Effect Semantics for Quantum Process Calculi

Lorenzo Ceragioli
IMT School for Advanced Studies Lucca
Lucca, Italy
lorenzo.ceragioli@imtlucca.it

Fabio Gadducci
University of Pisa
Department of Computer Science
Pisa, Italy
fabio.gadducci@unipi.it

Giuseppe Lomurno
University of Pisa
Department of Computer Science
Pisa, Italy
giuseppe.lomurno@phd.unipi.it

Gabriele Tedeschi
University of Pisa
Department of Computer Science
Pisa, Italy
gabriele.tedeschi@phd.unipi.it

ABSTRACT

Along with the development of quantum communication protocols, quantum extensions of process calculi have been explored together with different notions of behavioural equivalence. Recent works have shown that defining a bisimilarity that matches the observational properties of a quantum-capable system is a surprisingly difficult task. Moreover, the two proposals explicitly addressing this issue, namely qCCS and lqCCS, do not define an algorithmic verification scheme: in order to prove the bisimilarity of two processes, one has to compare their behaviour under any possible input state. 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 (eLTS), generalizing probability distributions and probabilistic labelled transition systems (pLTS), respectively. We give an eLTS-based semantics for a minimal quantum process algebra, featuring concurrent and non-deterministic behaviour, quantum measurements and unitaries, and we prove that this semantics is 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.

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 [30], cryptographic coin tossing [2], direct communication [27], and private information retrieval [13]. Protocols like BB84 QKD [2] are *unconditionally secure* [28], meaning that they are protected against all physically possible attackers. Quantum communication also promises to allow linking multiple computers via the *Quantum Internet* [4, 34], therefore providing quantum algorithms with large enough memories for practical applications.

Conference'17, July 2017, Washington, DC, USA
2024. ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Despite the rich theory and the potential applications, there is no accepted standard to model and verify quantum concurrent systems and protocols. Numerous works [6, 11, 14, 24, 33] rely on *quantum process calculi*, an algebraic formalism that has been successfully applied to classical protocols and concurrent systems. Their semantics is given by means of a *labeled transition system* (LTS) $(S, Act, \rightarrow)$: the relation $\rightarrow \subseteq S \times Act \times S$ specifies how a state $s \in S$ may evolve performing an action $\alpha \in Act$. The standard equivalence for such LTSs is *bisimilarity*, the largest relation on states that is "stable" for $\rightarrow$, meaning that bisimilar states evolve in bisimilar states.

There have been several attempts [6–9, 23] to adapt existing techniques to the quantum setting, mainly in terms of *probabilistic* LTSs (pLTs) $(Conf, Act, \rightarrow)$, where $Conf = \mathcal{H} \times S$ is a set of *configurations* composed by a quantum state (an element of a Hilbert space $\mathcal{H}$) and a process, and $\rightarrow \subseteq Conf \times Act \times \mathcal{D}(Conf)$ with $\mathcal{D}(Conf)$ probability distributions of configurations. This approach led to a plethora of different bisimilarities, yet most of them unsatisfactory since they spuriously distinguish processes that are deemed indistinguishable by the prescriptions of quantum theory [7, 12, 22]. Moreover, assessing bisimilarity of processes requires comparing infinitely many LTSs (one for each possible quantum state). Indeed, algorithmic verification is still missing. In [6], 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 novel semantic model for non-deterministic and concurrent quantum systems, generalizing pLTSs. In physics, *effects* represent the observable behaviour of quantum states, thus building on them allows us to express the correct observable properties of more complex structures, like *effect distributions* and eLTSs. At the same time, effects encode probabilistic properties that are *parametric* with respect to quantum states. We study effect distributions and eLTSs, either generalising the known results on probabilistic systems when possible, or proving they do not hold otherwise. We explore several notions of bisimilarity and investigate their relation with the prescriptions of quantum theory. We show that a Larsen-Skou-style bisimilarity is indeed adequate for comparing quantum systems.

To assess our proposal, we define a *minimal quantum process algebra* (mQPA) featuring actions, synchronisation, non-determinism,

parallel composition, destructive measurements and unitary transformations, and we enrich it with two different semantics: a stateful Schrödinger-style semantics that given a quantum state as input returns a pLTS representing the observable behaviour of the system; and an Heisenberg-style semantics in the form of an eLTS that is independent of the actual quantum input, in the style of [10, 19]. We prove that the Heisenberg-style eLTS is indeed the "symbolic" version of the Schrödinger-style pLTSs of the same system. In a nutshell, this means that we can prove bisimilarity just once on the Heisenberg semantics, and have it automatically verified for all the possible "ground" systems obtained by instantiating the quantum input. Notably, our notion of bisimilarity can be efficiently verified with standard techniques [21].

Synopsis. In section 2 we give some background about probability distributions and quantum theory. In section 3 we introduce effect distributions and eLTSs, we investigate their properties and compare eLTS bisimilarities. In section 4 we present our minimal process algebra, enriched with both a stateful and a stateless semantics, which are proved to coincide. Finally, we compare with related works in section 5, and we conclude in section 6. The full proofs of our results are postponed to the Appendix.

2 BACKGROUND

We recall some background on probability distributions, and we introduce quantum computing. Finally, we present density operators, modelling probability distributions of quantum systems. We refer to [29] for further reading on quantum computing.

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 call the *support* of a distribution Δ, written $\operatorname{supp}\Delta$, the set $\{s \in S \mid \Delta(s) > 0\}$. We write $\mathcal{D}S$ for the set of finitely supported distributions over S. We say that a probability distribution Δ is *total* when $\sum_{s\in S} \Delta(s) = 1$.

For each $s \in S$, we let $\overline{s}$ be the *point distribution* that assigns 1 to s. Given a finite set of non-negatives reals $\{p_i\}_{i\in I}$ such that $\sum_{i\in I} p_i \leq 1$, we write $\sum_{i\in I} p_i \cdot \Delta_i$ for the distribution determined by $(\sum_{i\in I} p_i \cdot \Delta_i)(s) = \sum_{i\in I} p_i \Delta_i(s)$.

Probability distributions form a *convex set* [3], meaning that for any two distribution Δ, Θ and any real $p \in [0,1]$ there exists a distribution $\Delta \,{}_p\!\oplus\, \Theta$ defined as $p \cdot \Delta_1 + (1-p) \cdot \Delta_2$. Given a function f between convex sets X and Y, we call f 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 State Space

A (finite-dimensional) *Hilbert space*, denoted as $\mathcal{H}$, is a complex vector space equipped with a binary operator $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ called *inner product*, defined as $\langle\psi|\phi\rangle = \sum_i \alpha_i^* \beta_i$, where $|\psi\rangle = (\alpha_1, \ldots, \alpha_i)^T$ and $|\phi\rangle = (\beta_1, \ldots, \beta_i)^T$. We indicate column vectors as $|\psi\rangle$ and their conjugate transpose as $\langle\psi| = |\psi\rangle^\dagger$. The state of an isolated physical system is represented as a *unit vector* $|\psi\rangle$ (called *state vector*), i.e. a vector such that $\langle\psi|\psi\rangle = 1$. The simplest example of a quantum physical system is a *qubit*, which is associated with the two-dimensional Hilbert space $\mathbb{C}^2$. The vectors $\{|0\rangle = (1,0)^T, |1\rangle = (0,1)^T\}$ form an orthonormal basis of $\mathbb{C}^2$, called the *computational basis*. Other important vectors in $\mathbb{C}^2$ 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*.

Intuitively, different bases represent different observable properties of a quantum system. Note that $|+\rangle$ and $|-\rangle$ are non-trivial linear combinations of $|0\rangle$ and $|1\rangle$, roughly meaning that the property associated with the computational basis is undetermined in $|+\rangle$ and $|-\rangle$. In the quantum jargon, $|+\rangle$ and $|-\rangle$ are *superpositions* with respect to the computational basis. Symmetrically, $|0\rangle$ and $|1\rangle$ are superpositions with respect to the Hadamard one.

2.3 Unitary Transformations

For each linear operator A on a Hilbert space $\mathcal{H}$, there is a linear operator $A^\dagger$, the *adjoint* of A, which is given by the conjugate transpose of A and is the unique operator such that $\langle\psi|A|\phi\rangle = \langle A^\dagger\psi|\phi\rangle$. A linear operator U is said to be *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. $|\psi'\rangle = U|\psi\rangle$.

In quantum computing, the programmer manipulates the state of qubits by applying unitary transformations. Some of the most common transformations on single qubits are: X that transforms the qubit $|0\rangle$ into $|1\rangle$ and vice-versa (corresponding to the classical logical not); Z that given $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ returns $\alpha|0\rangle - \beta|1\rangle$; and H that maps $|0\rangle$ and $|1\rangle$ into $|+\rangle$ and $|-\rangle$, respectively.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

2.4 Measurement

Quantum measurements are needed for describing systems that exchange information with the environment. Performing a measurement on a quantum state returns a probabilistic classical result and either destroys or otherwise changes the quantum system. We focus in this paper on destructive measurements.

The simplest kind of measurements are *effects*, i.e. yes-no tests over quantum systems. A complex matrix A is called *positive semi-definite*, shortly positive, when $\langle\psi|A|\psi\rangle \geq 0$ for any $|\psi\rangle$. The *Löwner order* is the partial order defined by $A \sqsubseteq B$ whenever $B - A$ is positive. Each effect can be represented as a positive matrix smaller than the identity in the Löwner order. We denote the set of effects on a d-dimensional Hilbert space as follows, where $\mathbb{I}_d$ is the $d \times d$ identity matrix.

$$\mathcal{E}f_d = \left\{ E \in \mathbb{C}^{d\times d} \mid 0_d \sqsubseteq E \sqsubseteq \mathbb{I}_d \right\}$$

The probability of getting a "yes" outcome when measuring an effect E on a state $|\psi\rangle$ is given by $\langle\psi|E|\psi\rangle$.

In general, a measurement with n different outcomes is a set $\{E_1, \ldots E_n\}$ of effects, such that the *completeness* equation $\sum_{i=1}^n E_i = \mathbb{I}$ holds. If the state of the system is $|\psi\rangle$ before the measurement, then the probability of the i outcome occurring is $p_i = \langle\psi| E_i |\psi\rangle$.

As examples of measurements, consider M_{01} and $M_\pm$ that project a state into the elements of the computational and Hadamard basis of $\mathbb{C}^2$ respectively. The measurement M_{01} is 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 $|+\rangle$, instead, the same result occurs with probability $\frac{1}{2}$.

2.5 Composite Quantum Systems

We represent the state space of a composite physical system as the *tensor product* of the state spaces of its components. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be n and m-dimensional Hilbert spaces: their tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ is an $n \cdot m$ Hilbert space. Moreover, if $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ and $\{|\phi_1\rangle, \ldots, |\phi_m\rangle\}$ are bases of respectively $\mathcal{H}_A$ and $\mathcal{H}_B$, then $\{|\psi_i\rangle \otimes |\phi_j\rangle \mid i = 1, \ldots, n, j = 1, \ldots, m\}$ is a basis of $\mathcal{H}_A \otimes \mathcal{H}_B$, where $|\psi\rangle \otimes |\phi\rangle$ is the Kronecker product, defined as

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

We often omit the tensor product and write $|\psi\rangle\,|\phi\rangle$ or $|\psi\phi\rangle$.

A measurement for a composite system may measure only some of the qubits, e.g. $\{E_0 \otimes \mathbb{I}, E_1 \otimes \mathbb{I}\}$ measures (in the computational basis) the first qubit of a pair.

A quantum state in $\mathcal{H}_A \otimes \mathcal{H}_B$ is *separable* when it can be expressed as the Kronecker product of two vectors of $\mathcal{H}_A$ and $\mathcal{H}_B$. Otherwise, it is *entangled*, like the so-called Bell states:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

When two qubits are entangled, the evolution of one depends on the transformations applied to the other. E.g. measuring the first qubit of $\left|\Phi^+\right\rangle$ in the computational basis causes the second qubit to *decay* into either $|0\rangle$ or $|1\rangle$ with equal probability, as will be explained in the next section. Note that, this means that even when performing a destructive measurement on a qubit, the state of the remaining part of the composite system must be updated in general, as the two components may be entangled.

2.6 Density Operator Formalism

The density operator formalism puts together quantum systems and probability by considering mixed states, i.e. *probabilistic mixture 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 total probability distribution Δ of n-dimensional states is represented as the matrix $\rho \in \mathbb{C}^{n\times n}$, known as its *density operator*, with $\rho = \sum_i \Delta(\psi_i)\,|\psi_i\rangle\langle\psi_i|$. For example, the mixed state $\overline{|0\rangle}\,{}_{1/3}\!\oplus\,\overline{|+\rangle}$ being $|0\rangle$ with probability $1/3$ and in $|+\rangle$ with probability $2/3$ is represented as

$$\frac{1}{3}\,|0\rangle\langle 0| + \frac{2}{3}\,|+\rangle\langle +| = \frac{1}{3}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Given an n-dimensional Hilbert space, the density operators constructed in this way are all and only the positive matrices of trace one. We denote such set as DM_n

$$DM_n = \left\{\, \rho \in \mathbb{C}^{d\times d} \mid \rho \sqsupseteq 0_d,\ \mathrm{tr}(\rho) = 1 \,\right\}$$

Note that the encoding of probabilistic mixtures of quantum states as density operators is not injective. For example, $\frac{1}{2}\mathbb{I}$ is called the *maximally mixed state* and represents both the distribution $\Delta_C = \overline{|0\rangle}\,{}_{1/2}\!\oplus\,\overline{|1\rangle}$ and $\Delta_H = \overline{|+\rangle}\,{}_{1/2}\!\oplus\,\overline{|-\rangle}$. This is a desired feature, as the laws of quantum mechanics deem indistinguishable all the distributions that result in the same density operator.

Density operators form a convex set, where the convex combination operator is defined by $\rho\ {}_p\!\oplus\,\sigma = p\rho + (1-p)\sigma$. Density operators and effects are dual, as effects are isomorphic to the convex functions from the set of density operators to the probability interval. The isomorphism is given by the so-called *Born rule*.

Theorem 1. *It holds that* $\mathcal{E}f_n \cong \mathbf{Conv}(DM_n, [0,1])$ *through the isomorphism* $E \mapsto \lambda\rho.\, tr(E\rho)$ *[17].*

Roughly, effects can be considered as probabilities *parametrized* on an unknown quantum state.

Density operators can be used to describe the state of a subsystem of a composite quantum system. Let $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ represent a composite system, with subsystems A and B. Given a (not necessarily separable) $\rho^{AB} \in \mathcal{H}_{AB}$, the *reduced density operator* of system A, $\rho^A = \mathrm{tr}_B(\rho^{AB})$, describes the state of the subsystem A, with tr_B the *partial trace over B*, defined as the linear transformation such that $\mathrm{tr}_B(|\psi\rangle\langle\psi'| \otimes |\phi\rangle\langle\phi'|) = |\psi\rangle\langle\psi'|\,\mathrm{tr}(|\phi\rangle\langle\phi'|)$. When applied to pure separable states, the partial trace returns the actual state of the subsystem. When applied to an entangled state, instead, it returns a probability distribution of states. For example, the partial trace over the first qubit of $\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|$ is the maximally mixed state.

The evolution of density operators is given as a *trace preserving superoperator* $\mathcal{E} : DM_n \to DM_m$, a function defined by its *Kraus operator sum decomposition* $\{E_i\}_i$ for a finite set of indexes $i = 1, \ldots, n \times m$, satisfying that $E_i \in \mathbb{C}^{m\times n}, \mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ and $\sum_i E_i^\dagger E_i = \mathbb{I}_n$. Superoperators can represent any unitary transformations U as the superoperator $\mathcal{E}_U$ having $\{U\}$ as its Kraus decomposition. The tensor product of density operators $\rho \otimes \sigma$ is defined as their Kronecker product, and of superoperators $\mathcal{E} \otimes \mathcal{F}$ as the superoperator having Kraus decomposition $\{E_i \otimes F_j\}_{i,j}$ with $\{E_i\}_i$ and $\{F_j\}_j$ Kraus decompositions of $\mathcal{E}$ and $\mathcal{F}$.

In the final section of this paper we will employ sub-probability distributions of pure states, thus leading to the notion of *partial density operators* and *trace non-increasing superoperators*. To each sub-probability distribution we associate a partial density operator, belonging to the set

$$pDM_n = \left\{\, \rho \in \mathbb{C}^{d\times d} \mid \rho \sqsupseteq 0_d,\ \mathrm{tr}(\rho) \le 1 \,\right\}.$$

Transformations between such density operators are trace non-increasing superoperators $\mathcal{E} : pDM_n \to pDM_m$, having Kraus operators $\{E_i\}_i$ satisfying $\sum_i E_i^\dagger E_i \sqsubseteq \mathbb{I}_n$. We let $\mathcal{SO}_d$ be the set of non-increasing superoperators with input in pDM_d.

Trace non-increasing superoperators allow us to describe how entangled systems change after a destructive measurement. Suppose having a compound system associated to a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. If we measure only the A sub-system using the measurement $M = \{E_1, \ldots E_n\}$, we can describe the transformation applied by this measurement with superoperators. For each effect E_i we define the associated superoperator $\mathcal{M}_{E_i}$:

$$\mathcal{M}_{E_i}(\rho) = tr_A((\sqrt{E_i} \otimes \mathbb{I}_B)\rho(\sqrt{E_i} \otimes \mathbb{I}_B))$$

We have that, if the system was in a state ρ, after observing the i-th measurement outcome the B sub-system will be in state $\mathcal{M}_{E_i}(\rho)$, which in general is a partial density operator, whose trace is exactly the probability of observing the i-th outcome.

Superoperators gives us information on both the probability of an outcome and how the state is modified. Thus, we can define also the converse operation, introducing for each superoperator $\mathcal{E}$ its *associated effect*

$$E_{\mathcal{E}} = \sum_i E_i^\dagger E_i$$

where $\{E_i\}_i$ is any Kraus decomposition of $\mathcal{E}$.

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 case for eLTSs, and we advocate for the latter being adequate for comparing the behaviour of quantum systems. Finally, we define semantic operations over eLTSs suited for modelling concurrent quantum systems, and we study their limitations.

3.1 Effect Distribution

We introduce effect distributions, i.e. functions associating each element of a given set X with some d-dimensional effect.

Definition 1. *Given a set X, the set of d-*dimensional finite effect (sub)distributions *over X is*

$$\mathcal{Q}_d X = \left\{ \mathfrak{D} \in \mathcal{E}f_d{}^X \;\middle|\; \mathrm{supp}(\mathfrak{D}) \text{ is finite}, \sum_{x \in \mathrm{supp}(\mathfrak{D})} \mathfrak{D}(x) \sqsubseteq I_d \right\}$$

where $supp(\mathfrak{D})$ is the set $\{\, x \in X \mid \mathfrak{D}(x) \neq 0_d \,\}$.

Effect distributions are finite non-normalized POVMs [17] and they generalize probability distributions. More in detail, 1×1 positive matrices are isomorphic to real numbers, hence $\mathcal{Q}_1 X$ coincides with the usual set of probability distributions $\mathcal{D}X$.

Since effects can be regarded as functions from states to probabilities, an effect distribution $\mathfrak{D} \in \mathcal{Q}_d X$ denotes a function $\mathfrak{D}{\downarrow}_{\_} \in (\mathcal{D}X)^{DM_d}$ associating any $\rho \in DM_d$ with the probability distribution $\mathfrak{D}{\downarrow}_\rho$ such that $\mathfrak{D}{\downarrow}_\rho(x) = tr(\mathfrak{D}(x) \cdot \rho)$ 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 2. *Effect distributions correspond to all and only the parameterized sub-probability distributions that are convex and have an "overall" finite support.*

$$\mathcal{Q}_d \cong \left\{ \mathfrak{D}{\downarrow}_{\_} \in (\mathcal{D}(X))^{DM_d} \;\middle|\; \begin{array}{l} \mathfrak{D}{\downarrow}_{\rho \,{}_p\!\oplus\, \sigma} = (\mathfrak{D}{\downarrow}_\rho) \,{}_p\!\oplus\, (\mathfrak{D}{\downarrow}_\sigma) \\ \bigcup_{\rho \in DM_d} \mathrm{supp}(\mathfrak{D}{\downarrow}_\rho) \text{ is finite} \end{array} \right\}$$

Proof sketch. We begin from the isomorphism between effects and functions in $\mathbf{Conv}(DM_d, [0,1])$, and we lift it in a point-wise manner to effect distributions, making them isomorphic to functions in $\mathbf{Conv}(DM_d, [0,1])^X$. Thus, we swap the arguments and check both convexity and finiteness of the union of supports. □

We represent effect distributions as indexed 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 $\mathfrak{D}(x_i) = \sum_{x_i = x} E_i$. 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. We let $\overline{x} \in \mathcal{Q}_1 X$ be the point distribution $\overline{x}(x) = 1$.

Example 1. *Let $X = \{x, y\}$. The effect distribution $\mathfrak{D} = \{x \rhd \frac{1}{2}, y \rhd \frac{1}{2}\}$ is indeed a fair probability distribution, i.e. an effect distribution in a 1-dimensional Hilbert space.*

A similar distribution on a two-dimensional Hilbert space is $\mathfrak{G} = \{x \rhd \frac{1}{2}\mathbb{I}, y \rhd \frac{1}{2}\mathbb{I}\}$, associating x and y with the same probability once an input quantum state is given.

Finally, given the quantum input $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$ and the distribution $\mathfrak{T} = \{x \rhd |0\rangle\langle 0|, y \rhd |1\rangle\langle 1|\}$, the probability distribution $\mathfrak{T}{\downarrow}_\rho$ associates x with the probability $\frac{3}{4}$ and y with $\frac{1}{4}$.

As for probability distributions, we compose multiple effect distributions in an effect-weighted sum.

Definition 2. *Given n effect distributions $\{\mathfrak{D}_i\}_{i \in I}$, and n effects $\{E_i\}_{i \in I}$ such that $\sum_i E_i \sqsubseteq \mathbb{I}$, the weighted sum of $\{\mathfrak{D}_i\}_{i \in I}$ with effects $\{E_i\}_{i \in I}$ is an effect distribution*

$$\sum_{i \in I} E_i \otimes \mathfrak{D}_i \text{ such that } \left(\sum_{i \in I} E_i \otimes \mathfrak{D}_i \right)(x) = \sum_{i \in I} E_i \otimes \mathfrak{D}_i(x)$$

This composition results in a distribution on a Hilbert space of dimension $d \cdot d'$, and coincides with the usual weighted sum of probability distributions if $d = d' = 1$. Intuitively, $\mathfrak{D}$ measures a portion of the quantum state to choose between the distributions $\mathfrak{D}_i$ (which in turn behave accordingly to the quantum state). We will sometimes write $E_1 \otimes \mathfrak{D}_1 + \cdots + E_n \otimes \mathfrak{D}_n$ for $\sum_i E_i \otimes \mathfrak{D}_i$.

Example 2. *Take $\mathfrak{G}$ and $\mathfrak{T}$ of Example 1. The effect distribution $|+\rangle\langle +| \otimes \mathfrak{G} + |-\rangle\langle -| \otimes \mathfrak{T}$ can be rewritten as*

$$\left\{ x \rhd \frac{1}{2}|+\rangle\langle +| \otimes \mathbb{I}, y \rhd \frac{1}{2}|+\rangle\langle +| \otimes \mathbb{I}, x \rhd |-0\rangle\langle -0|, y \rhd |-1\rangle\langle -1| \right\}.$$

Intuitively, this represents the probabilistic outcome of applying the following cascade of two measurement procedures to the input quantum state: measure the first qubit over the Hadamard basis, if the qubit is found in $|+\rangle$ then discard the second qubit and returns either x or y with the same probability, otherwise measure the second qubit in the computational basis and return x if you observe $|0\rangle$ and y otherwise.

In the probabilistic case, it is usual to consider just the binary composition $\Delta \,{}_p\!\oplus\, \Theta$, defined as $p \cdot \Delta + (1-p) \cdot \Theta$. 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 3. *Let $\mathfrak{D} \,{}_E\!\oplus\, \mathfrak{T}$ be the weighted sum $E \otimes \mathfrak{D} + (\mathbb{I} - E) \otimes \mathfrak{T}$.*

Some effect distributions with support bigger than two can be defined by a nesting of $\oplus$ expressions over point distributions.

Example 3. *The effect distribution over* $S = \{x_1, x_2, x_3, x_4\}$

$$\mathfrak{D} = \{x_1 \rhd |0+\rangle\langle 0+|\,, x_2 \rhd |0-\rangle\langle 0-|\,,$$
$$x_3 \rhd |1+\rangle\langle 1+|\,, x_4 \rhd |1-\rangle\langle 1-|\}$$

can be obtained as $(\overline{x_1}\ {}_{|+\rangle\langle+|}\oplus\ \overline{x_2})\ {}_{|0\rangle\langle 0|}\oplus\ (\overline{x_3}\ {}_{|+\rangle\langle+|}\oplus\ \overline{x_4})$.

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 $\oplus$.

Definition 4. *Given a set* X*, we let* $\mathcal{Q}^{\oplus}X$ *be the smallest family of sets* $\mathcal{Q}^{\oplus}_d X \subseteq \mathcal{Q}_d X$ *such that* $\mathcal{Q}^{\oplus}_1 X$ *contains* $\overline{x}$ *for any* $x \in X$*, and, if* $\mathfrak{D}, \mathfrak{T} \in \mathcal{Q}^{\oplus}_d X$ *then* $\mathfrak{D}\ {}_E\oplus\ \mathfrak{T} \in \mathcal{Q}^{\oplus}_{d\cdot d'} X$ *for any effect* $E \in \mathcal{E}f_{d'}$.

Some (finite support) effect distributions cannot be defined using $\oplus$, as stated by the following theorem.

Theorem 3. *If the cardinality of* X *and* d *are at least four, then* $\mathcal{Q}^{\oplus}_d X \neq \mathcal{Q}_d X$.

Proof sketch. First, we show that the effect $\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|$ cannot be expressed as the tensor product of two-dimensional effects. We then consider the following effect distribution

$$\{x_1 \rhd \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|, x_2 \rhd |\Phi^-\rangle\langle\Phi^-|\,, x_3 \rhd \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right|, x_4 \rhd |\Psi^-\rangle\langle\Psi^-|\}$$

and we prove by induction that it is not in $\mathcal{Q}^{\oplus}_4 X$. □

Adhering with the previous result, we use general n-ary composition of effect distributions.

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 requiring paired distributions to associate related states with the same effects.

Definition 5. *For any dimension* d*, we let* $\overset{\square}{\mathcal{R}}_d \subseteq \mathcal{Q}_d X \times \mathcal{Q}_d X$ *be the* lifting *of dimension* d *of* $\mathcal{R} \subseteq X \times X$ *given as the least relation satisfying the following rules*

$$\frac{s\,\mathcal{R}\,t}{\overline{s}\ \overset{\square}{\mathcal{R}}_1\ \overline{t}} \qquad \frac{\mathfrak{D}_i\ \overset{\square}{\mathcal{R}}_{d'}\ \mathfrak{T}_i}{(\textstyle\sum_{i\in I} E_i \otimes \mathfrak{D}_i)\ \overset{\square}{\mathcal{R}}_{d\cdot d'}\ (\sum_{i\in I} E_i \otimes \mathfrak{T}_i)}\ (E_i \in \mathcal{E}f_d)$$

Note that $\overset{\square}{\mathcal{R}}_1$ is the usual probabilistic lifting of [18]. We then recover the following property, known as decomposability.

Lemma 1. *Let* $\mathcal{R} \subseteq X \times X$*. Then* $\mathfrak{D}\ \overset{\square}{\mathcal{R}}_d\ \mathfrak{T}$ *if and only if there is a finite index set* I *and an effect set* $E_i \in \mathcal{E}f_d$ *such that*

(1) $\mathfrak{D} = \{x_i \rhd E_i\}_{i\in I}$
(2) $\mathfrak{T} = \{y_i \rhd E_i\}_{i\in I}$
(3) $x_i\,\mathcal{R}\,y_i$ *for each* $i \in I$

Proof sketch. Proving that this condition implies $\mathfrak{D}\ \overset{\square}{\mathcal{R}}_d\ \mathfrak{T}$ is trivial. Then we proceed by induction on the rules of the lifting. □

3.2 Effect Transition Systems

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

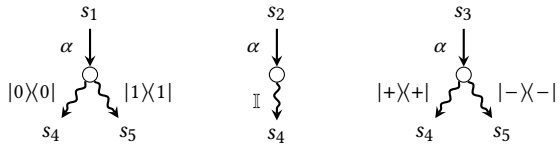


Figure 1: ELTs for the states of Example 4.

Definition 6. *An eLTS of dimension* d *is a triple* $(S, Act, \longrightarrow)$ *where* S *is a set of states,* Act *is a set of labels, and* $\longrightarrow \subseteq S \times Act \times \mathcal{Q}_d S$ *is the transition relation. As usual, we write* $s \xrightarrow{\mu} \mathfrak{D}$ *for* $(s, \mu, \mathfrak{D}) \in \longrightarrow$.

Hereafter, we assume as given a d-dimensional eLTS $(S, Act, \longrightarrow)$. We instantiate two distinct definitions of semantic equivalence on quantum systems: *Aczel-Mendler* and *Larsen-Skou* bisimilarities [32]. They are known to coincide on classical probabilistic processes [18]. Notably, they do not in the quantum case.

Definition 7. *A symmetric relation* $\mathcal{R} \subseteq S \times S$ *is an* AM-bisimulation *if for any* $s\mathcal{R}t$

$$\text{if } s \xrightarrow{\mu} \mathfrak{D} \text{ then } t \xrightarrow{\mu} \mathfrak{T} \text{ for some } \mathfrak{T} \text{ such that } \mathfrak{D}\ \overset{\square}{\mathcal{R}}_d\ \mathfrak{T}$$

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

Example 4. *Consider the states* s_1, s_2, s_3, s_4 *and* s_5 *such that:*

- s_1 *transitions with* α *to* $\mathfrak{D} = \{s_4 \rhd |0\rangle\langle 0|\,, s_5 \rhd |1\rangle\langle 1|\}$;
- s_2 *transitions with* α *to* $\mathfrak{G} = \{s_4 \rhd \mathbb{I}\}$;
- s_3 *transitions with* α *to* $\mathfrak{T} = \{s_4 \rhd |+\rangle\langle+|\,, s_5 \rhd |-\rangle\langle-|\}$;
- *there is no other transition for* s_1, s_2, s_3, s_4 *and* s_5.

We depict their eLTSs in Figure 1 (note that s_4 *and* s_5 *are deadlock states). We have that* $s_1 \sim_{am} s_2$ *and* $s_2 \sim_{am} s_3$*. Indeed,*

$$|0\rangle\langle 0| + |1\rangle\langle 1| = I = |+\rangle\langle+| + |-\rangle\langle-|\,, \text{ and hence}$$
$$\mathfrak{D}\ \overset{\square}{\sim}_{am}\ \{Y \rhd |0\rangle\langle 0|\,, s_4 \rhd |1\rangle\langle 1|\} = \mathfrak{G},$$
$$\mathfrak{T}\ \overset{\square}{\sim}_{am}\ \{Y \rhd |+\rangle\langle+|\,, s_4 \rhd |-\rangle\langle-|\} = \mathfrak{G}.$$

Nonetheless, $s_1 \not\sim_{am} s_3$ *as we cannot write* $\mathfrak{D}$ *and* $\mathfrak{T}$ *using the same effects, as it would be required by Lemma 1.*

This example, inspired by [31], proves that $\sim_{am}$ is not transitive. We thus generalize *Larsen-Skou bisimilarity* [25] to the quantum case (named kernel bisimilarity in [32]).

Definition 8. *An equivalence relation* $\mathcal{R} \subseteq S \times S$ *is an* LS-bisimulation *if for any* $s\mathcal{R}t$

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

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 $\sim_{am}$.

Example 5. *Consider Example 4. 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* $\mathbb{I}$.

Indeed, LS-bisimilarity is coarser than AM-bisimilarity.

Theorem 4. *For any eLTS, $\sim_{am} \subseteq \sim_{ls}$. Moreover, $\sim_{am} = \sim_{ls}$ in eLTSs of dimension one, and $\sim_{am} \subsetneq \sim_{ls}$ for any eLTS of dimension at least two with S of cardinality at least four.*

Proof. For $\subseteq$ it is sufficient to show that $\mathfrak{D} \overset{\square}{\mathcal{R}} \mathfrak{T}$ requires $\mathfrak{D}$ and $\mathfrak{T}$ to assign the same effect to each class in $S/_{\mathcal{R}}$, by Lemma 1. The equality $\sim_{am} = \sim_{ls}$ in eLTSs of dimension one is a classical for pLTSs [18]. Then it suffices to consider Example 5. □

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

Since probabilistic behaviour is the only observable property of quantum systems, we consider this characterization as the ground truth our behavioural equivalence must comply with. We now 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.

Definition 9. *Given $\rho \in DM_d$, a symmetric relation $\mathcal{R} \subseteq S \times S$ is a* ρ-bisimulation *if for any $s\mathcal{R}t$*

$$\text{if } s \xrightarrow{\mu} \mathfrak{D} \text{ then } t \xrightarrow{\mu} \mathfrak{T} \text{ for some } \mathfrak{T} \text{ such that } \mathfrak{D}\downarrow_\rho \overset{\square}{\mathcal{R}}_1 \mathfrak{T}\downarrow_\rho$$

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

$$\simeq_{pbe} \;=\; \bigcap_{\rho \in DM_d} \sim_\rho$$

As effects and effect distributions are convex parameterized probabilities and probability distributions respectively, eLTSs are can be seen as parameterized pLTSs. Along the same correspondence, LS-bisimilarity can be shown to relate states that behave the same for every possible choice of quantum input at every step. We define such a relation as a locally-parameterised probabilistic bisimilarity.

Definition 10. *A symmetric relation $\mathcal{R} \subseteq S \times S$ is a* lpp-bisimulation *if for any $s\mathcal{R}t$*

$$\text{if } s \xrightarrow{\mu} \mathfrak{D} \text{ then } t \xrightarrow{\mu} \mathfrak{T} \text{ for some } \mathfrak{T} \text{ such that}$$

$$\mathfrak{D}\downarrow_\rho \overset{\square}{\mathcal{R}}_1 \mathfrak{T}\downarrow_\rho \quad \text{for any } \rho \in DM_d$$

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

Theorem 5. *For any $s, t \in S$, $s \sim_{ls} t$ if and only if $s \sim_{lpp} t$.*

Proof sketch. We employ Theorem 2, telling us that comparing effects directly or through their probabilistic behaviour is the same. Thus, LS-bisimilarity is a lpp-bisimulation, and *vice versa*. □

Note that the difference between lpp-bisimilarity and probabilistic behavioural equivalence (our ground truth) is essentially that for disproving bisimilarity one can choose a different state ρ at any step for the former and a single, global one for the latter.

Example 6. *Consider the eLTS in Figure 2. To show that $s_1 \nsim_{lpp} s_2$ it suffices to choose $|0\rangle\langle 0|$ for the first reduction of s 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, since $\mathfrak{G}\downarrow_{|+\rangle\langle +|} = \overline{s_5}$ and $\mathfrak{R}\downarrow_{|+\rangle\langle +|} = \overline{s_8}$, $s_3 \sim_{lpp} s_4$ requires $s_5 \sim_{lpp} s_8$ which is trivially disproved by observing the labels of the available transitions.*

Finally, note that neither $|0\rangle\langle 0|$ nor $|+\rangle\langle +|$ 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 $\mathfrak{D}\downarrow_{|+\rangle\langle +|} = \mathfrak{T}\downarrow_{|+\rangle\langle +|}$, and hence $s_1 \sim_{|j\rangle\langle j|} s_2$ for $|j\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

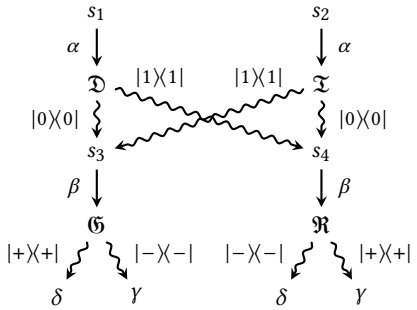


Figure 2: An eLTS where $s_1 \nsim_{lpp} s_2$.

Quite surprisingly, for finite eLTSs the two relations $\sim_{lpp}$ and $\simeq_{pbe}$ coincides in spite of that, and hence, we deem LS-bisimilarity as ours bisimilarity of choice, as it precisely capture the observable properties of quantum systems.

Theorem 6. *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 sketch. By Theorem 5, for proving $\sim_{ls} \subseteq \simeq_{pbe}$ it suffices to show that $\sim_{lpp} \subseteq \simeq_{pbe}$, which holds by definition.

For $\simeq_{pbe} \subseteq \sim_{ls}$, we consider the (finite) set of effects $\mathbb{E}$ that may be applied to equivalence classes in the eLTS, and we build a density operator $\rho_{\mathbb{E}}$ that distinguish all the effects in $\mathbb{E}$. This allows us to prove that $\sim_{\rho_{\mathbb{E}}}$ is an LS-bisimilarity, since associating the same probability to all classes with quantum input $\rho_{\mathbb{E}}$ requires the effects to be the same. We conclude by noticing that $\simeq_{pbe} \subseteq \sim_{\rho_{\mathbb{E}}} \subseteq \sim_{ls}$. □

Indeed, $s_1 \simeq_{pbe} s_3$ for s_1 and s_3 of Example 4, and a single quantum state is sufficient for distinguishing s_1 and s_2 of Example 6.

Example 7. *Consider Figure 2, and let $\rho = |0\rangle\langle 0| \;\frac{1}{2}\oplus\; |+\rangle\langle +|$. Then $s_1 \nsim_\rho s_2$ (and hence $s_1 \nsim_{pbe} s_2$). 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 $s_3 \sim_\rho s_4$. Since $\mathfrak{G}\downarrow_\rho = \overline{\delta} \;\frac{3}{4}\oplus\; \overline{\gamma}$ and $\mathfrak{R}\downarrow_\rho = \overline{\delta} \;\frac{1}{4}\oplus\; \overline{\gamma}$, $s_3 \sim_\rho s_4$ implies $\delta \sim_\rho \gamma$, which is trivially disproved.*

3.3 Operators on eLTSs

Languages for defining labelled transition systems commonly relies on suitable composition operators, in the fashion of process algebras like CCS and CSP. In particular, when distributions are considered, like for pLTSs and eLTSs, one usually considers both operators acting on states and on distributions.

3.3.1 Operators on States. In the following we will discuss the lifting of operators commonly considered for probabilistic systems to the case of eLTSs, starting from nondeterministic sum and parallel

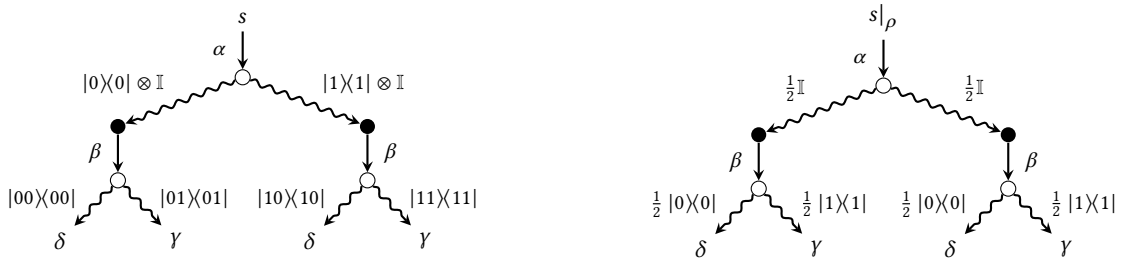


Figure 3: A 4-dimensional ELTS and its quantum partial evaluated version with $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$.

composition of states. We will then propose a new operator that is tailored for the quantum case.

Definition 11. *Given two d-dimensional eLTSs $(S_1, Act_1, \rightarrow_1)$ and $(S_2, Act_2, \rightarrow_2)$, their non-deterministic sum is a d-dimensional eLTS with states $S_1 \cup S_2 \cup \{s_1 + s_2 \text{ with } s_i \in S_i \text{ for } i = 1, 2\}$, actions $Act_1 \cup Act_2$ and such that the transitions is the smallest set including both $\rightarrow_1$ and $\rightarrow_2$ and satisfying the following rules*

$$\frac{s_1 \xrightarrow{\mu} \mathfrak{D}}{s_1 + s_2 \xrightarrow{\mu} \mathfrak{D}}\ \textsc{ExtL} \qquad \frac{s_2 \xrightarrow{\mu} \mathfrak{D}}{s_1 + s_2 \xrightarrow{\mu} \mathfrak{D}}\ \textsc{ExtR}$$

Theorem 7. *If $s_1 \sim_{ls} s_2$ and $t_1 \sim_{ls} t_2$ then $s_1 + t_1 \sim_{ls} s_2 + t_2$.*

Proof sketch. By cases on the rules ExtL and ExtR. □

Synchronization is a crucial aspect of protocols and process algebras. Therefore, from now on we assume that *Act* contains a distinguished element τ, and that every other operation $\alpha \in Act$ has in inverse $\overline{\alpha}$ such that $\overline{\overline{\alpha}} = \alpha$.

Definition 12. *Given two eLTSs $(S_1, Act_1, \rightarrow_1)$ of dimension d and $(S_2, Act_2, \rightarrow_2)$ of dimension d', their parallel composition is a eLTS of dimension $d \cdot d'$ with states $s_1 \parallel s_2$ with $s_i \in S_i$ for $i = 1, 2$, actions $Act_1 \cup Act_2$ and such that the transitions are defined by*

$$\frac{s_1 \xrightarrow{\mu} \mathfrak{D}}{s_1 \parallel s_2 \xrightarrow{\mu} \mathfrak{D} \parallel \{s_2 \rhd \mathbb{I}_{d'}\}}\ \textsc{ParL} \qquad \frac{s_2 \xrightarrow{\mu} \mathfrak{D}}{s_1 \parallel s_2 \xrightarrow{\mu} \{s_1 \rhd \mathbb{I}_d\} \parallel \mathfrak{D}}\ \textsc{ParR}$$

$$\frac{s_1 \xrightarrow{\mu} \mathfrak{D} \quad s_2 \xrightarrow{\overline{\mu}} \mathfrak{T}}{s_1 \parallel s_2 \xrightarrow{\tau} \mathfrak{D} \parallel \mathfrak{T}}\ \textsc{Synch}$$

$$\text{where } (\mathfrak{D} \parallel \mathfrak{T})(s) = \begin{cases} \mathfrak{D}(s_1) \otimes \mathfrak{T}(s_2) & \text{if } s = s_1 \parallel s_2 \\ 0 & \text{otherwise} \end{cases}$$

Theorem 8. *If $s_1 \sim_{ls} s_2$ and $t_1 \sim_{ls} t_2$, then $s_1 \parallel t_1 \sim_{ls} s_2 \parallel t_2$.*

Proof sketch. By cases on the rules ParL, ParR and Synch. □

The next operator is specific for the quantum case. Since effects are essentially classical probabilities parameterized over an input quantum state, it is reasonable to consider the operation of instantiating some of the input qubits of an eLTS via a partial evaluation. As expected, the result will be an eLTS that takes as input a quantum state in a smaller Hilbert space (possibly even no input at all, meaning that the behaviour is now unconditionally probabilistic).

We first define partial evaluation of an effect.

Definition 13. *Let A and B be two quantum systems, with states in the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Let ρ be a density operator in $\mathcal{H}_A$ and E be an effect on $\mathcal{H}_A \otimes \mathcal{H}_B$. The partial evaluation of E with input ρ is the effect*

$$E\big|_\rho = tr_A(E(\rho \otimes \mathbb{I}_C)).$$

We can now instantiate the same over states of an eLTS.

Definition 14. *Given an eLTSs $(S, Act, \rightarrow)$ of dimension $d \cdot d'$ and a density operator $\rho \in DM_d$, the quantum partial evaluation of the eLTS with ρ is a d'-dimensional eLTS with states $s|_\rho$ for $s \in S$, actions Act and such that the transitions are defined by the following rule*

$$\frac{s \xrightarrow{\mu} \mathfrak{D}}{s|_\rho \xrightarrow{\mu} \mathfrak{D}|_\rho}\ \textit{QInst}$$

$$\text{where } \mathfrak{D}\big|_\rho(s) = \begin{cases} \mathfrak{D}(s')|_\rho & \text{if } s = s'|_\rho \\ 0 & \text{otherwise} \end{cases}$$

Theorem 9. *If $s \sim_{ls} t$ then $s|_\rho \sim_{ls} t|_\rho$ for any ρ.*

Proof sketch. By definition of $s|_\rho$ and $\mathfrak{D}|_\rho$. □

As previously stated, for ρ sufficiently large the partial evaluation returns a probabilistic system obtained by taking the same quantum input for each effect distribution of the eLTS. This means that $s|_\rho \sim_{ls} t|_\rho$ corresponds to verifying $s \sim_\rho t$, hence, as a corollary of Theorem 6, it allows also to prove LS-bisimilarity.

Corollary 1. *Given a d-dimensional eLTS $(S, Act, \rightarrow)$ and two states $s, t \in S$, if for any $\rho \in DM_d$ we have $s|_\rho \sim_{ls} t|_\rho$, then $s \sim_{ls} t$.*

Proof sketch. We show that if $s|_\rho \sim_{ls} t|_\rho$, then s and t are ρ-bisimilar, thus allowing us to apply Theorem 6. □

Example 8. *Consider the eLTS of Figure 3, where $s|_\rho$ is the partial evaluation of s with $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$.*

3.3.2 Operators on Distributions. We now discuss how effect distributions can be composed, extending the usual definitions for probabilistic systems. We present a pair of no-go theorems that distinguishes the quantum case from the classical probabilistic one. Common simplifications and extensions that can be safely applied for probabilistic systems make no sense or impact the expressivity when modelling quantum systems.

A corollary of Theorem 3 is that it is possible with n-ary composition to define eLTSs with states for which no bisimilar state can

be defined using the binary operator $\oplus$ only. Roughly, this means that the lack of expressivity of $\oplus$ is not only syntactical.

Corollary 2. *There exists $S_1, Act, s_1 \in S_1$, and $\rightarrow_1 \in S_1 \times Act \times \mathcal{Q}_d S_1$ such that $s_1 \not\sim_{ls} s_2$ in all the eLTSs $(S_1 \cup S_2, Act, \rightarrow_1 \cup \rightarrow_2)$ with S_2 disjoint from S_1, and $\rightarrow_2 \in S_2 \times Act \times \mathcal{Q}_d^{\oplus} S_2$.*

Proof sketch. We give an example of a state that evolves in a distribution $\mathfrak{D} \notin \mathcal{Q}_d^{\oplus} S_1$. Then it is shown that it is not possible to build $\mathfrak{T} \in \mathcal{Q}_d^{\oplus} S_1$ associating the needed effects to equivalence classes without violating Theorem 3. □

Our last remark is about non-deterministic composition of effect distributions. It may be desirable to extend the notion of non-deterministic sum of Definition 11 to effect distributions as it is commonly done for probabilistic distributions [18]. The semantic of a non-deterministic sum of probability distributions $\Delta + \Theta$ is usually defined as

$$(\Delta + \Theta)(s) = \begin{cases} \Delta(s_1) \cdot \Theta(s_2) & \text{if } s = s_1 + s_2 \\ 0 & \text{otherwise} \end{cases}$$

Given the interpretation of effect distributions as parameterized probability distributions, we can lift the previous definition to the quantum case.

Definition 15. *Given a pair of d-dimensional effect distributions $\mathfrak{D}, \mathfrak{T}$ over S, a distribution $\mathfrak{D} + \mathfrak{T}$ is a non-deterministic sum of $\mathfrak{D}$ and $\mathfrak{T}$ if for any density operator $\rho \in DM_d$,*

$$(\mathfrak{D} + \mathfrak{T})\downarrow_\rho (s) = \begin{cases} \mathfrak{D}\downarrow_\rho (s_1) \cdot \mathfrak{T}\downarrow_\rho (s_2) & \text{if } s = s_1 + s_2 \\ 0 & \text{otherwise} \end{cases}$$

Example 9. *Consider the following distributions*

$$\mathfrak{D} = \{s_1 \triangleright |0\rangle\langle 0|, s_2 \triangleright |1\rangle\langle 1|\} \text{ and } \mathfrak{T} = \{s_3 \triangleright \frac{1}{2}\mathbb{I}, s_4 \triangleright \frac{1}{2}\mathbb{I}\}$$

The non-deterministic sum $\mathfrak{D} + \mathfrak{T}$ is then

$$\mathfrak{D} + \mathfrak{T} = \{s_1 + s_3 \triangleright \frac{1}{2}|0\rangle\langle 0|, s_1 + s_4 \triangleright \frac{1}{2}|0\rangle\langle 0|, s_2 + s_3 \triangleright \frac{1}{2}|1\rangle\langle 1|, s_2 + s_4 \triangleright \frac{1}{2}|1\rangle\langle 1|\}$$

In this example the effect distribution $\mathfrak{D}$ is non-deterministically composed with a rather "probability-like" distribution $\mathfrak{T}$, being $tr(\frac{1}{2}\mathbb{I} \cdot \rho) = \frac{1}{2}$ for any ρ. Indeed, the non-deterministic composition of effect distributions is not defined in general. More in details, it is undefined between "purely quantum" effects.

Theorem 10. *If the dimension of the Hilbert space is two or greater, then $\mathfrak{D} + \mathfrak{T}$ is undefined if $\mathfrak{D}(s) = |\psi\rangle\langle\psi|$ and $\mathfrak{T}(t) = |\phi\rangle\langle\phi|$ for some states $s, t \in S$ and quantum states $|\psi\rangle$ and $|\phi\rangle$.*

Proof sketch. We exploit the fact that $|\psi\rangle$ has at least an orthogonal vector $|a\rangle$ if the dimension is at least two. We show that the convexity of $E = (\mathfrak{D} + \mathfrak{T})(s + t)$ leads to contradiction, requiring $tr(E \cdot |a\rangle\langle a|)$ to be negative. □

This is a quite severe limitation for non-deterministic sum of effect distributions.

Example 10. *Let $\mathfrak{D} = \{s_1 \triangleright |0\rangle\langle 0|, s_2 \triangleright |1\rangle\langle 1|\}$ and $\mathfrak{T} = \{s_3 \triangleright |+\rangle\langle +|, s_4 \triangleright |-\rangle\langle -|\}$. There is no effect distribution that is a non-deterministic sum for $\mathfrak{D} + \mathfrak{D}$, $\mathfrak{D} + \mathfrak{T}$ or $\mathfrak{T} + \mathfrak{T}$.*

The results above give suggestions and limitations for the definition of a process algebra for quantum processes: two proposals are given in the following section.

4 MODELLING PROCESSES WITH eLTSs

In this section, we explore the design of a process algebra evaluated over eLTSs. More in details, we enrich our algebra with a pair of different semantics: the stateful Schrödinger-style one is a fairly standard pLTS semantics for a quantum process algebra, and it assumes a given quantum input; the stateless Heisenberg-style instead returns a unique eLTS that is parametric with respect to the input quantum state. We prove that the two coincide, also when unitary transformations are considered, paving the way for automatic verification using standard techniques [21].

4.1 A Minimal Quantum Process Algebra

We will follow the tradition of using CCS-style process calculi to describe LTSs. The minimal quantum process algebra (mQPA) features a parallel operator, a non-deterministic choice operator and destructive measurements. An mQPA process P is defined as

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

where $\mu \in Act$ is an action and $\{P_i \triangleright E_i\}_{i \in I}$ is a full effect distribution over mQPA processes. Intuitively, an *atomic* process s controls the behaviour of the quantum system, while P represents an effect distribution of atomic processes. Note that we use n-ary composition of effects, as a binary operator would have been less expressive, and that we do not consider ill-defined non-deterministic sum over general processes (Theorem 10). In the following, we sometimes write μ for the process $\mu.\mathbf{0}$.

In order to simplify the definition of the semantics of mQPA, we define a syntactic flattening operation, translating sequences of syntactic effect distributions (i.e. destructive measurements) into a single effect distribution.

Definition 16. *The flattening operator* $\mathrm{flat}(\cdot)$ *on mQPA processes is described by the following inductive rules*

$$\frac{}{\mathrm{flat}(s) = ([1]s)} \qquad \frac{\mathrm{flat}(P_i) = ([E_{ij}]s_{ij})_{j \in J_i}}{\mathrm{flat}([E_i]P_i)_{i \in I} = ([E_i \otimes E_{ij}]s_{ij})_{i \in I, j \in J_i}}$$

Note that a mQPA process needs a Hilbert space of a given dimension from which the input quantum states are taken. We define the operator dim, returning the required Hilbert space dimension. Roughly, this is the maximum number of qubits needed by any branch of the process to perform its measurements.

Definition 17. *The minimum dimension for a mQPA process P is called* $\dim(P)$*, where*

$$\dim(\mathbf{0}) = 1 \qquad \dim(\mu.P) = \dim(P)$$
$$\dim(s + t) = \max\{\dim(s), \dim(t)\} \qquad \dim(s \parallel t) = \dim(s) \cdot \dim(t)$$
$$\dim(([E_i]P_i)_{i \in I}) = \max\{\dim(E_i) \cdot \dim(P_i)\}_{i \in I}$$

Finally, we define an operator that lifts an effect to a larger Hilbert space with the identity effect

$$\frac{\mathrm{flat}(s) = ([E_i]s_i)_{i\in I}}{\langle \rho, \mu.s\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\rho), s_i\rangle \rhd \mathrm{tr}(\mathcal{M}_{E_i}(\rho))\}_{i\in I}}\ \textsc{SPre}$$

$$\frac{\langle \rho, s\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \rho, s+t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{SSumL} \qquad \frac{\langle \rho, t\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \rho, s+t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{SSumR}$$

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

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

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

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

(a) Rules for Schrödinger-style stateful semantics

$$\frac{\mathrm{flat}(s) = ([E_i]s_i)_{i\in I}}{\langle 1, \mu.s\rangle \xrightarrow{\mu} \{\langle E_i, s_i\rangle \rhd \mathrm{pad}_D(E_i)\}_{i\in I}}\ \textsc{HPre}$$

$$\frac{\langle 1, s\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle 1, s+t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{HSumL} \qquad \frac{\langle 1, t\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle 1, s+t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{HSumR}$$

$$\frac{\langle 1, s\rangle \xrightarrow{\mu} \{\langle E_i, s_i\rangle \rhd \mathrm{pad}_D(E_i)\}_{i\in I}}{\langle 1, s \parallel t\rangle \xrightarrow{\mu} \{\langle E_i, s_i \parallel t\rangle \rhd \mathrm{pad}_D(E_i)\}_{i\in I}}\ \textsc{HParL}$$

$$\frac{\langle 1, t\rangle \xrightarrow{\mu} \{\langle E_j, t_j\rangle \rhd \mathrm{pad}_D(E_j)\}_{j\in J}}{\langle 1, s \parallel t\rangle \xrightarrow{\mu} \{\langle E_j, s \parallel t_j\rangle \rhd \mathrm{pad}_D(E_j)\}_{j\in J}}\ \textsc{HParR}$$

$$\frac{\langle 1, s\rangle \xrightarrow{\mu} \{\langle E_i, s_i\rangle \rhd \mathrm{pad}_D(E_i)\}_{i\in I} \quad \langle 1, t\rangle \xrightarrow{\overline{\mu}} \{\langle E_j, t_j\rangle \rhd \mathrm{pad}_D(E_j)\}_{j\in J}}{\langle 1, s \parallel t\rangle \xrightarrow{\tau} \{\langle E_i \otimes E_j, s_i \parallel t_j\rangle \rhd \mathrm{pad}_D(E_i \otimes E_j)\}_{(i,j)\in I\times J}}\ \textsc{HSyncL}$$

$$\frac{\langle 1, s\rangle \xrightarrow{\mu} \{\langle E_i, s_i\rangle \rhd \mathrm{pad}_D(E_i)\}_{i\in I} \quad \langle 1, t\rangle \xrightarrow{\overline{\mu}} \{\langle E_j, t_j\rangle \rhd \mathrm{pad}_D(E_j)\}_{j\in J}}{\langle 1, s \parallel t\rangle \xrightarrow{\tau} \{\langle E_j \otimes E_i, s_i \parallel t_j\rangle \rhd \mathrm{pad}_D(E_j \otimes E_i)\}_{(i,j)\in I\times J}}\ \textsc{HSyncR}$$

$$\frac{\langle 1, s\rangle \xrightarrow{\mu} \{\langle E_i, s_i\rangle \rhd E_i\}_{i\in I}}{\langle E, s\rangle \xrightarrow{\mu} \{\langle E \otimes E_i, s_i\rangle \rhd \mathrm{pad}_D(E \otimes E_i)\}_{i\in I}}\ \textsc{HLift}$$

(b) Rules for Heisenberg-style stateless semantics

Figure 4: Stateful and stateless semantics for mQPA processes

Definition 18. *The padding operator that lifts an effect to a larger Hilbert space of dimension D is called* $\mathrm{pad}_D(\cdot)$

$$\mathrm{pad}_D : \bigcup_{d\le D} \mathcal{E}f_d \to \mathcal{E}f_D$$
$$\mathrm{pad}_D(E) = E \otimes \mathbb{I}_{D-d}$$

4.2 Schrödinger approach

A natural, stateful semantics for an atomic mQPA process s is given in terms of a pLTS, where each state is a pair of a density operator and an atomic process. The pLTS is rooted in the pair $\langle \rho, s\rangle$, where $\rho \in DM_{\dim(s)}$. All the successor states have some subterm s' of s, and some possibly smaller state $\rho' \in pDM_d$ with $d \le \dim(s)$, because of destructive measurements. The transition relation is the smallest relation satisfying the rules in Figure 4a. In the SPre rule the quantum state is updated with the destructive measurement operator $\mathcal{M}_{E_i}(\rho)$ associated to the effect E_i in the process. Note that the resulting effect distribution is always a probability distribution, obtained by tracing the measured density operator. As a result of that, the eLTS is a pLTS, as expected when the quantum input is fully instantiated. 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. A trivial consequence of the rules is that all the distributions in the right-hand side of $\to$ are of the form $\{\langle \rho_i, s_i\rangle \rhd \mathrm{tr}(\rho_i)\}_{i\in I}$.

Example 11. *Consider a process P that first performs a one-qubit measurement in the computational basis and then measure another qubit in the Hadamard basis*

$$P = \tau.([|0\rangle\langle 0|]Q, [|1\rangle\langle 1|]R), \text{ with}$$
$$Q = \tau.([|+\rangle\langle +|]\alpha, [|-\rangle\langle -|]\beta) \text{ and } R = \tau.([|+\rangle\langle +|]\gamma, [|-\rangle\langle -|]\delta).$$

The stateful semantics of $\langle |\Phi^+\rangle\langle\Phi^+|, P\rangle$ is given in Figure 5a. Note that measurements are destructive and do not cause a τ-transition (contrary of other approaches [6, 8]) and thus after the measurement the distribution is $\{\langle |0\rangle\langle 0|, Q\rangle \rhd \frac{1}{2}, \langle |1\rangle\langle 1|, R\rangle \rhd \frac{1}{2}\}$ and not $\{\langle |00\rangle\langle 00|, Q\rangle \rhd \frac{1}{2}, \langle |11\rangle\langle 11|, R\rangle \rhd \frac{1}{2}\}$.

4.3 Heisenberg approach

For any given atomic process s, the stateful semantics results in infinitely many distinct pLTSs according to the input quantum state ρ. We seek an alternative stateless characterization, adequate for algorithmic verification. We therefore give a new semantics for mQPA processes whose states are pairs of effects E and atomic processes s. For each D-dimensional atomic process s we build a D-dimensional eLTS rooted in $\langle 1, s\rangle$, where 1 is the unit 1-dimensional effect. The transition relation is defined as the smallest relation satisfying the rules in Figure 4b. Note that, while in the Schrödinger semantics s is paired with the remaining part of the input quantum state, in this new *Heisenberg semantics*, s is paired with an effect describing the measurements done so far. The HPre rule simply records the effect that must be observed in order to reach the paired mQPA state. As in the stateful semantics, HSyncL and HSyncR differ only in the application order of the measurements. Note that we are dealing with destructive measurements, while in general eLTS allows applying different effects on the same qubit over and over. This is forbidden

in mQPA, where consecutive measurements act on different qubits, and thus must be scaled up via tensor product. Storing the effects along the mQPA processes is needed for constraining subsequent distributions to be consistent with the previously measured qubits, which allows for correctly dealing with entangled inputs.

Example 12. *Consider the process P of Example 11. Figure 5c shows its stateless semantics, instantiated in Figure 5b with $|\Phi^+\rangle\langle\Phi^+|$ by the quantum partial evaluation operator on eLTSs of Definition 14. As expected, the evaluated eLTS is indistinguishable from the pLTS of the stateful semantics in Figure 5a.*

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 stateless semantics have exactly the same transitions of the stateful semantics, thus they are bisimilar.

Theorem 11. *For any atomic state s and $\rho \in DM_{\dim(s)}$*

$$\langle 1, s\rangle\big|_\rho \sim_{ls} \langle \rho, s\rangle$$

Proof sketch. Take the relation

$$\mathcal{R} = \left\{ \left(\langle E, s\rangle\big|_\rho, \langle \mathcal{M}_E(\rho), s\rangle \right) \,\middle|\, \rho \in DM_d, E \in \mathcal{E}f_{d'}, d \geq d' \cdot \dim(s) \right\}$$

The result follows from the inductively demonstrable lemma

$$\langle E, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd p_i\} \text{ iff } \langle \mathcal{M}_E(\rho), s\rangle \xrightarrow{\mu} \{\mathcal{M}_{E_i}(\rho) \rhd p_i\} \quad \square$$

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

Theorem 12. *Given two d-dimensional atomic processes s and t, $\langle 1, s\rangle \sim_{ls} \langle 1, t\rangle$ if and only if for any $\rho \in DM_d$, $\langle \rho, s\rangle \sim_{ls} \langle \rho, t\rangle$.*

Proof. We can prove by Theorem 9 and Corollary 1 that the hypothesis is equivalent to $\langle 1, s\rangle\big|_\rho \sim_{ls} \langle 1, t\rangle\big|_\rho$. Then we can apply the duality result of Theorem 11, thus getting $\langle \rho, s\rangle \sim_{ls} \langle \rho, t\rangle$. $\square$

4.4 Unitary extension

Our proposed eLTSs are sufficiently expressive to model also languages with unitaries. As before, we will define both a stateful and a stateless semantics. The syntax of mQPA processes is extended with unitary transformations. As for measurement, unitaries are not observable actions.

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

We extend the dimension operator imposing that $\dim(U; P) = \max\{d, \dim(P)\}$ when U is a d-dimensional matrix. To give the semantics of a D-dimensional atomic process s, we update the flattening function with a rule for unitaries. Note that, instead of effects, it returns processes guarded by D-dimensional superoperators.

$$\frac{}{\text{flat}(s) = ([\mathcal{I}_D]s)} \qquad \frac{\text{flat}(P_i) = ([\mathcal{E}_{ij}]s_{ij})_{j\in J}}{\text{flat}([E_i]P_i)_{i\in I} = ([\mathcal{E}_{ij} \circ \mathcal{M}_{E_i}]s_{ij})_{(i,j)\in I\times J}}$$
$$\frac{\text{flat}(P) = ([\mathcal{E}_i]s_i)_{i\in I}}{\text{flat}(U; P) = ([\mathcal{E}_i \circ \mathcal{E}_U]s_i)_{i\in I}}$$

where $\mathcal{E}_U(\rho) = U\rho U^\dagger$ is the superoperator corresponding to the unitary U, $\mathcal{I}_d$ is the identity superoperator of dimension d and $\mathcal{E} \circ \mathcal{F}$ is the composition on superoperators where $\mathcal{F}$ is tensored with identity operators in order to reach the same dimension of $\mathcal{E}$, e.g. $(\mathcal{E}_{CNOT} \circ \mathcal{E}_H(\rho)) = CNOT(H \otimes \mathbb{I})\rho(H \otimes \mathbb{I})CNOT$.

The Schrödinger-style semantics is defined over the same configurations as before. The transition relation is the smallest relation satisfying the previous rules with the following updated SPre

$$\frac{\text{flat}(s) = ([\mathcal{E}_i]s_i)_{i\in I}}{\langle \rho, \mu.s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}(\rho), s_i\rangle \rhd \text{tr}(\mathcal{E}_i(\rho))\}_{i\in I}} \text{ SPre}$$

The Heisenberg-style semantics of an atomic D-dimensional process is defined as a D-dimensional eLTS made of pairs $\langle \mathcal{E}, s\rangle$, where the superoperator $\mathcal{E}$ represents at the same time measurements and unitaries. The transition relation is the smallest relation satisfying the rules in Figure 6, where $E_{\mathcal{E}}$ is the effect associated with the superoperator $\mathcal{E}$.

Note that, while the states of the transition system contain superoperators, the resulting semantics is still an eLTS. On the one hand, indeed, superoperators are only required for describing how the quantum input evolves upon unitaries and measurements, while the visible, probabilistic behaviour is still encoded as effect distributions. On the other hand, effects in mQPA processes represent destructive measurements, therefore they can be represented as superoperators and composed with the unitary transformations.

As before, we formalize the connection between the two semantics in terms of bisimulations.

Theorem 13. *For any d-dimensional atomic process s and any $\rho \in DM_d$, $\langle \mathcal{I}_d, s\rangle|_\rho \sim_{ls} \langle \rho, s\rangle$.*

Proof sketch. Take the relation

$$\mathcal{R} = \left\{ \left(\langle \mathcal{E}, s\rangle\big|_\rho, \langle \mathcal{E}(\rho), s\rangle \right) \mid \rho \in DM_d, \mathcal{E} \in \mathcal{SO}_d \right\}$$

The results follow trivially from the inductively demonstrable lemma

$$\langle \mathcal{E}, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd p_i\} \Leftrightarrow \langle \mathcal{E}(\rho), s\rangle \xrightarrow{\mu} \{\mathcal{E}_i(\rho) \rhd p_i\} \quad \square$$

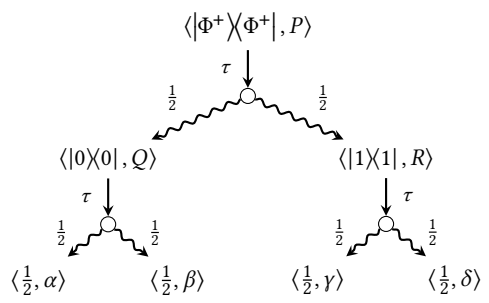
Thus, we can restate Theorem 12 for our extension of mQPA.

Theorem 14. *Given two d-dimensional atomic processes s and t, $\langle \mathcal{I}_d, s\rangle \sim_{ls} \langle \mathcal{I}_d, s\rangle$ if and only if for any $\rho \in DM_d$, $\langle \rho, s\rangle \sim_{ls} \langle \rho, t\rangle$.*

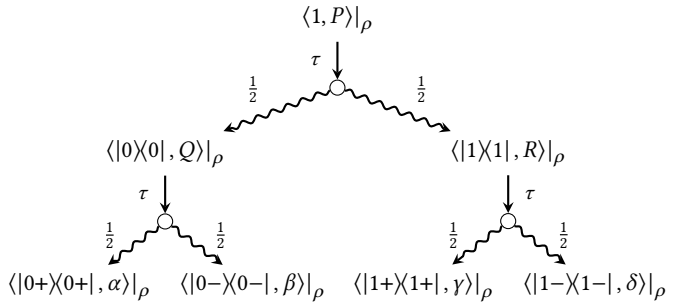
Proof. As for Theorem 12, but using the duality that is described in Theorem 13. $\square$

5 RELATED WORKS

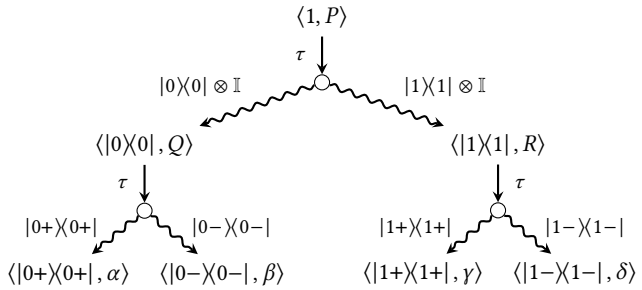
In our work we follow a foundational approach to quantum bisimilarity, extending what is done by [18] for probabilistic bisimilarity. We employ effect distributions (i.e. finite non-normalized POVMs) as a generalization of sub-probability distributions, finding them particularly well suited to model 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 [20]. More in depth, the author in [20] 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 instead apply



(a) Schrödinger-style semantics of P with $\rho = |\Phi^+\rangle\langle\Phi^+|$



(b) Heisenberg-style semantics of $P|_\rho$ with $\rho = |\Phi^+\rangle\langle\Phi^+|$



(c) Heisenberg-style semantics of P

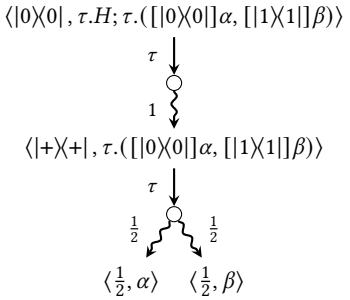
Figure 5: Semantics eLTSs for the process $P = \tau.([|0\rangle\langle 0|]Q, [|1\rangle\langle 1|]R)$ with $Q = \tau.([|+\rangle\langle +|]\alpha, [|-\rangle\langle -|]\beta)$ and $R = \tau.([|+\rangle\langle +|]\gamma, [|-\rangle\langle -|]\delta)$.

$$\frac{\langle \mathcal{I}, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle \rhd E_{\mathcal{E}_i}\}_{i\in I}}{\langle \mathcal{E}, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i \circ \mathcal{E}, s_i\rangle \rhd E_{\mathcal{E}_i\circ\mathcal{E}}\}_{i\in I}}\ \textsc{HLift} \qquad \frac{\mathrm{flat}(s) = ([\mathcal{E}_i]s_i)_{i\in I}}{\langle \mathcal{I}, \mu.P\rangle \xrightarrow{\mu} \{\langle \mathcal{E}, s_i\rangle \rhd E_{\mathcal{E}}\}_{i\in I}}\ \textsc{HPre} \qquad \frac{\langle \mathcal{I}, s\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \mathcal{I}, s+t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{HSumL} \qquad \frac{\langle \mathcal{I}, t\rangle \xrightarrow{\mu} \mathfrak{D}}{\langle \mathcal{I}, s+t\rangle \xrightarrow{\mu} \mathfrak{D}}\ \textsc{HSumR}$$

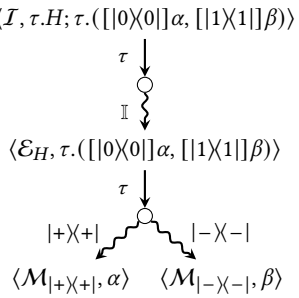
$$\frac{\langle \mathcal{I}, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle \rhd E_{\mathcal{E}_i}\}_{i\in I}}{\langle \mathcal{I}, s \parallel t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i \parallel t\rangle \rhd E_{\mathcal{E}_i}\}_{i\in I}}\ \textsc{HParL} \qquad \frac{\langle \mathcal{I}, t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_j, t_j\rangle \rhd E_{\mathcal{E}_j}\}_{j\in J}}{\langle \mathcal{I}, s \parallel t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_j, s \parallel t_j\rangle \rhd E_{\mathcal{E}_j}\}_{j\in J}}\ \textsc{HParR}$$

$$\frac{\langle \mathcal{I}, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle \rhd E_{\mathcal{E}_i}\}_{i\in I} \quad \langle \mathcal{I}, t\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_j, t_j\rangle \rhd E_{\mathcal{E}_j}\}_{j\in J}}{\langle \mathcal{I}, s \parallel t\rangle \xrightarrow{\tau} \{\langle \mathcal{E}_j \circ \mathcal{E}_i, s_i \parallel t_j\rangle \rhd E_{\mathcal{E}_j\circ\mathcal{E}_i}\}_{(i,j)\in I\times J}}\ \textsc{HSyncL} \qquad \frac{\langle \mathcal{I}, t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i, t_i\rangle \rhd E_{\mathcal{E}_i}\}_{i\in I} \quad \langle \mathcal{I}, s\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_j, s_j\rangle \rhd E_{\mathcal{E}_j}\}_{j\in J}}{\langle \mathcal{I}, s \parallel t\rangle \xrightarrow{\tau} \{\langle \mathcal{E}_j \circ \mathcal{E}_i, s_i \parallel t_j\rangle \rhd E_{\mathcal{E}_j\circ\mathcal{E}_i}\}_{(i,j)\in I\times J}}\ \textsc{HSyncR}$$

Figure 6: Heisenberg-style semantics for mQPA processes with unitaries



(a) Example of Schrödinger-style semantics



(b) Example of Heisenberg-style semantics

Figure 7: Example of stateful and stateless semantics for mQPA processes with unitaries

these concepts to quantum protocol semantics, introducing eLTSs and studying their composition and their behavioural equivalences.

Our eLTS can be seen as a labelled, non-deterministic version of the effect-valued Quantum Markov Chain of [15], where tensor products is used instead of sequential effect composition. The most general model of "quantum transition system" is the one of [26, 31], where the weights are superoperators instead of effects, so to capture also non-destructive measurements and qubit initialization. The author of [31] introduces two different notions of bisimilarity, that we recover in our minimal, effect-based setting as AM and LS bisimilarity. However, none of these works feature nondeterminism, nor do they apply the proposed coalgebraic model to process calculi suitable for expressing quantum protocols.

Usually in the literature the semantics of quantum processes is described via pLTSs and probabilistic bisimilarity [6–9, 23]. Despite their differences, these works all define a pLTS made of configurations, i.e. pairs of quantum values and syntactic processes. Bisimilar systems exhibit the same probabilistic behaviour as labels or barbs, and the same observable quantum values inside the configurations. 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 a purely quantum transition system, and we do not manipulate directly quantum values but only their observable probabilistic behaviour in the form of effects. Moreover, to verify the equivalence of two processes the previous proposals have to instantiate them with each possible quantum input, impeding algorithmic verification. Using effects, instead, we can describe the "symbolic" semantics of a protocol, abstracting away from the input, as done in Theorem 12 and Theorem 14.

Most similar to our work is [10], which introduces superoperator-valued quantum distributions, analogous to the ones in [16, 26, 31]. This allows modelling the more expressive non-destructive measurements and quantum communication, but their proposed bisimilarity does not respect the observational properties prescribed by quantum theory [6, 12, 22]. When giving the operational semantics of their language, they employ configurations composed of superoperators and processes, and they build a superoperator-weighted transition system made of such configurations. In subsection 4.4, we use the same kind of configurations, but we propose an effect-weighted transition system. They compare superoperators via pointwise Loewner order, which is equivalent to comparing the superoperators effects as in subsection 4.4.

The bisimilarity proposed in [10] is proven to be equivalent to the one in [9], and it is strictly finer than ours. The authors require bisimilar transition systems to have 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 example, written in mQPA syntax.

Example 13. *Let P and Q be the processes*

$$P = ([|0\rangle\langle 0|]R, [|1\rangle\langle 1|]R') \quad \textit{and} \quad Q = ([|+\rangle\langle +|]R, [|-\rangle\langle -|]R')$$

where R and R' are two deadlock processes which maintain the ownership of the measured qubit (recall that [10] 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 [9, 10], as can be seen studying the ground behaviour of $\langle \Phi^+, P\rangle$ and $\langle \Phi^+, Q\rangle$.

The two processes above are instead considered bisimilar in our proposals, as well as in other more recent works [6, 8, 22]. The bisimilarity of [9] has been relaxed in subsequent works [8, 12], but no symbolic version of this coarser bisimilarity has been proposed.

6 CONCLUSIONS

We provided a purely quantum-based semantics of quantum protocols and proved its correctness with respect to the observable probabilistic behaviour prescribed by quantum theory. The advantages of using LS-bisimilarity and eLTSs is that it provides a symbolic and algorithmically verifiable semantic equivalence. To assess two processes probabilistically, their behaviour must be compared on every possible quantum state, thus considering a continuously infinite set of cases. This is the standard approach in the quantum process calculi literature [5–9, 23]. Our eLTSs instead allow the description of quantum systems in general, implicitly parameterising them with respect to the initial quantum state and thus permitting algorithmic verification. Indeed, eLTSs can be easily defined in a coalgebraic fashion, allowing e.g. to resort to the general algorithm for partition refinement of [21] for proving LS-bisimilarity.

Future work. We proved that non-deterministic sum and parallel composition of eLTSs preserves bisimilarity. As a future work, we will address the same problem over all mQPA operators, thus investigating whether our bisimilarity is a congruence. We assessed our approach in a minimal setting, i.e. only considering destructive measurements, unitaries and non-determinism. We plan to include recursively defined processes and quantum value passing, i.e. allowing processes to exchange qubits, as in [10], and we will investigate the extension of our results in this framework.

REFERENCES

[1] Samson Abramsky, Rui Soares Barbosa, Nadish de Silva, and Octavio Zapata. 2017. The Quantum Monad on Relational Structures. (2017), 19 pages. https://doi.org/10.4230/LIPIcs.MFCS.2017.35 arXiv:1705.07310 [quant-ph]

[2] Charles H. Bennett and Gilles Brassard. 2014. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theoretical Computer Science* 560 (Dec. 2014), 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

[3] Filippo Bonchi, Alexandra Silva, and Ana Sokolova. 2017. The Power of Convex Algebras. In *28th International Conference on Concurrency Theory (CONCUR 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

[4] Marcello Caleffi, Angela Sara Cacciapuoti, and Giuseppe Bianchi. 2018. Quantum Internet: From Communication to Distributed Computing!. In *Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication*. ACM, Reykjavik Iceland, 1–4. https://doi.org/10.1145/3233188.3233224

[5] Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. 2023. Quantum Bisimilarity via Barbs and Contexts: Curbing the Power of Non-Deterministic Observers (Extended Version). *CoRR* abs/2311.06116 (2023). https://doi.org/10.48550/ARXIV.2311.06116 arXiv:2311.06116

[6] Lorenzo Ceragioli, Fabio Gadducci, Giuseppe Lomurno, and Gabriele Tedeschi. 2024. Quantum Bisimilarity via Barbs and Contexts: Curbing the Power of Non-deterministic Observers. *Proc. ACM Program. Lang.* 8, POPL (Jan. 2024), 43:1269–43:1297. https://doi.org/10.1145/3632885

[7] Timothy AS Davidson. 2012. *Formal Verification Techniques Using Quantum Process Calculus*. Ph. D. Dissertation. University of Warwick.

[8] Yuxin Deng. 2018. Bisimulations for Probabilistic and Quantum Processes (Invited Paper). In *29th International Conference on Concurrency Theory (CONCUR 2018) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 118)*, Sven Schewe and Lijun Zhang (Eds.). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2:1–2:14. https://doi.org/10.4230/LIPIcs.CONCUR.2018.2

[9] Yuxin Deng and Yuan Feng. 2012. Open Bisimulation for Quantum Processes. In *Theoretical Computer Science (Lecture Notes in Computer Science)*, Jos C. M.

Baeten, Tom Ball, and Frank S. de Boer (Eds.). Springer, Berlin, Heidelberg, 119–133. https://doi.org/10.1007/978-3-642-33475-7_9

[10] Yuan Feng, Yuxin Deng, and Mingsheng Ying. 2014. Symbolic Bisimulation for Quantum Processes. *ACM Trans. Comput. Logic* 15, 2 (May 2014), 14:1–14:32. https://doi.org/10.1145/2579818

[11] Yuan Feng, Runyao Duan, and Mingsheng Ying. 2012. Bisimulation for Quantum Processes. *ACM Trans. Program. Lang. Syst.* 34, 4 (Dec. 2012), 17:1–17:43. https://doi.org/10.1145/2400676.2400680

[12] Yuan Feng and Mingsheng Ying. 2015. Toward Automatic Verification of Quantum Cryptographic Protocols. In *26th International Conference on Concurrency Theory (CONCUR 2015) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 42)*, Luca Aceto and David de Frutos Escrig (Eds.). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 441–455. https://doi.org/10.4230/LIPIcs.CONCUR.2015.441

[13] Fei Gao, SuJuan Qin, Wei Huang, and QiaoYan Wen. 2019. Quantum Private Query: A New Kind of Practical Quantum Cryptographic Protocol. *Sci. China Phys. Mech. Astron.* 62, 7 (Jan. 2019), 70301. https://doi.org/10.1007/s11433-018-9324-6

[14] Simon J. Gay and Rajagopal Nagarajan. 2005. Communicating Quantum Processes. In *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '05)*. Association for Computing Machinery, New York, NY, USA, 145–157. https://doi.org/10.1145/1040305.1040318

[15] Stanley Gudder. 2008. Quantum Markov Chains. *J. Math. Phys.* 49, 7 (July 2008), 072105. https://doi.org/10.1063/1.2953952

[16] Ichiro Hasuo and Naohiko Hoshino. 2011. Semantics of Higher-Order Quantum Computation via Geometry of Interaction. In *2011 IEEE 26th Annual Symposium on Logic in Computer Science*. 237–246. https://doi.org/10.1109/LICS.2011.26

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

[18] Matthew Hennessy. 2012. Exploring Probabilistic Bisimulations, Part I. *Form. Asp. Comput.* 24, 4-6 (July 2012), 749–768. https://doi.org/10.1007/s00165-012-0242-7

[19] M Hennessy and H Lin. 1995. Symbolic Bisimulations. *Theoretical Computer Science* 138, 2 (Feb. 1995), 353–389. https://doi.org/10.1016/0304-3975(94)00172-F

[20] Bart Jacobs. 2011. Probabilities, Distribution Monads, and Convex Categories. *Theoretical Computer Science* 412, 28 (June 2011), 3323–3336. https://doi.org/10.1016/j.tcs.2011.04.005

[21] Jules Jacobs and Thorsten Wißmann. 2023. Fast Coalgebraic Bisimilarity Minimization. *Proc. ACM Program. Lang.* 7, POPL (Jan. 2023), 52:1514–52:1541. https://doi.org/10.1145/3571245

[22] Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano, and Hideki Sakurada. 2012. Application of a Process Calculus to Security Proofs of Quantum Protocols. In *Proceedings of the International Conference on Foundations of Computer Science (FCS)*. The Steering Committee of The World Congress in Computer Science, Computer . . . , 1.

[23] Marie Lalire. 2006. Relations among Quantum Processes: Bisimilarity and Congruence. arXiv:quant-ph/0603274

[24] Marie Lalire and Philippe Jorrand. 2004. A Process Algebraic Approach to Concurrent and Distributed Quantum Computation: Operational Semantics. arXiv:quant-ph/0407005

[25] Kim G. Larsen and Arne Skou. 1991. Bisimulation through Probabilistic Testing. *Information and Computation* 94, 1 (Sept. 1991), 1–28. https://doi.org/10.1016/0890-5401(91)90030-6

[26] Ai Liu and Meng Sun. 2019. A Coalgebraic Semantics Framework for Quantum Systems. In *Formal Methods and Software Engineering (Lecture Notes in Computer Science)*, Yamine Ait-Ameur and Shengchao Qin (Eds.). Springer International Publishing, Cham, 387–402. https://doi.org/10.1007/978-3-030-32409-4_24

[27] Gui-lu Long, Fu-guo Deng, Chuan Wang, Xi-han Li, Kai Wen, and Wan-ying Wang. 2007. Quantum Secure Direct Communication and Deterministic Secure Quantum Communication. *Front. Phys. China* 2, 3 (July 2007), 251–272. https://doi.org/10.1007/s11467-007-0050-3

[28] Dominic Mayers. 2001. Unconditional Security in Quantum Cryptography. *J. ACM* 48, 3 (May 2001), 351–406. https://doi.org/10.1145/382780.382781

[29] Michael A. Nielsen and Isaac L. Chuang. 2010. *Quantum Computation and Quantum Information* (10th anniversary ed ed.). Cambridge University Press, Cambridge ; New York.

[30] Ali Ibnun Nurhadi and Nana Rachmana Syambas. 2018. Quantum Key Distribution (QKD) Protocols: A Survey. In *2018 4th International Conference on Wireless and Telematics (ICWT)*. 1–5. https://doi.org/10.1109/ICWT.2018.8527822

[31] Hiroshi Ogawa. 2014. Coalgebraic Approach to Equivalences of Quantum Systems. *Master's thesis, University of Tokyo* (2014).

[32] Sam Staton. 2011. Relating Coalgebraic Notions of Bisimulation. *Logical Methods in Computer Science* 7 (2011).

[33] Yong Wang. 2019. Probabilistic Process Algebra to Unifying Quantum and Classical Computing in Closed Systems. *Int J Theor Phys* 58, 10 (Oct. 2019), 3436–3509. https://doi.org/10.1007/s10773-019-04216-2

[34] Peiying Zhang, Ning Chen, Shigen Shen, Shui Yu, Sheng Wu, and Neeraj Kumar. 2022. Future Quantum Communications and Networking: A Review and Vision. *IEEE Wireless Commun.* (2022), 1–8. https://doi.org/10.1109/MWC.012.2200295

A PROOFS

We list some known facts about effects that directly comes from linear algebra.

Proposition 1. *Given two effects E_1 and E_2, if $E_1 + E_2 = |\psi\rangle\langle\psi|$ then $E_i = p_i\,|\psi\rangle\langle\psi|$ for some P_i, $i = 1, 2$.*

Proposition 2. *Given two effects E_1 and E_2, if $E_1 \,{}_p\!\oplus\, E_2 = |\psi\rangle\langle\psi|$ then $E_i = |\psi\rangle\langle\psi|$ for $i = 1, 2$.*

Theorem 2. *Effect distributions correspond to all and only the parameterized sub-probability distributions that are convex and have an "overall" finite support.*

$$\mathcal{Q}_d \cong \left\{ \mathfrak{D}{\downarrow_\_} \in (\mathcal{D}(X))^{DM_d} \;\middle|\; \begin{array}{l} \mathfrak{D}{\downarrow_{\rho \,{}_p\!\oplus\, \sigma}} = (\mathfrak{D}{\downarrow_\rho}) \,{}_p\!\oplus\, (\mathfrak{D}{\downarrow_\sigma}) \\ \bigcup_{\rho \in DM_d} \mathrm{supp}(\mathfrak{D}{\downarrow_\rho}) \text{ is finite} \end{array} \right\}$$

Proof. Recall that $(\mathcal{E}f_d, 0_d, +)$ forms a Partial Commutative Monoid (PCM), i.e. an algebraic structure where the sum between two elements is not always defined. Each PCM has a partial order, defined as $a \preceq b$ if and only if $\exists c. a + c = b$. In the case of $\mathcal{E}f_d$, two effects can be summed if and only if their sum is smaller or equal to I_d in the l owner order, and the resulting partial order $\preceq$ is exactly $\sqsubseteq$. We employ a known result in quantum theory [17], specifying that the set of effects $\mathcal{E}f_d$ is isomorphic to $\mathbf{Conv}(DM_d, [0, 1])$, the set of convex maps from DM_d to the real interval $[0, 1]$. 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 $\mathcal{E}f_d$ 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. Now, we will prove that the set above is isomorphic to

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

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

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

For the finite support, we have that

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

For the sum over the support, we have that

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

□

Lemma 1. *Let $\mathcal{R} \subseteq X \times X$. Then $\mathfrak{D} \,\overset{\square}{\mathcal{R}}_d\, \mathfrak{T}$ if and only if there is a finite index set I and an effect set $E_i \in \mathcal{E}f_d$ such that*

1. $\mathfrak{D} = \{x_i \triangleright E_i\}_{i \in I}$
2. $\mathfrak{T} = \{y_i \triangleright E_i\}_{i \in I}$
3. $x_i \,\mathcal{R}\, y_i$ *for each* $i \in I$

Proof. ($\Leftarrow$) Suppose there is a finite index set I such that (1) $\mathfrak{D} = \{s_i \triangleright E_i\}_{i \in I}$, (2) $\mathfrak{T} = \{t_i \triangleright E_i\}_{i \in I}$ and (3) $s_i \,\mathcal{R}\, t_i$ for each $i \in I$. By (3) and by definition, it follows that $\overline{s}_i \,\overset{\square}{\mathcal{R}}\, \overline{t}_i$ for each $i \in I$. Then, by Definition 5, $\mathfrak{D} = (\sum_{i \in I} E_i \otimes \overline{s_i}) \,\overset{\square}{\mathcal{R}}_{1 \times d}\, (\sum_{i \in I} E_i \otimes \overline{t_i}) = \mathfrak{T}$.

($\Rightarrow$) By induction on the rules for $\overset{\square}{\mathcal{R}}_d$: For the first rule, assume $s \,\mathcal{R}\, t$ and $\overline{s}\,\mathcal{R}\overline{t}$, then $\overline{s} = \{s \triangleright 1\}$ and $\overline{t} = \{t \triangleright 1\}$. For the second rule, assume $\mathfrak{D}_i \,\mathcal{R} \mathfrak{T}_i$. Then by induction hypothesis, for any $i \in I$, it holds that $\mathfrak{D}_i = \{s_{i,j} \triangleright E_{i,j}\}_{j \in i_i}$ and $\mathfrak{T}_i = \{t_{i,j} \triangleright E_{i,j}\}_{j \in i_i}$, with $s_{i,j} \,\mathcal{R}\, t_{i,j}$. Hence it is true that

$$\sum_{i \in I} E_i \otimes \mathfrak{D}_i = \{s_{i,j} \triangleright E_i \otimes E_{i,j}\}_{i \in I, j \in i_i}$$
$$\sum_{i \in I} E_i \otimes \mathfrak{T}_i = \{t_{i,j} \triangleright E_i \otimes E_{i,j}\}_{i \in I, j \in i_i}$$

And the result follows by definition. □

Lemma 2. *Let $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, the effect $|\Phi^+\rangle\langle\Phi^+|$ cannot be expressed as the tensor product of two-dimensional effects.*

Proof. It is simply not possible to obtain $|\Phi^+\rangle\langle\Phi^+|$ as the tensor product of two $2x2$ matrices. Note that

$$|\Phi^+\rangle\langle\Phi^+| = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Assume $|\Phi^+\rangle\langle\Phi^+| = A \otimes B$. Then $A_{0,0}B_{0,0} = 1$ and $A_{0,1}B_{0,1} = 1$, but since $A_{0,0}B_{0,1} = 0$ then either $A_{0,0} = 0$ or $B_{0,1} = 0$. □

Lemma 3. *Let $\{s_\alpha, s_\beta, s_\gamma, s_\delta\} \subseteq X$, and let $\mathfrak{D}$ be defined as*

$$\mathfrak{D} = \{s_\alpha \rhd \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|, s_\beta \rhd |\Phi^-\rangle\langle\Phi^-|, \\ s_\gamma \rhd \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right|, s_\delta \rhd |\Psi^-\rangle\langle\Psi^-|\},$$

$$\text{where } \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

There is no $\mathfrak{T} \in Q_4^{\oplus} X$ and subsets $X_\alpha, X_\beta, X_\gamma, X_\delta$ of X such that

$$\sum_{x \in X_y} \mathfrak{T}(x) = \mathfrak{D}(s_y) \text{ for } y \in \{\alpha, \beta, \gamma, \delta\}.$$

Proof. We proceed by induction on the number of application of $\oplus$. 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 $\oplus$ n times starting from point distributions, and let $\mathfrak{T} = \mathfrak{T}_1 {}_E\!\oplus \mathfrak{T}_2$. 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 2, 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 $\mathfrak{T}_1$ and $\mathfrak{T}_2$ also must be of dimension 2, and it must be that

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

By Proposition 1, $E \otimes \sum_{x \in X_y}$ must be equal to $p \cdot \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|$ for some p. But then, $\frac{1}{p} E \otimes \sum_{x \in X_y} = \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|$, contradicting Lemma 2.

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 grater than 4, because $\mathfrak{D}$ is of dimension 4. □

Theorem 3. *If the cardinality of X and d are at least four, then $Q_d^{\oplus} X \neq Q_d X$.*

Proof. For $d = 4$ it is sufficient to note that this equivalence would contradict Lemma 3. This trivially generalizes to higher dimensional Hilbert spaces. □

Corollary 2. *There exists $S_1, Act, s_1 \in S_1$, and $\rightarrow_1 \in S_1 \times Act \times Q_d S_1$ such that $s_1 \nsim_{ls} s_2$ in all the eLTSs $(S_1 \cup S_2, Act, \rightarrow_1 \cup \rightarrow_2)$ with S_2 disjoint from S_1, and $\rightarrow_2 \in S_2 \times Act \times Q_d^{\oplus} S_2$.*

Proof. Let $S_1 = \{s_1, s_\alpha, s_\beta, s_\gamma, s_\delta, s_0\}$, $Act = \{\tau, \alpha, \beta, \gamma, \delta\}$, and let $\rightarrow_1$ be defined as

$$s_1 \xrightarrow{\tau}_1 \mathfrak{D} = \{s_\alpha \rhd \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|, s_\beta \rhd |\Phi^-\rangle\langle\Phi^-|, \\ s_\gamma \rhd \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right|, s_\delta \rhd |\Psi^-\rangle\langle\Psi^-|\}, \text{ and}$$

$$s_x \xrightarrow{x}_1 s_0 \text{ for } x \in \{\alpha, \beta, \gamma, \delta\}$$

$$\text{where } \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Note that $s_x \nsim s_y$ for any $x \neq y \in \{\alpha, \beta, \gamma, \delta\}$.

Now, assume $s_1 \sim_{ls} s_2$, then it must be that $s_2 \xrightarrow{\tau}_2 \mathfrak{T}$ with

$$\sum_{x \sim s_y} \mathfrak{T}(x) = \mathfrak{D}(s_y) \text{ for } y \in \{\alpha, \beta, \gamma, \delta\}.$$

It is sufficient to note that this would contradict Lemma 3 with X_y the equivalence class of $\{x \in X \mid x \sim_{ls} y\}$. Hence, no $\mathfrak{T}$ satisfying this condition is in $Q^{\oplus} S_2$. □

Theorem 5. *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 2, 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 2 in the other direction. □

Lemma 4. *Given a set of effects $\mathbb{E}$ of a fixed dimension, there exists a state ρ such that*

$$\forall i, j \in \mathbb{E}.\ tr(E_i \rho_{\mathbb{E}}) = tr(E_j \rho_{\mathbb{E}}) \text{ iff } i = j.$$

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 now 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 indexes $a \neq b$. 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 indexes 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 6. *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 5, 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 $next(s, \mu)$ be defined as

$$next(s, \mu) = \{\mathfrak{D} \mid \exists s' \in S. s \xrightarrow{\mu} \mathfrak{D}\}.$$

We let n be the maximum of the cardinality of X for $X \in next(s, \mu)$ for some s and μ.

Consider now the following set of effects:

$$\mathbb{E}^0 = \{E \mid \exists s, s' \in S, \mu \in Act. s \xrightarrow{\mu} \mathfrak{D} \text{ and } \mathfrak{D}(s') = E\}$$

We let $\mathbb{E}$ be the set of the effects obtained by summing up to n effects in $\mathbb{E}^0$.

By Lemma 4, there is a quantum state $\rho_{\mathbb{E}}$ such that

$$\forall E_i, E_j \in \mathbb{E}. tr(E_i \rho_{\mathbb{E}}) = tr(E_j \rho_{\mathbb{E}}) \text{ iff } E_i = E_j.$$

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 $\mathfrak{D}\downarrow_{\rho_{\mathbb{E}}} \sim^{\square}_{\rho_{\mathbb{E}}1} \mathfrak{T}\downarrow_{\rho_{\mathbb{E}}}$. 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 are left with proving 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 this is not the case, i.e. there is some C for which the condition above does not hold. Then it suffices to note that

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

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. □

Theorem 7. *If $s_1 \sim_{ls} s_2$ and $t_1 \sim_{ls} t_2$ then $s_1 + t_1 \sim_{ls} s_2 + t_2$.*

Proof. Let $\mathcal{R}_s$ ($\mathcal{R}_t$) be the LS-bisimilarity of the eLTS of s_1 and s_2 (of t_1 and t_2 rispectively). We will show that the following relation is a LS-bisimulation in the non-deterministic sum eLTS.

$$\mathcal{R} = \mathcal{R}_{s+t} \cup \mathcal{R}_s \cup \mathcal{R}_t \text{ where}$$
$$\mathcal{R}_{s+t} = \{(s_1 + t_1, s_2 + t_2) \mid s_1 \mathcal{R}_s s_2,\ t_1 \mathcal{R}_t t_2\}$$

Assume $x \mathcal{R} y$, then either $x \mathcal{R}_s y$, $x \mathcal{R}_t y$ or $s \mathcal{R}_{s+t} t$. The first two cases are trivial, since $\mathcal{R}_s$ and $\mathcal{R}_t$ are bisimilarity and are included in $\mathcal{R}$. Assume then that $x = s_1 + t_1$ and $y = s_2 + t_2$, and that $s_1 + t_1 \xrightarrow{\mu} \mathfrak{D}$. By definition of nondeterministic sum, either $s_1 \xrightarrow{\mu} \mathfrak{D}$ or $t_1 \xrightarrow{\mu} \mathfrak{D}$. In the first case, since $s_1 \sim s_2$, $s_2 \xrightarrow{\mu} \mathfrak{T}$ with

$$\forall C \in S/_{\mathcal{R}_s} \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x).$$

and by Ext.L, $s_2 + t \xrightarrow{\mu} \mathfrak{T}$.

We are left with proving that

$$\forall C \in S/_{\mathcal{R}} \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x).$$

We can reduce this condition to the former by simply noticing that $S/_{\mathcal{R}} = S/_{\mathcal{R}_s} \cup S/_{\mathcal{R}_t} \cup S/_{\mathcal{R}_{s+t}}$, and that

$$\forall C \in (S/_{\mathcal{R}_t} \cup S/_{\mathcal{R}_{s+t}}) \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x) = 0.$$

The second case, $t_1 \xrightarrow{\mu} \mathfrak{D}$ is similar, by considering Ext.R. □

Theorem 8. *If $s_1 \sim_{ls} s_2$ and $t_1 \sim_{ls} t_2$, then $s_1 \parallel t_1 \sim_{ls} s_2 \parallel t_2$.*

Proof. Let $\mathcal{R}_s$ ($\mathcal{R}_t$) be the LS-bisimilarity of the eLTS of s_1 and s_2 with states S_s (of t_1 and t_2 in S_t respectively). We will show that the following relation is a LS-bisimulation in the parallel composition eLTS.

$$\mathcal{R} = \{(s_1 \parallel t_1, s_2 \parallel t_2) \mid s_1 \mathcal{R}_s s_2,\ t_1 \mathcal{R}_t t_2\}$$

Take $(s_1 \parallel t_1, s_2 \parallel t_2) \in \mathcal{R}$, and assume $s_1 \parallel t_1$ performs a reduction, then it bust be one of the forms of the rules in Definition 12.

(Case ParL) We have that $s_1 \parallel t_1 \xrightarrow{\mu} \mathfrak{D} \parallel \{t_1 \triangleright \mathbb{I}\}$, and $s_1 \xrightarrow{\mu} \mathfrak{D}$. Then, since $s_1 \sim s_2$, it holds that $s_2 \xrightarrow{\mu} \mathfrak{T}$ with

$$\forall C \in S_s/_{\mathcal{R}_s} \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x).$$

By rule ParL, $s_2 \parallel t_2 \xrightarrow{\mu} \mathfrak{T} \parallel \{t_2 \triangleright \mathbb{I}\}$.

We are left with proving that

$$\forall C \in S/_{\mathcal{R}} \sum_{x \in C} (\mathfrak{D} \parallel \{t_1 \triangleright \mathbb{I}\})(x) = \sum_{x \in C} (\mathfrak{T} \parallel \{t_2 \triangleright \mathbb{I}\})(x).$$

We can rewrite this condition as follows, by omitting elements that are not in the support of the effect distributions.

$$\forall C \in S/_{\mathcal{R}} \sum_{x \parallel t_1 \in C} (\mathfrak{D} \parallel \{t_1 \triangleright \mathbb{I}\})(x) = \sum_{x \parallel t_2 \in C} (\mathfrak{T} \parallel \{t_2 \triangleright \mathbb{I}\})(x).$$

Moreover, we can define equivalence classes explicitly,

$$\forall s \in S_s \sum_{x \parallel t_1 \text{ s.t. } s \mathcal{R}_s x} (\mathfrak{D} \parallel \{t_1 \triangleright \mathbb{I}\})(x) = \sum_{x \parallel t_2 \text{ s.t. } s \mathcal{R}_s x} (\mathfrak{T} \parallel \{t_2 \triangleright \mathbb{I}\})(x).$$

We substitute the parallel composition of distributions with its definition.

$$\forall s \in S_s \sum_{x \text{ s.t. } s \mathcal{R}_s x} (\mathfrak{D}(x) \otimes \mathbb{I}) = \sum_{x \text{ s.t. } s \mathcal{R}_s x} (\mathfrak{T}(x) \otimes \mathbb{I}).$$

which clearly derives from our hypothesis by linearity of $\otimes$.

(Case ParR) It is similar to the previous case.

(Case Synch) We have that $s_1 \parallel t_1 \xrightarrow{\tau} \mathfrak{D}_1 \parallel \mathfrak{T}_1$, and both $s_1 \xrightarrow{\mu} \mathfrak{D}_1$ and $t_1 \xrightarrow{\overline{\mu}} \mathfrak{T}_1$. Since $s_1 \sim s_2$, it holds that $s_2 \xrightarrow{\mu} \mathfrak{D}_2$, with $\mathfrak{D}_1$ and $\mathfrak{D}_2$ satisfying the following

$$\forall C \in S_s/_{\mathcal{R}_s} \sum_{x \in C} \mathfrak{D}_1(x) = \sum_{x \in C} \mathfrak{D}_2(x).$$

Similarly, $t_2 \xrightarrow{\mu} \mathfrak{T}_2$, with $\mathfrak{T}_1$ and $\mathfrak{T}_2$ satisfying

$$\forall C \in S_t/_{\mathcal{R}_t} \sum_{x \in C} \mathfrak{T}_1(x) = \sum_{x \in C} \mathfrak{T}_2(x).$$

Then, by rule Synch, $s_2 \parallel t_2 \xrightarrow{\tau} \mathfrak{D}_2 \parallel \mathfrak{T}_2$.

We are left with proving that

$$\forall C \in S/_{\mathcal{R}} \sum_{x \in C} (\mathfrak{D}_1 \parallel \mathfrak{T}_1)(x) = \sum_{x \in C} (\mathfrak{D}_2 \parallel \mathfrak{T}_2)(x).$$

Notice that by construction of $\mathcal{R}$,

$$S/_{\mathcal{R}} = \{\{x \parallel y \mid x \in C_s,\ y \in C_t\} \mid C_s \in S_s/_{\mathcal{R}_s}, C_t \in S_t/_{\mathcal{R}_t}\}.$$

we can therefore rewrite our condition as

$$\forall C_s \in S_s/_{\mathcal{R}_s}, C_t \in S_t/_{\mathcal{R}_t} \quad \sum_{x \in C_s, y \in C_t} (\mathfrak{D}_1 \parallel \mathfrak{T}_1)(x \parallel y) = \sum_{x \in C_s, y \in C_t} (\mathfrak{D}_2 \parallel \mathfrak{T}_2)(x \parallel y)$$

By definition of the parallel composition of distributions, we obtain the following.

$$\forall C_s \in S_s/_{\mathcal{R}_s}, C_t \in S_t/_{\mathcal{R}_t} \quad \sum_{x \in C_s, y \in C_t} \mathfrak{D}_1(x) \otimes \mathfrak{T}_1(y) = \sum_{x \in C_s, y \in C_t} \mathfrak{D}_2(x) \otimes \mathfrak{T}_2(y)$$

It is the sufficient to resort to linearity of $\otimes$ to obtain the following which is trivially derivable from our hypothesis

$$\forall C_s \in S_s/_{\mathcal{R}_s}, C_t \in S_t/_{\mathcal{R}_t} \quad \left(\sum_{x \in C_s} \mathfrak{D}_1(x)\right) \otimes \left(\sum_{y \in C_t} \mathfrak{T}_1(y)\right) = \left(\sum_{x \in C_s} \mathfrak{D}_2(x)\right) \otimes \left(\sum_{y \in C_t} \mathfrak{T}_2(y)\right)$$

□

Theorem 9. *If $s \sim_{ls} t$ then $s|_\rho \sim_{ls} t|_\rho$ for any ρ.*

Proof. We prove the following $\mathcal{R}$ to be a ls-bisimulation.

$$\mathcal{R} = \left\{(s|_\rho, t|_\rho) \mid s \sim_{ls} t, \rho \in DM\right\}$$

Take $(s|_\rho, t|_\rho) \in \mathcal{R}$, and assume $s|_\rho$ performs a reduction, then, by Definition 14 it must be of the form $s|_\rho \xrightarrow{\mu} \mathfrak{D}|_\rho$, and it must be that $s \xrightarrow{\mu} \mathfrak{D}$.

Since $s \sim_{ls} t$, $t \xrightarrow{\mu} \mathfrak{T}$ such that

$$\forall C \in S/_{\sim_{ls}} \sum_{x \in C} \mathfrak{D}(x) = \sum_{x \in C} \mathfrak{T}(x). \tag{1}$$

Moreover, $t|_\rho \xrightarrow{\mu} \mathfrak{T}|_\rho$ by Definition 14.

We are left with proving that

$$\forall C \in S/_{\mathcal{R}} \sum_{x \in C} \mathfrak{D}|_\rho(x) = \sum_{x \in C} \mathfrak{T}|_\rho(x).$$

Note that, by definition of $\mathcal{R}$, given any $\rho \in DM$,

$$C \in S/_{\sim_{ls}} \text{ if and only if } \left\{x|_\rho \mid x \in C\right\} \in S/_{\mathcal{R}}.$$

Therefore, we can rewrite our condition as

$$\forall C \in S/_{\sim_{ls}} \sum_{x \in C} \mathfrak{D}|_\rho(x|_\rho) = \sum_{x \in C} \mathfrak{T}|_\rho(x|_\rho),$$

which clearly derives from Equation 1, by definition of $\mathfrak{D}|_\rho$ in Definition 14. □

Lemma 5. *For any d-dimensional eLTS $(S, Act, \rightarrow)$ and state $\rho \in DM_d$, 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*

$$s|_\rho \ \mathcal{R}|_\rho \ t|_\rho \text{ if and only if } s \ \mathcal{R} \ t$$

Proof. First of all note that for any two distribution $\mathfrak{D}, \mathfrak{T}$, it holds

$$\mathfrak{D}{\downarrow_\rho} \ \overset{\square}{\mathcal{R}} \ \mathfrak{T}{\downarrow_\rho} \text{ iff } \mathfrak{D}|_\rho \ \overset{\square}{\mathcal{R}|_\rho} \ \mathfrak{T}|_\rho$$

since $\mathfrak{D}{\downarrow_\rho}$ and $\mathfrak{D}|_\rho$ assign the same probability the same elements, modulo the $|_\rho$ renaming.

Now we prove the "only if" direction, proving that $\mathcal{R}|_\rho$ is a bisimulation. The other direction is similar. 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 $\mathfrak{D}{\downarrow_\rho} \ \overset{\square}{\mathcal{R}} \ \mathfrak{T}{\downarrow_\rho}$, because since they are probability distributions the equivalence class condition of ρ bisimilarity is equivalent to the relational lifting. Thus we get $\mathfrak{D}|_\rho \ \overset{\square}{\mathcal{R}|_\rho} \ \mathfrak{T}|_\rho$, showing that $\mathcal{R}|_\rho$ is a bisimulation. □

Corollary 1. *Given a d-dimensional eLTS $(S, Act, \rightarrow)$ and two states $s, t \in S$, if for any $\rho \in DM_d$ we have $s|_\rho \sim_{ls} t|_\rho$, then $s \sim_{ls} t$.*

Proof. We build the relation $\mathcal{R} = \{(x, y) \mid x|_\rho \sim_{ls} y|_\rho\}$, and of course we have $s\mathcal{R}t$. Then we can show that $\mathcal{R}|_\rho$ is a bisimulation, because when $x|_\rho \xrightarrow{\mu} \mathfrak{D}|_\rho$ we have $y|_\rho \xrightarrow{\mu} qT|_\rho$, and $\mathfrak{D}|_\rho, \mathfrak{T}|_\rho$ are not only in $\overset{\square}{\sim_{ls}}$, but also in $\overset{\square}{\mathcal{R}|_\rho}$. Thus, for Lemma 5, it must be that $\mathcal{R}$ is a ρ-bisimulation, and so s and t are ρ-bisimilar for any ρ. Tanks to Theorem 6, they are LS-bisimilar. □

Theorem 10. *If the dimension of the Hilbert space is two or greater, then $\mathfrak{D} + \mathfrak{T}$ is undefined if $\mathfrak{D}(s) = |\psi\rangle\langle\psi|$ and $\mathfrak{T}(t) = |\phi\rangle\langle\phi|$ for some states $s, t \in S$ and quantum states $|\psi\rangle$ and $|\phi\rangle$.*

Proof. Assume $\mathfrak{D} + \mathfrak{T}$ exists. Then $tr(|\psi\rangle\langle\psi| \cdot \rho) \cdot tr(|\phi\rangle\langle\phi| \cdot \rho) = tr(E \cdot \rho)$ for any ρ where $E = (\mathfrak{D} + \mathfrak{T})(s + t)$. Take $\rho = |\psi\rangle\langle\psi|$, then

$$\begin{aligned} &tr(|\psi\rangle\langle\psi| \cdot \rho) \cdot tr(|\phi\rangle\langle\phi| \cdot \rho) = \\ &= \langle\psi|\psi\rangle \langle\psi|\psi\rangle \cdot \langle\psi|\phi\rangle \langle\phi|\psi\rangle = \\ &= \langle\psi|\phi\rangle \langle\phi|\psi\rangle \text{ must be equal to } tr(E \cdot |\psi\rangle\langle\psi|). \end{aligned}$$

Similarly, by considering $\rho = |\phi\rangle\langle\phi|$, then

$$\begin{aligned} &tr(|\psi\rangle\langle\psi| \cdot \rho) \cdot tr(|\phi\rangle\langle\phi| \cdot \rho) = \\ &= \langle\phi|\psi\rangle \langle\psi|\phi\rangle \cdot \langle\phi|\phi\rangle \langle\phi|\phi\rangle = \\ &= \langle\phi|\psi\rangle \langle\psi|\phi\rangle = \langle\psi|\phi\rangle \langle\phi|\psi\rangle \\ &\text{must be equal to } tr(E \cdot |\phi\rangle\langle\phi|) = tr(E \cdot |\psi\rangle\langle\psi|). \end{aligned}$$

Consider now $\rho = \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\phi\rangle\langle\phi|$.

$$
\begin{aligned}
&tr(|\psi\rangle\langle\psi| \cdot \rho) \cdot tr(|\phi\rangle\langle\phi| \cdot \rho) = \\
&= tr(|\psi\rangle\langle\psi| \cdot (\frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\phi\rangle\langle\phi|)) \cdot \\
&\quad tr(|\phi\rangle\langle\phi| \cdot (\frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\phi\rangle\langle\phi|)) = \\
&= \frac{1}{2}tr(|\psi\rangle\langle\psi| \cdot |\psi\rangle\langle\psi| + |\psi\rangle\langle\psi| \cdot |\phi\rangle\langle\phi|) \cdot \\
&\quad \frac{1}{2}tr(|\phi\rangle\langle\phi| \cdot |\psi\rangle\langle\psi| + |\phi\rangle\langle\phi| \cdot |\phi\rangle\langle\phi|) = \\
&= \frac{1}{2}(tr(|\psi\rangle\langle\psi| \cdot |\psi\rangle\langle\psi|) + tr(|\psi\rangle\langle\psi| \cdot |\phi\rangle\langle\phi|)) \cdot \\
&\quad \frac{1}{2}(tr(|\phi\rangle\langle\phi| \cdot |\psi\rangle\langle\psi|) + tr(|\phi\rangle\langle\phi| \cdot |\phi\rangle\langle\phi|)) = \\
&= \frac{1}{2}(\langle\psi|\psi\rangle\langle\psi|\psi\rangle + \langle\phi|\psi\rangle\langle\psi|\phi\rangle) \cdot \\
&\quad \frac{1}{2}(\langle\phi|\psi\rangle\langle\psi|\phi\rangle + \langle\phi|\phi\rangle\langle\phi|\phi\rangle) = \\
&= \frac{1}{2}(1 + \langle\phi|\psi\rangle\langle\psi|\phi\rangle) \cdot \frac{1}{2}(\langle\phi|\psi\rangle\langle\psi|\phi\rangle + 1)
\end{aligned}
$$

must be equal to

$$
\begin{aligned}
&tr(E \cdot \rho) = tr(E \cdot (\frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\phi\rangle\langle\phi|)) = \\
&= \frac{1}{2}tr(E \cdot |\psi\rangle\langle\psi| + E \cdot |\phi\rangle\langle\phi|) = \\
&= \frac{1}{2}tr(E \cdot |\psi\rangle\langle\psi|) + \frac{1}{2}tr(E \cdot |\phi\rangle\langle\phi|) = \\
&= \frac{1}{2}\langle\psi|\phi\rangle\langle\phi|\psi\rangle + \frac{1}{2}\langle\psi|\phi\rangle\langle\phi|\psi\rangle = \langle\psi|\phi\rangle\langle\phi|\psi\rangle .
\end{aligned}
$$

The only solution is that $tr(E \cdot |\phi\rangle\langle\phi|) = tr(E \cdot |\psi\rangle\langle\psi|) = \langle\psi|\phi\rangle\langle\phi|\psi\rangle = 1$.

Since the dimension of the Hilbert space is at least 2, we can choose a state $|a\rangle$ such that $\langle a|\psi\rangle\langle\psi|a\rangle = 0$. Then also $\langle a|\phi\rangle\langle\phi|a\rangle = 0$. Take then $\rho = \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|a\rangle\langle a|$.

$$
\begin{aligned}
&tr(|\psi\rangle\langle\psi| \cdot \rho) \cdot tr(|\phi\rangle\langle\phi| \cdot \rho) = \\
&= \frac{1}{2}(\langle\psi|\psi\rangle\langle\psi|\psi\rangle + \langle a|\psi\rangle\langle\psi|a\rangle) \cdot \\
&\quad \frac{1}{2}(\langle\phi|\psi\rangle\langle\psi|\phi\rangle + \langle a|\phi\rangle\langle\phi|a\rangle) = \frac{1}{4}
\end{aligned}
$$

must be equal to

$$
\begin{aligned}
&tr(E \cdot \rho) = tr(E \cdot (\frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|a\rangle\langle a|)) = \\
&= \frac{1}{2}tr(E \cdot |\psi\rangle\langle\psi|) + \frac{1}{2}tr(E \cdot |a\rangle\langle a|) = \\
&= \frac{1}{2} + \frac{1}{2}tr(E \cdot |a\rangle\langle a|).
\end{aligned}
$$

Hence, $tr(E \cdot |a\rangle\langle a|) = -\frac{1}{2}$, which is impossible for an effect. □

Lemma 6. *Let $\rho \in DM_D$, $E \in \mathcal{E}f_d$, and s such that $d \cdot \dim(s) \leq D$. Then*

$$\langle E, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd p_i\} \Leftrightarrow \langle \mathcal{M}_E(\rho), s\rangle \xrightarrow{\mu} \{\mathcal{M}_{E_i}(\rho) \rhd p_i\}$$

Proof. First, let us prove

$$\langle E, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd p_i\} \Rightarrow \langle \mathcal{M}_E(\rho), s\rangle \xrightarrow{\mu} \{\mathcal{M}_{E_i}(\rho) \rhd p_i\}$$

by induction on the transitions obtained by instantiating the only rule for $\cdot|_\rho$ with each rule of the Heisenberg-style semantics.

(Case HPre) By induction hypothesis, it must be that $\mathrm{flat}(s) = ([E_i]s_i)_{i\in I}$ for some set I. Therefore, the SPre rule is applicable to $\langle \rho, \alpha.P\rangle$.

$$
\begin{array}{c}
\langle 1, \alpha.P\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}((E_i \otimes \mathbb{I})\rho)\} \\
\Updownarrow \\
\langle \rho, \alpha.P\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\rho), s_i\rangle \rhd \mathrm{tr}\big(\mathcal{M}_{E_i}(\rho)\big)\}
\end{array}
$$

It straightforward to show that $\mathrm{tr}(\mathcal{M}_E(\rho)) = \mathrm{tr}((E \otimes \mathbb{I})\rho)$ for any effect E and any partial density matrix ρ, defined over a state possibly larger than the state of E

$$
\begin{aligned}
\mathrm{tr}(\mathcal{M}_E(\rho)) &= \mathrm{tr}\Big(\mathrm{tr}_A\Big(\Big(\sqrt{E} \otimes \mathbb{I}\Big)\,\rho\,\Big(\sqrt{E} \otimes \mathbb{I}\Big)\Big)\Big) \\
&= \mathrm{tr}\Big(\Big(\sqrt{E} \otimes \mathbb{I}\Big)\,\rho\,\Big(\sqrt{E} \otimes \mathbb{I}\Big)\Big) \\
&= \mathrm{tr}((E \otimes \mathbb{I})\rho)
\end{aligned}
$$

(Case HSumL) By induction hypothesis, we have

$$
\begin{array}{c}
\langle 1, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}((E_i \otimes I)\rho)\} \\
\Updownarrow \\
\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\rho), s_i\rangle \rhd \mathrm{tr}((E_i \otimes I)\rho)\}
\end{array}
$$

Therefore, the SSumL rule is applicable to $\langle \rho, s + t\rangle$.

$$
\begin{array}{c}
\langle 1, s + t\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}((E_i \otimes I)\rho)\} \\
\Updownarrow \\
\langle \rho, s + t\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\rho), s_i\rangle \rhd \mathrm{tr}((E_i \otimes I)\rho)\}
\end{array}
$$

(Case HSumR) Analogous to the case for HSumL

(Case HParL) By induction hypothesis, we have

$$
\begin{array}{c}
\langle 1, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}((E_i \otimes I)\rho)\} \\
\Updownarrow \\
\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\rho), s_i\rangle \rhd \mathrm{tr}((E_i \otimes I)\rho)\}
\end{array}
$$

Therefore, the SParL rule is applicable to $\langle \rho, s \parallel t\rangle$.

$$
\begin{array}{c}
\langle 1, s \parallel t\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i \parallel t\rangle\big|_\rho \rhd \mathrm{tr}((E_i \otimes I)\rho)\} \\
\Updownarrow \\
\langle \rho, s \parallel t\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\rho), s_i \parallel t\rangle \rhd \mathrm{tr}((E_i \otimes I)\rho)\}
\end{array}
$$

(Case HParR) Analogous to the case for HParL

(Case HSyncL) By induction hypothesis, we have

$$
\begin{array}{c}
\langle 1, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}((E_i \otimes I)\rho)\} \\
\Updownarrow \\
\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\rho), s_i\rangle \rhd \mathrm{tr}((E_i \otimes I)\rho)\}
\end{array}
$$

and

$$
\begin{array}{c}
\langle 1, t\rangle\big|_\rho \xrightarrow{\overline{\mu}} \{\langle E_j, t_j\rangle\big|_\rho \rhd \mathrm{tr}\big((E_j \otimes I)\rho\big)\} \\
\Updownarrow \\
\langle \rho, t\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{M}_{E_j}(\rho), t_j\rangle \rhd \mathrm{tr}\big((E_j \otimes I)\rho\big)\}
\end{array}
$$

Therefore, the SSyncL rule is applicable to $\langle \rho, s \parallel t\rangle$.

$$\langle 1, s \parallel t\rangle\big|_\rho \xrightarrow{\tau} \{\langle E_i \otimes E_j, s_i \parallel t_j\rangle\big|_\rho \rhd \mathrm{tr}(((E_i \otimes E_j) \otimes \mathbb{I})\rho)\}$$
$$\Updownarrow$$
$$\langle \rho, s \parallel t\rangle \xrightarrow{\tau} \{\langle \mathcal{M}_{F_j}(\mathcal{M}_{E_i}(\rho)), s_i \parallel t_j\rangle \rhd \mathrm{tr}\Big(\mathcal{M}_{E_j}(\mathcal{M}_{E_i}(\rho))\Big)\}$$

However, since measurements are destructive, it holds that

$$\mathrm{tr}\Big(\mathcal{M}_{E_j}(\mathcal{M}_{E_i}(\rho))\Big) = \mathrm{tr}\Big(\mathcal{M}_{E_i\otimes E_j}(\rho)\Big) = \mathrm{tr}\big(((E_i \otimes E_j) \otimes \mathbb{I})\rho\big)$$

(Case HSyncR) Analogous to the case for HSyncL

(Case HLift) By induction hypothesis,

$$\langle 1, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}((E_i \otimes I)\rho)\}$$
$$\Updownarrow$$
$$\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\rho), s_i\rangle \rhd \mathrm{tr}((E_i \otimes I)\rho)\}$$

Notice that, if $\langle \sigma, s\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\sigma), s_i\rangle \rhd \mathrm{tr}((E_i \otimes I)\sigma)\}$ for some σ, then all σ' behaves similarly with possibly different weights, i.e.

$$\langle \sigma', s\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\sigma'), s_i\rangle \rhd \mathrm{tr}\big((E_i \otimes I)\sigma'\big)\}$$

Therefore,

$$\langle E, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle E \otimes E_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}(((E \otimes E_i) \otimes I)\rho)\}$$
$$\Updownarrow$$
$$\langle \mathcal{M}_E(\rho), s\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\mathcal{M}_E(\rho)), s_i\rangle \rhd \mathrm{tr}\big(\mathcal{M}_{E_i}(\mathcal{M}_E(\rho))\big)\}$$

As for the previous case, $\mathrm{tr}\big(\mathcal{M}_{E_i}(\mathcal{M}_E(\rho))\big) = \mathrm{tr}(((E \otimes E_i) \otimes \mathbb{I})\rho)$.

Second, let us prove

$$\langle E, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle E_i, s_i\rangle\big|_\rho \rhd p_i\} \Leftarrow \langle \mathcal{M}_E(\rho), s\rangle \xrightarrow{\mu} \{\mathcal{M}_{E_i}(\rho) \rhd p_i\}$$

by induction on the transitions in the Schrödinger-style semantics.

(Case SPre) By rule precondition it must be that $\mathrm{flat}(s) = ([E_i]s_i)_{i\in I}$ for some set I. Therefore, the HLift followed by the HPre rule are applicable to $\langle E, \mu.P\rangle$.

$$\langle \mathcal{M}_E(\rho), \mu.P\rangle \xrightarrow{\mu} \{\langle \mathcal{M}_{E_i}(\mathcal{M}_E(\rho)), s_i\rangle \rhd \mathrm{tr}\big(\mathcal{M}_{E_i}(\mathcal{M}_E(\rho))\big)\}$$
$$\Updownarrow$$
$$\langle E, \mu.P\rangle\big|_\rho \xrightarrow{\mu} \{\langle E \otimes E_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}((E \otimes E_i \otimes \mathbb{I})\rho)\}$$

But, as showed before, $\mathrm{tr}\big(\mathcal{M}_{E_i}(\mathcal{M}_E(\rho))\big) = \mathrm{tr}((E \otimes E_i \otimes \mathbb{I})(\rho))$

(Other cases) All other cases follow the same line of reasoning of SPre, where we first need to apply a HLift. □

Theorem 11. *For any atomic state s and $\rho \in DM_{\dim(s)}$*

$$\langle 1, s\rangle\big|_\rho \sim_{ls} \langle \rho, s\rangle$$

Proof. Let $D = dim(s)$, take the relation

$$\mathcal{R}_D = \left\{ \left(\langle E, t\rangle\big|_\rho, \langle \mathcal{M}_E(\rho), t\rangle\right) \;\middle|\; \begin{array}{l} t \in S, \rho \in DM_D, E \in \mathcal{E}f_d \\ d \cdot \dim(t) \le D \end{array} \right\}$$

From Lemma 6 it is trivial to show that such relation is a bisimulation and it includes $(\langle 1, s\rangle\big|_\rho, \langle \rho, s\rangle)$ □

Lemma 7. *Let $\rho \in DM_d$ with $d \ge \dim(s)$,*

$$\langle \mathcal{E}, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd p_i\} \Leftrightarrow \langle \mathcal{E}(\rho), s\rangle \xrightarrow{\mu} \{\mathcal{E}_i(\rho) \rhd p_i\}$$

Proof. First, let us prove

$$\langle \mathcal{E}, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd p_i\} \Rightarrow \langle \mathcal{E}(\rho), s\rangle \xrightarrow{\mu} \{\mathcal{E}_i(\rho) \rhd p_i\}$$

by induction on the transitions in the restricted Heisenberg-style semantics.

(Case HPre) By rule precondition it must be that $\mathrm{flat}(s) = ([\mathcal{E}_i]s_i)_{i\in I}$ for some set I. Therefore, the SPre rule is applicable to $\langle \rho, \alpha.P\rangle$.

$$\langle \mathcal{I}, \alpha.P\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}(\rho)\big)\}$$
$$\Updownarrow$$
$$\langle \rho, \alpha.P\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd \mathrm{tr}(\mathcal{E}_i(\rho))\}$$

It is straightforward to show that $\mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big) = \mathrm{tr}(\mathcal{E}_i(\rho))$:

$$\begin{aligned}\mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big) &= \mathrm{tr}\left(\left(\sum_k E_k^\dagger E_k\right)\rho\right) \\ &= \mathrm{tr}\left(\sum_k E_k \rho E_k^\dagger\right) \\ &= \mathrm{tr}(\mathcal{E}_i(\rho))\end{aligned}$$

where $\{E_k\}_k$ is a Kraus decomposition of $\mathcal{E}_i$.

(Case HSumL) By induction on the precondition

$$\langle \mathcal{I}, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$
$$\Updownarrow$$
$$\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$

Therefore, the SSumL rule is applicable to $\langle \rho, s + t\rangle$.

$$\langle \mathcal{I}, s + t\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$
$$\Updownarrow$$
$$\langle \rho, s + t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$

(Case HSumR) Analogous to the case for HSumL

(Case HParL) By induction on the precondition

$$\langle \mathcal{I}, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$
$$\Updownarrow$$
$$\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$

Therefore, the SParL rule is applicable to $\langle \rho, s \parallel t\rangle$.

$$\langle \mathcal{I}, s \parallel t\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i \parallel t\rangle\big|_\rho \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$
$$\Updownarrow$$
$$\langle \rho, s \parallel t\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\rho), s_i \parallel t\rangle \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$

(Case HParR) Analogous to the case for HParL

(Case HSyncL) By induction on the preconditions

$$\langle \mathcal{I}, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$
$$\Updownarrow$$
$$\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$

and

$$\langle \mathcal{I}, t\rangle\big|_\rho \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_j, t_j\rangle\big|_\rho \rhd \mathrm{tr}\Big(E_{\mathcal{E}_j}\rho\Big)\}$$
$$\Updownarrow$$
$$\langle \rho, t\rangle \xrightarrow{\overline{\mu}} \{\langle \mathcal{E}_j(\rho), t_j\rangle \rhd \mathrm{tr}\Big(E_{\mathcal{E}_j}\rho\Big)\}$$

Therefore, the SSyncL rule is applicable to $\langle \rho, s \parallel t\rangle$.

$$\langle \mathcal{I}, s \parallel t\rangle\big|_\rho \xrightarrow{\tau} \{\langle \mathcal{E}_j \circ \mathcal{E}_i, s_i \parallel t_j\rangle\big|_\rho \rhd \mathrm{tr}\Big(E_{\mathcal{E}_i \otimes \mathcal{E}_j}\rho\Big)\}$$
$$\Updownarrow$$
$$\langle \rho, s \parallel t\rangle \xrightarrow{\tau} \{\langle \mathcal{E}_j(\mathcal{E}_i(\rho)), s_i \parallel t_j\rangle \rhd \mathrm{tr}\big(\mathcal{E}_j(\mathcal{E}_i(\rho))\big)\}$$

However, $\mathrm{tr}\big(\mathcal{E}_j(\mathcal{E}_i(\rho))\big) = \mathrm{tr}\Big(E_{\mathcal{E}_j\circ\mathcal{E}_i}\rho\Big)$

$$\mathrm{tr}\big(\mathcal{E}_j(\mathcal{E}_i(\rho))\big) = \mathrm{tr}\big((\mathcal{E}_j \circ \mathcal{E}_i)(\rho)\big) = \mathrm{tr}\Big(E_{\mathcal{E}_j\circ\mathcal{E}_i}\rho\Big)$$

(Case HSyncR) Analogous to the case for HSyncL

(Case HLift) By induction on the precondition

$$\langle \mathcal{I}, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$
$$\Updownarrow$$
$$\langle \rho, s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\rho), s_i\rangle \rhd \mathrm{tr}\big(E_{\mathcal{E}_i}\rho\big)\}$$

Therefore, by selecting $\rho = \mathcal{M}_E(\rho)$

$$\langle \mathcal{E}, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i \circ \mathcal{E}, s_i\rangle\big|_\rho \rhd \mathrm{tr}\big(E_{\mathcal{E}_i\circ\mathcal{E}}\rho\big)\}$$
$$\Updownarrow$$
$$\langle \mathcal{M}_E(\rho), s\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\mathcal{E}(\rho)), s_i\rangle \rhd \mathrm{tr}(\mathcal{E}_i(\mathcal{E}(\rho)))\}$$

As for the previous case, $\mathrm{tr}(\mathcal{E}_i(\mathcal{E}(\rho))) = \mathrm{tr}\big(E_{\mathcal{E}_i\circ\mathcal{E}}\rho\big)$.

Second, let us prove

$$\langle \mathcal{E}, s\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i, s_i\rangle\big|_\rho \rhd p_i\} \Leftarrow \langle \mathcal{E}(\rho), s\rangle \xrightarrow{\mu} \{\mathcal{E}_i(\rho) \rhd p_i\}$$

by induction on the transitions in the Schrödinger-style semantics.

(Case SPre) By rule precondition it must be that $\mathrm{flat}(s) = ([\mathcal{E}_i]s_i)_{i\in I}$ for some set I. Therefore, the HLift followed by the HPre rule are applicable to $\langle \mathcal{E}, \mu.P\rangle$.

$$\langle \mathcal{E}_i(\mathcal{E}(\rho)), \mu.P\rangle \xrightarrow{\mu} \{\langle \mathcal{E}_i(\mathcal{E}(\rho)), s_i\rangle \rhd \mathrm{tr}(\mathcal{E}_i(\mathcal{E}(\rho)))\}$$
$$\Updownarrow$$
$$\langle \mathcal{E}, \mu.P\rangle\big|_\rho \xrightarrow{\mu} \{\langle \mathcal{E}_i \circ \mathcal{E}, s_i\rangle\big|_\rho \rhd \mathrm{tr}\big(E_{\mathcal{E}_i\circ\mathcal{E}}\rho\big)\}$$

But, as showed before, $\mathrm{tr}(\mathcal{E}_i(\mathcal{E}(\rho))) = \mathrm{tr}\big(E_{\mathcal{E}_i\circ\mathcal{E}}\rho\big)$

(Other cases) All other cases follow the same line of reasoning of SPre, where we first need to apply a HLift. □

Theorem 13. *For any d-dimensional atomic process s and any* $\rho \in DM_d$, $\langle \mathcal{I}_d, s\rangle|_\rho \sim_{ls} \langle \rho, s\rangle$.

Proof. Take the relation

$$\mathcal{R} = \left\{\Big(\langle \mathcal{E}, s\rangle\big|_\rho, \langle \mathcal{E}(\rho), s\rangle\Big) \mid s \in S, \rho \in DM_d, \mathcal{E} \in \mathcal{SO}_d\right\}$$

From Lemma 7 it is trivial to show that such relation is a bisimulation and thus the theorem holds. □