \mathcal{I}, P\rangle \sim \langle \mathcal{I}, R\rangle$ if and only if $\langle \rho, P\rangle \sim \langle \rho, R\rangle$ for any $\rho \in DM_{Q_P}$.*

Proof. By Corollary 29 and Theorem 36. ◀