Open Bisimulation for Quantum Processes

Yuxin Deng[1] Yuan Feng[2]
[1]Shanghai Jiao Tong University, China
[2] University of Technology, Sydney, Australia, and Tsinghua University, China

January 4, 2012

Abstract

Quantum processes describe concurrent communicating systems that may involve quantum information. We propose a notion of open bisimulation for quantum processes and show that it provides both a sound and complete proof methodology for a natural extensional behavioural equivalence between quantum processes. We also give a modal characterisation of open bisimulation, by extending the Hennessy-Milner logic to a quantum setting.

1 Introduction

The theory of quantum computing has attracted considerable research efforts in the past twenty years. Benefiting from the superposition of quantum states and linearity of quantum operations, quantum computing may provide considerable speedup over its classical analogue [39, 14, 15]. However, functional quantum computers which can harness this potential in dealing with practical applications are extremely difficult to implement. On the other hand, quantum cryptography, of which the security and ability to detect the presence of eavesdropping are provable based on the principles of quantum mechanics, has been developed so rapidly that quantum cryptographic systems are already commercially available by a number of companies such as Id Quantique, Cerberis, MagiQ Technologies, SmartQuantum, and NEC.

As is well known, it is very difficult to guarantee the correctness of classical communication protocols at the design stage, and some simple protocols were finally found to have fundamental flaws. Since human intuition is poorly adapted to the quantum world, quantum protocol designers will definitely make more faults than classical protocol designers, especially when more and more complicated quantum protocols can be implemented by future physical technology. In view of the success that classical process algebras [28, 19, 1] achieved in analyzing and verifying classical communication protocols, several research groups proposed various quantum process algebras with the purpose of modeling quantum protocols. Jorrand and Lalire [25, 27] defined a language QPAlg (Quantum Process Algebra) by adding primitives expressing unitary transformations and quantum measurements, as well as communications of quantum states, to a CCS-like classical process algebra. An operational semantics of QPAlg is given, and further a probabilistic branching bisimulation between quantum processes is defined. Gay and Nagarajan [12, 13] proposed a language CQP (Communicating Quantum Processes), which is obtained from the pi-calculus [29] by adding primitives for measurements and transformations of quantum states, and allowing transmission of qubits. They presented a type system for CQP, and in particular proved that the semantics preserves typing and that typing guarantees that each qubit is owned by a unique process within a system. The second author of the current paper, together with his colleagues, proposed a language named qCCS [9, 41, 10] for quantum communicating systems by adding quantum input/output and quantum operation/measurement primitives to classical value-passing CCS [16, 17]. One distinctive feature of qCCS, compared to QPAlg and CQP, is that it provides a framework to describe, as well as reason about, the communication of quantum systems which are entangled with other systems. Furthermore, a bisimulation for processes in qCCS has been introduced, and the associated bisimilarity is proven to be a congruence with respect to all process constructors of qCCS.

Uniqueness of the solutions to recursive process equations is also established, which provides a powerful proof technique for verifying complex quantum protocols.

In the study of quantum systems, as well as classical communicating systems, an important problem is to tell if two given systems exhibit the same behaviour. To approach the problem we first need to give criteria for reasonable behavioural equivalence. Two systems should only be distinguished on the basis of the chosen criteria. Therefore, these criteria induce an extensional equivalence between systems, $\approx_{\mathrm{behav}}$, namely the largest equivalence which satisfies them.

Having an independent notion of which systems should, and which should not, be distinguished, one can then justify a particular notion of equivalence, e.g. bisimulation, by showing that it captures precisely the touchstone equivalence. In other words, a particular definition of bisimulation is appropriate because $\approx_{\mathrm{bisi}}$, the associated bisimulation equivalence,

(i) is *sound* with respect to the touchstone equivalence, that is $s_1 \approx_{bis} s_2$ implies $s_1 \approx_{\mathrm{behav}} s_2$;

(ii) provides a *complete* proof methodology for the touchstone equivalence, that is $s_1 \approx_{\mathrm{behav}} s_2$ implies $s_1 \approx_{bis} s_2$.

This approach originated in [20] but has now been widely used for different process description languages; for example, see [21, 34] for its application to higher-order process languages, [32] for mobile ambients, [11] for asynchronous languages and [5] for probabilistic timed languages. Moreover, in each case the distinguishing criteria are more or less the same. The touchstone equivalence should

(i) be *compositional*; that is preserved by some natural operators for constructing systems;

(ii) *preserve barbs*; barbs are simple experiments which observers may perform on systems [33];

(iii) be *reduction-closed*; this is a natural condition on the reduction semantics of systems which ensures that nondeterministic choices are in some sense preserved.

We adapt this approach to quantum processes. Using natural versions of these criteria we obtain an appropriate touchstone equivalence, which we call *reduction barbed congruence*, $\approx_r$. We then develop a theory of bisimulations which is both sound and complete for $\approx_r$. Moreover, we provide a modal characterisation of $\approx_r$ in a quantum logic based on Hennessy-Milner logic [18]by establishing the coincidence of the largest bisimilation with logical equivalence.

The remainder of the paper is organised as follows. In the next section we recall some preliminary concepts from quantum theory. In Section 3 we review the model of probabilistic labelled transition systems, based on which we give the operational semantics of qCCS in Section 4. Section 5 contains the main theoretical results of the paper. We define a notion of open bisimulation, which is shown to be a congruence relation in the language of qCCS. It turns out that open bisimilarity precisely captures reduction barbed congruence, thus provides a sound and complete proof methodology for our touchstone equivalence. In addition, we give a modal characterisation of the equivalence in a quantum logic obtained by an extension of Hennessy-Milner logic with a probabilistic choice modality and a super-operator application modality. To illustrate the application of open bisimulation and its modal characterisation, in Section 6 we describe the key distribution protocol BB84 as qCCS processes and compare a specification with its implementations of the protocol. The paper ends with a brief comparison with related work in Section 7.

2 Preliminaries on quantum mechanics

In this section, we briefly recall some basic concepts from quantum theory, which requires first some notions from linear algebra. More details about quantum computation can be found in many books, e.g. [30].

2.1 Basic linear algebra

A *Hilbert space* $\mathcal{H}$ is a complete vector space equipped with an inner product

$$\langle\cdot|\cdot\rangle : \mathcal{H}\times\mathcal{H}\to\mathbf{C}$$

such that

1. $\langle\psi|\psi\rangle \geq 0$ for any $|\psi\rangle\in\mathcal{H}$, with equality if and only if $|\psi\rangle = 0$;
2. $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$;
3. $\langle\phi|\sum_i c_i|\psi_i\rangle = \sum_i c_i\langle\phi|\psi_i\rangle$,

where $\mathbf{C}$ is the set of complex numbers, and for each $c\in\mathbf{C}$, c^* stands for the complex conjugate of c. For any vector $|\psi\rangle\in\mathcal{H}$, its length $|||\psi\rangle||$ is defined to be $\sqrt{\langle\psi|\psi\rangle}$, and it is said to be *normalized* if $|||\psi\rangle|| = 1$. Two vectors $|\psi\rangle$ and $|\phi\rangle$ are *orthogonal* if $\langle\psi|\phi\rangle = 0$. An *orthonormal basis* of a Hilbert space $\mathcal{H}$ is a basis $\{|i\rangle\}$ where each $|i\rangle$ is normalized and any pair of them are orthogonal.

Let $\mathcal{L}(\mathcal{H})$ be the set of linear operators on $\mathcal{H}$. For any $A\in\mathcal{L}(\mathcal{H})$, A is *Hermitian* if $A^\dagger = A$ where $A^\dagger$ is the adjoint operator of A such that $\langle\psi|A^\dagger|\phi\rangle = \langle\phi|A|\psi\rangle^*$ for any $|\psi\rangle, |\phi\rangle\in\mathcal{H}$. The fundamental *spectral theorem* [30] states that the set of all normalized eigenvectors of a Hermitian operator in $\mathcal{L}(\mathcal{H})$ constitutes an orthonormal basis for $\mathcal{H}$. That is, there exists a so-called spectral decomposition for each Hermitian A such that

$$A = \sum_i \lambda_i|i\rangle\langle i| = \sum_{\lambda_i\in spec(A)} \lambda_i E_i$$

where the set $\{|i\rangle\}$ constitutes an orthonormal basis of $\mathcal{H}$, $spec(A)$ denotes the set of eigenvalues of A, and E_i is the projector to the corresponding eigenspace of λ_i. A linear operator $A\in\mathcal{L}(\mathcal{H})$ is *unitary* if $A^\dagger A = AA^\dagger = I_\mathcal{H}$, where $I_\mathcal{H}$ is the identity operator on $\mathcal{H}$. For instance, a well-known unitary operator is the 1-qubit Hadamard operator H defined as follows:

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

The *trace* of $A\in\mathcal{L}(\mathcal{H})$ is defined as $\mathrm{tr}(A) = \sum_i\langle i|A|i\rangle$ for some given orthonormal basis $\{|i\rangle\}$ of $\mathcal{H}$. It is worth noting that trace function is actually independent of the chosen orthonormal basis. It is also easy to check that trace function is linear and $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for any operators $A, B\in\mathcal{L}(\mathcal{H})$.

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces. Their *tensor product* $\mathcal{H}_1\otimes\mathcal{H}_2$ is defined as a vector space consisting of linear combinations of the vectors $|\psi_1\psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\rangle\otimes|\psi_2\rangle$ with $|\psi_1\rangle\in\mathcal{H}_1$ and $|\psi_2\rangle\in\mathcal{H}_2$. Here the tensor product of two vectors is defined by a new vector such that

$$\left(\sum_i \lambda_i|\psi_i\rangle\right)\otimes\left(\sum_j \mu_j|\phi_j\rangle\right) = \sum_{i,j}\lambda_i\mu_j|\psi_i\rangle\otimes|\phi_j\rangle.$$

Then $\mathcal{H}_1\otimes\mathcal{H}_2$ is also a Hilbert space where the inner product is defined as the following: for any $|\psi_1\rangle, |\phi_1\rangle\in\mathcal{H}_1$ and $|\psi_2\rangle, |\phi_2\rangle\in\mathcal{H}_2$,

$$\langle\psi_1\otimes\psi_2|\phi_1\otimes\phi_2\rangle = \langle\psi_1|\phi_1\rangle_{\mathcal{H}_1}\langle\psi_2|\phi_2\rangle_{\mathcal{H}_2}$$

where $\langle\cdot|\cdot\rangle_{\mathcal{H}_i}$ is the inner product of $\mathcal{H}_i$. For any $A_1\in\mathcal{L}(\mathcal{H}_1)$ and $A_2\in\mathcal{L}(\mathcal{H}_2)$, $A_1\otimes A_2$ is defined as a linear operator in $\mathcal{L}(\mathcal{H}_1\otimes\mathcal{H}_2)$ such that for each $|\psi_1\rangle\in\mathcal{H}_1$ and $|\psi_2\rangle\in\mathcal{H}_2$,

$$(A_1\otimes A_2)|\psi_1\psi_2\rangle = A_1|\psi_1\rangle\otimes A_2|\psi_2\rangle.$$

The *partial trace* of $A\in\mathcal{L}(\mathcal{H}_1\otimes\mathcal{H}_2)$ with respected to $\mathcal{H}_1$ is defined as $\mathrm{tr}_{\mathcal{H}_1}(A) = \sum_i\langle i|A|i\rangle$ where $\{|i\rangle\}$ is an orthonormal basis of $\mathcal{H}_1$. Similarly, we can define the partial trace of A with respected to $\mathcal{H}_2$. Partial trace functions are also independent of the orthonormal basis selected.

An operator $A \in \mathcal{L}(\mathcal{H})$ is *positive* if $\langle\psi|A\psi\rangle \geq 0$ for every $\psi \in \mathcal{H}$. A linear operator $\mathcal{E}$ on $\mathcal{L}(\mathcal{H})$ is *completely positive* if it maps positive operators in $\mathcal{L}(\mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H})$, and for any auxiliary Hilbert space $\mathcal{H}'$, the trivially extended operator $\mathcal{I}_{\mathcal{H}'} \otimes \mathcal{E}$ also maps positive operators in $\mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$. Here $\mathcal{I}_{\mathcal{H}'}$ is the identity operator on $\mathcal{L}(\mathcal{H}')$. The elegant and powerful *Kraus representation theorem* [26] of completely positive operators states that a linear operator $\mathcal{E}$ is completely positive if and only if there is some set of operators $\{E_i\}$ with appropriate dimension such that

$$\mathcal{E}(A) = \sum_i E_i A E_i^\dagger$$

for any $A \in \mathcal{L}(\mathcal{H})$. The operators E_i are called Kraus operators of $\mathcal{E}$. A linear operator is said to be a *super-operator* if it is completely positive and trace-nonincreasing. Here an operator $\mathcal{E}$ is *trace-nonincreasing* if $\mathrm{tr}(\mathcal{E}(A)) \leq \mathrm{tr}(A)$ for any positive $A \in \mathcal{L}(\mathcal{H})$, and it is said to be *trace-preserving* if the equality always holds. Then a super-operator (resp. a trace-preserving super-operator) is a completely positive operator with its Kraus operators E_i satisfying $\sum_i E_i^\dagger E_i \leq I$ (resp. $\sum_i E_i^\dagger E_i = I$). We denote by $\mathcal{SO}(\mathcal{H})$ the set of trace-preserving super-operators on the Hilbert space $\mathcal{H}$.

2.2 Basic quantum mechanics

According to von Neumann's formalism of quantum mechanics [40], an isolated physical system is associated with a Hilbert space which is called the *state space* of the system. A *pure state* of a quantum system is a normalized vector in its state space, and a *mixed state* is represented by a density operator on the state space. Here a density operator ρ on Hilbert space $\mathcal{H}$ is a positive linear operator such that $\mathrm{tr}(\rho) = 1$. Another equivalent representation of density operator is probabilistic ensemble of pure states. In particular, given an ensemble $\{(p_i, |\psi_i\rangle)\}$ where $p_i \geq 0$, $\sum_i p_i = 1$, and $|\psi_i\rangle$ are pure states, then $\rho = \sum_i p_i[|\psi_i\rangle]$ is a density operator. Here $[|\psi_i\rangle]$ denotes the abbreviation of $|\psi_i\rangle\langle\psi_i|$. Conversely, each density operator can be generated by an ensemble of pure states in this way. The set of density operators on $\mathcal{H}$ can be defined as

$$\mathcal{D}(\mathcal{H}) = \{\ \rho \in \mathcal{L}(\mathcal{H})\ :\ \rho \text{ is positive and } \mathrm{tr}(\rho) = 1\}.$$

The state space of a composite system (for example, a quantum system consisting of many qubits) is the tensor product of the state spaces of its components. For a mixed state ρ on $\mathcal{H}_1 \otimes \mathcal{H}_2$, partial traces of ρ have explicit physical meanings: the density operators $\mathrm{tr}_{\mathcal{H}_1}\rho$ and $\mathrm{tr}_{\mathcal{H}_2}\rho$ are exactly the reduced quantum states of ρ on the second and the first component system, respectively. Note that in general, the state of a composite system cannot be decomposed into tensor product of the reduced states on its component systems. A well-known example is the 2-qubit state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

This kind of state is called *entangled state*. To see the strangeness of entanglement, suppose a measurement $M = \lambda_0[|0\rangle] + \lambda_1[|1\rangle]$ is applied on the first qubit of $|\Psi\rangle$ (see the following for the definition of quantum measurements). Then after the measurement, the second qubit will definitely collapse into state $|0\rangle$ or $|1\rangle$ depending on whether the outcome λ_0 or λ_1 is observed. In other words, the measurement on the first qubit changes the state of the second qubit in some way. This is an outstanding feature of quantum mechanics which has no counterpart in classical world, and is the key to many quantum information processing tasks such as teleportation [3] and superdense coding [4].

The evolution of a closed quantum system is described by a unitary operator on its state space: if the states of the system at times t_1 and t_2 are ρ_1 and ρ_2, respectively, then $\rho_2 = U\rho_1 U^\dagger$ for some unitary operator U which depends only on t_1 and t_2. In contrast, the general dynamics which can occur in a physical system is described by a trace-preserving super-operator on its state space. Note that the unitary transformation $U(\rho) = U\rho U^\dagger$ is a trace-preserving super-operator.

A quantum *measurement* is described by a collection $\{M_m\}$ of measurement operators, where the indices m refer to the measurement outcomes. It is required that the measurement operators satisfy the completeness equation $\sum_m M_m^\dagger M_m = I_{\mathcal{H}}$. If the system is in state ρ, then the probability that measurement result m occurs is given by

$$p(m) = \mathrm{tr}(M_m^\dagger M_m \rho),$$

and the state of the post-measurement system is $M_m \rho M_m^\dagger / p(m)$.

A particular case of measurement is *projective measurement* which is usually represented by a Hermitian operator. Let M be a Hermitian operator and

$$M = \sum_{m \in spec(M)} m E_m \tag{1}$$

its spectral decomposition. Obviously, the projectors $\{E_m : m \in spec(M)\}$ form a quantum measurement. If the state of a quantum system is ρ, then the probability that result m occurs when measuring M on the system is $p(m) = \mathrm{tr}(E_m \rho)$, and the post-measurement state of the system is $E_m \rho E_m / p(m)$. Note that for each outcome m, the map

$$\mathcal{E}_m(\rho) = E_m \rho E_m$$

is again a super-operator by Kraus Theorem; it is not trace-preserving in general.

Let M be a projective measurement with Eq.(1) its spectral decomposition. We call M non-degenerate if for any $m \in spec(M)$, the corresponding projector E_m is 1-dimensional; that is, all eigenvalues of M are non-degenerate. Non-degenerate measurement is obviously a very special case of general quantum measurement. However, when an ancilla system lying at a fixed state is provided, non-degenerate measurements together with unitary operators are sufficient to implement general measurements [30].

3 A probabilistic model

In this section we review the model of probabilistic labelled transition systems (pLTSs), and some properties of weak transitions. Later on we will interpret the behaviour of quantum processes in terms of pLTSs.

3.1 Probabilistic labelled transition systems

We begin with some notation. A (discrete) probability distribution over a set S is a function $\Delta : S \to [0, 1]$ with $\sum_{s \in S} \Delta(s) = 1$; the support of such a Δ is the set $\lceil \Delta \rceil = \{ s \in S \mid \Delta(s) > 0 \}$. The point distribution $\overline{s}$ assigns probability 1 to s and 0 to all other elements of S, so that $\lceil \overline{s} \rceil = s$. We use $\mathcal{D}(S)$ to denote the set of distributions over S, ranged over by Δ, Θ etc. If $\sum_{k \in K} p_k = 1$ for some collection of $p_k \geq 0$, and the Δ_k are distributions, then so is $\sum_{k \in K} p_k \cdot \Delta_k$ with $(\sum_{k \in K} p_k \cdot \Delta_k)(s) \;=\; \sum_{i \in I} p_i \cdot \Delta_i(s)$.

Definition 3.1. *A* probabilistic labelled transition system *(pLTS) is a triple $\langle S, \mathsf{Act}_\tau, \to \rangle$, where*

(i) S is a set of states;

(ii) Act_τ is a set of transition labels, with distinguished element τ;

(iii) the relation $\to$ is a subset of $S \times \mathsf{Act}_\tau \times \mathcal{D}(S)$.

In the literature essentially the same model has appeared under different names such as *NP-systems* [22], *probabilistic processes* [23], *simple probabilistic automata* [37], *probabilistic transition systems* [24] etc. Furthermore, there are strong structural similarities with *Markov Decision Processes* [31, 8].

A (non-probabilistic) labelled transition system (LTS) may be viewed as a degenerate pLTS, one in which only point distributions are used.

3.2 Lifting relations

In a pLTS actions are only performed by states, in that actions are given by relations from states to distributions. But in general we allow distributions over states to perform an action. For this purpose, we *lift* these relations so that they also apply to distributions [7].

Definition 3.2 (Lifting)**.** *Let $\mathcal{R} \subseteq S \times \mathcal{D}(S)$ be a relation from states to distributions in a pLTS. Then $\mathcal{R}^\dagger \subseteq \mathcal{D}(S) \times \mathcal{D}(S)$ is the smallest relation that satisfies*

(i) $s \mathrel{\mathcal{R}} \Theta$ implies $\overline{s} \mathrel{\mathcal{R}^\dagger} \Theta$, and

(ii) (Linearity) $\Delta_i \mathrel{\mathcal{R}^\dagger} \Theta_i$ for $i \in I$ implies $(\sum_{i\in I} p_i \cdot \Delta_i) \mathrel{\mathcal{R}^\dagger} (\sum_{i\in I} p_i \cdot \Theta_i)$ for any $p_i \in [0,1]$ with $\sum_{i\in I} p_i = 1$, where I is a finite index set.

There are numerous ways of formulating this concept of lifting relations. The following is particularly useful.

Lemma 3.3. *$\Delta \mathrel{\mathcal{R}^\dagger} \Theta$ if and only if there is a finite index set I such that*

(i) $\Delta = \sum_{i\in I} p_i \cdot \overline{s_i}$,

(ii) $\Theta = \sum_{i\in I} p_i \cdot \Theta_i$,

(iii) $s_i \mathrel{\mathcal{R}} \Theta_i$ for each $i \in I$.

Proof. ($\Leftarrow$) Suppose there is an index set I such that (i) $\Delta = \sum_{i\in I} p_i \cdot \overline{s_i}$, (ii) $\Theta = \sum_{i\in I} p_i \cdot \Theta_i$, and (iii) $s_i \mathrel{\mathcal{R}} \Theta_i$ for each $i \in I$. By (iii) and the first rule in Definition 3.2, we have $\overline{s_i} \mathrel{\mathcal{R}^\dagger} \Theta_i$ for each $i \in I$. By the second rule in Definition 3.2 we obtain that $(\sum_{i\in I} p_i \cdot \overline{s_i}) \mathrel{\mathcal{R}^\dagger} (\sum_{i\in I} p_i \cdot \Theta_i)$, that is $\Delta \mathrel{\mathcal{R}^\dagger} \Theta$.

($\Rightarrow$) We proceed by rule induction.

- If $\Delta \mathrel{\mathcal{R}^\dagger} \Theta$ because of $\Delta = \overline{s}$ and $s \mathrel{\mathcal{R}} \Theta$, then we can simply take I to be the singleton set $\{i\}$ with $p_i = 1$ and $\Theta_i = \Theta$.
- If $\Delta \mathrel{\mathcal{R}^\dagger} \Theta$ because of the conditions $\Delta = \sum_{i\in I} p_i \cdot \Delta_i$, $\Theta_i = \sum_{i\in I} p_i \cdot \Theta_i$ for some index set I, and $\Delta_i \mathrel{\mathcal{R}^\dagger} \Theta_i$ for each $i \in I$, then by induction hypothesis there are index sets J_i such that $\Delta_i = \sum_{j\in J_i} p_{ij} \cdot \overline{s_{ij}}$, $\Theta_i = \sum_{j\in J_i} p_{ij} \cdot \Theta_{ij}$, and $s_{ij} \mathrel{\mathcal{R}} \Theta_{ij}$ for each $i \in I$ and $j \in J_i$. It follows that $\Delta = \sum_{i\in I} \sum_{j\in J_i} p_i p_{ij} \cdot \overline{s_{ij}}$, $\Theta = \sum_{i\in I} \sum_{j\in J_i} p_i p_{ij} \cdot \Theta_{ij}$, and $s_{ij} \mathrel{\mathcal{R}} \Theta_{ij}$ for each $i \in I$ and $j \in J_i$. So it suffices to take $\{ij \mid i \in I, j \in J_i\}$ to be the index set and $\{p_i p_{ij} \mid i \in I, j \in J_i\}$ be the collection of probabilities.

$\square$

We apply this operation to the relations $\xrightarrow{\alpha}$ in the pLTS for $\alpha \in \mathsf{Act}_\tau$, where we also write $\xrightarrow{\alpha}$ for $(\xrightarrow{\alpha})^\dagger$. Thus as source of a relation $\xrightarrow{\alpha}$ we now also allow distributions. But note that $\overline{s} \xrightarrow{\alpha} \Delta$ is more general than $s \xrightarrow{\alpha} \Delta$. In papers such as [38, 6] the former is refered to as a *combined transition* because if $\overline{s} \xrightarrow{\alpha} \Delta$ then there is a collection of distributions Δ_i and probabilities p_i such that $s \xrightarrow{\alpha} \Delta_i$ for each $i \in I$ and $\Delta = \sum_{i\in I} p_i \cdot \Delta_i$ with $\sum_{i\in I} p_i = 1$.

In Definition 3.2, linearity tells us how to compare two linear combinations of distributions. Sometimes we need a dual notion of decomposition. Intuitively, if a relation $\mathcal{R}$ is *left-decomposable* and $\Delta \mathrel{\mathcal{R}} \Theta$, then for any decomposition of Δ there exists some corresponding decomposition of Θ.

Definition 3.4 (Left-decomposable)**.** *A binary relation over distributions, $\mathcal{R} \subseteq \mathcal{D}(S) \times \mathcal{D}(S)$, is called* left-decomposable *if $(\sum_{i\in I} p_i \cdot \Delta_i) \mathrel{\mathcal{R}} \Theta$, where I is a finite index set, implies that Θ can be written as $(\sum_{i\in I} p_i \cdot \Theta_i)$ such that $\Delta_i \mathrel{\mathcal{R}} \Theta_i$ for every $i \in I$.*

Proposition 3.5. *For any $\mathcal{R} \subseteq S \times \mathcal{D}(S)$ the relation $\mathcal{R}^\dagger$ over distributions is left-decomposable.*

Proof. Suppose $\Delta = (\sum_{i\in I} p_i \cdot \Delta_i)$ and $\Delta \ \mathcal{R}^\dagger \ \Theta$. We have to find a family of Θ_i such that

(i) $\Delta_i \ \mathcal{R}^\dagger \ \Theta_i$ for each $i \in I$,

(ii) $\Theta = \sum_{i\in I} p_i \cdot \Theta_i$.

From the alternative characterisation of lifting, Lemma 3.3, we know that

$$\Delta = \sum_{j\in J} q_j \cdot \overline{s_j} \qquad s_j \ \mathcal{R} \ \Theta^j \qquad \Theta = \sum_{j\in J} q_j \cdot \Theta^j$$

Define Θ_i to be

$$\sum_{s\in\lceil\Delta_i\rceil} \Delta_i(s) \cdot (\sum_{\{\, j\in J \,|\, s=s_j \,\}} \frac{q_j}{\Delta(s)} \cdot \Theta^j)$$

Note that $\Delta(s)$ can be written as $\sum_{\{\, j\in J \,|\, s=s_j \,\}} q_j$ and therefore

$$\Delta_i = \sum_{s\in\lceil\Delta_i\rceil} \Delta_i(s) \cdot (\sum_{\{\, j\in J \,|\, s=s_j \,\}} \frac{q_j}{\Delta(s)} \cdot \overline{s_j})$$

Since $s_j \ \mathcal{R} \ \Theta_j$ this establishes (i) above.

To establish (ii) above let us first abbreviate the sum $\sum_{\{\, j\in J \,|\, s=s_j \,\}} \frac{q_j}{\Delta(s)} \cdot \Theta^j$ to $X(s)$. Then $\sum_{i\in I} p_i \cdot \Theta_i$ can be written as

$$\begin{array}{rl} & \sum_{s\in\lceil\Delta\rceil} \sum_{i\in I} p_i \cdot \Delta_i(s) \cdot X(s) \\ = & \sum_{s\in\lceil\Delta\rceil} (\sum_{i\in I} p_i \cdot \Delta_i(s)) \cdot X(s) \\ = & \sum_{s\in\lceil\Delta\rceil} \Delta(s) \cdot X(s) \end{array}$$

The last equation is justified by the fact that $\Delta(s) = \sum_{i\in I} p_i \cdot \Delta_i(s)$.

Now $\Delta(s) \cdot X(s) = \sum_{\{\, j\in J \,|\, s=s_j \,\}} q_j \cdot \Theta^j$ and therefore we have

$$\begin{array}{ll} \sum_{i\in I} p_i \cdot \Theta_i & = \sum_{s\in\lceil\Delta\rceil} \sum_{\{\, j\in J \,|\, s=s_j \,\}} q_j \cdot \Theta^j \\ & = \sum_{j\in J} q_j \cdot \Theta^j \\ & = \Theta \end{array}$$

□

We write $s \xrightarrow{\hat{\tau}} \Delta$ if either $s \xrightarrow{\tau} \Delta$ or $\Delta = \overline{s}$, and $s \xrightarrow{\hat{a}} \Delta$ iff $s \xrightarrow{a} \Delta$ for $a \in \mathsf{Act}$. For any $a \in \mathsf{Act}_\tau$, we know that $\xrightarrow{\hat{a}} \subseteq S \times \mathcal{D}(S)$, so we can lift it to be a transition relation between distributions. With a slight abuse of notation we simply write $\Delta \xrightarrow{\hat{a}} \Theta$ for $\Delta \ (\xrightarrow{\hat{a}})^\dagger \ \Theta$. Then we define weak transitions $\xRightarrow{\hat{a}}$ by letting $\xRightarrow{\hat{\tau}}$ be the reflexive and transitive closure of $\xrightarrow{\hat{\tau}}$ and writing $\Delta \xRightarrow{\hat{a}} \Theta$ for $a \in \mathsf{Act}$ whenever $\Delta \xRightarrow{\hat{\tau}} \xrightarrow{\hat{a}} \xRightarrow{\hat{\tau}} \Theta$. If Δ is a point distribution, we often write $s \xRightarrow{\hat{a}} \Theta$ instead of $\overline{s} \xRightarrow{\hat{a}} \Theta$.

Proposition 3.6. *The action relations $\xRightarrow{\hat{\alpha}}$ are both linear and left-decomposable.*

Proof. It is easy to check that both properties are preserved by composition; that is if $\mathcal{R}_i, i = 1, 2$, are linear, left-decomposable respectively, then so is $\mathcal{R}_1 \cdot \mathcal{R}_2$. The result now follows since $\xRightarrow{\hat{\alpha}}$ is formed by repeated composition from two relations $\xrightarrow{\hat{\tau}}$ and $\xrightarrow{\hat{\alpha}}$ which we know are both linear and left-decomposable. □

Let $\mathcal{R} \subseteq S \times S$ be a relation between states. It induces a speical relation $\hat{\mathcal{R}} \subseteq S \times \mathcal{D}(S)$ between states and distributions:

$$\hat{\mathcal{R}} := \{(s, \overline{t}) \mid s \ \mathcal{R} \ t\}.$$

Then we can use Definition 3.2 to lift $\hat{\mathcal{R}}$ to be a relation $(\hat{\mathcal{R}})^\dagger$ between distributions. For simplicity, we combine the above two lifting operations and directly write $\mathcal{R}^\dagger$ for $(\hat{\mathcal{R}})^\dagger$ in the sequel, with the intention that a relation between states can be lifted to a relation between distributions via a special application of Definition 3.2. Consequently, we have the following corollary of Lemma 3.3.

Corollary 3.7. *Suppose $\mathcal{R} \subseteq S \times S$. Then $\Delta\ \mathcal{R}^\dagger\ \Theta$ if and only if there is a finite index set I such that*

(i) $\Delta = \sum_{i \in I} p_i \cdot \overline{s_i}$,

(ii) $\Theta = \sum_{i \in I} p_i \cdot \overline{t_i}$,

(iii) $s_i\ \mathcal{R}\ t_i$ *for each* $i \in I$.

Relations over distributions obtained by *lifting* enjoy some very useful properties. The following one will be used in Section 5 to show the transitivity of open bisimilarity.

Proposition 3.8. *Let $\mathcal{R}_1, \mathcal{R}_2 \subseteq S \times S$ be two binary relations. The forward relation $(\mathcal{R}_1 \cdot \mathcal{R}_2)^\dagger$ coincides with ${\mathcal{R}_1}^\dagger \cdot {\mathcal{R}_2}^\dagger$.*

Proof. We first show that $(\mathcal{R}_1 \cdot \mathcal{R}_2)^\dagger \ \subseteq\ {\mathcal{R}_1}^\dagger \cdot {\mathcal{R}_2}^\dagger$. Suppose there are two distributions Δ_1, Δ_2 such that $\Delta_1\ (\mathcal{R}_1 \cdot \mathcal{R}_2)^\dagger\ \Delta_2$. Then we have that

$$\Delta_1 = \sum_{i \in I} p_i \cdot \overline{s_i}, \qquad s_i\ \ \mathcal{R}_1 \cdot \mathcal{R}_2\ \ s_i', \qquad \Delta_2 = \sum_{i \in I} p_i \cdot \overline{s_i'}\ . \tag{2}$$

The middle part of (2) implies the existence of some states t_i such that $s_i\ \mathcal{R}_1\ t_i$ and $t_i\ \mathcal{R}\ s_i'$. Let Θ be the distribution $\sum_{i \in I} p_i \cdot \overline{t_i}$. It is clear that $\Delta_1\ {\mathcal{R}_1}^\dagger\ \Theta$ and $\Theta\ {\mathcal{R}_2}^\dagger\ \Delta_2$. It follows that $\Delta_1\ {\mathcal{R}_1}^\dagger \cdot {\mathcal{R}_2}^\dagger\ \Delta_2$.

Then we show the inverse inclusion ${\mathcal{R}_1}^\dagger \cdot {\mathcal{R}_2}^\dagger \ \subseteq\ (\mathcal{R}_1 \cdot \mathcal{R}_2)^\dagger$. Given three distributions $\Delta_1, \Delta_2, \Delta_3$, we show that if $\Delta_1\ {\mathcal{R}_1}^\dagger\ \Delta_2$ and $\Delta_2\ {\mathcal{R}_2}^\dagger\ \Delta_3$ then $\Delta_1\ (\mathcal{R}_1 \cdot \mathcal{R}_2)^\dagger\ \Delta_3$.

First $\Delta_1\ {\mathcal{R}_1}^\dagger\ \Delta_2$ means that

$$\Delta_1 = \sum_{i \in I} p_i \cdot \overline{s_i}, \qquad s_i\ \ \mathcal{R}_1\ \ s_i', \qquad \Delta_2 = \sum_{i \in I} p_i \cdot \overline{s_i'}. \tag{3}$$

Then from $\Delta_2\ {\mathcal{R}_2}^\dagger\ \Delta_3$ and Proposition 3.5, we have $\Delta_3 = \sum_{i \in I} p_i \cdot \Theta_i$ with $\overline{s_i'}\ {\mathcal{R}_2}^\dagger\ \Theta_i$ for each $i \in I$. Now by Corollary 3.7, Θ_i can be further decomposed as $\Theta_i = \sum_{j \in J_i} q_{ij} \cdot \overline{t_{ij}}$ such that $s_i'\ \mathcal{R}_2\ t_{ij}$ for each $j \in J_i$. In summary, we have

$$\Delta_1 = \sum_{i \in I} p_i \cdot \sum_{j \in J_i} q_{ij} \cdot \overline{s_i}, \qquad \text{and} \qquad \Delta_3 = \sum_{i \in I} p_i \cdot \sum_{j \in J_i} q_{ij} \cdot \overline{t_{ij}}. \tag{4}$$

Finally, it follows from (4) and the fact $s_i\ \mathcal{R}_1\ s_i'\ \mathcal{R}_2\ t_{ij}$ that $\Delta_1\ (\mathcal{R}_1 \cdot \mathcal{R}_2)^\dagger\ \Delta_3$. $\square$

4 Quantum CCS

We introduce the language qCCS which was originally studied in [9, 41, 10]. Three types of data are considered in qCCS: as classical data we have `Bool` for booleans and `Real` for real numbers, and as quantum data we have `Qbt` for qubits. Consequently, two countably infinite sets of variables are assumed: $cVar$ for classical variables, ranged over by $x, y, ...$, and $qVar$ for quantum variables, ranged over by $q, r, ...$ We assume a set Exp, which includes $cVar$ as a subset and is ranged over by $e, e', \ldots$, of classical data expressions over `Real`, and a set of boolean-valued expressions $BExp$, ranged over by $b, b', \ldots$, with the usual boolean constants `true`, `false`, and operators $\neg$, $\wedge$, $\vee$, and $\rightarrow$. In particular, we let $e \bowtie e'$ be a boolean expression for any $e, e' \in Exp$ and $\bowtie \in \{>, <, \geq, \leq, =\}$. We further assume that only classical variables can occur free in both data expressions and boolean expressions. Two types of channels are used: $cChan$ for classical channels, ranged over by $c, d, ...$, and $qChan$ for quantum channels, ranged over by $\mathtt{c}, \mathtt{d}, ...$ A relabelling function f is a map on $cChan \cup qChan$ such that $f(cChan) \subseteq cChan$ and $f(qChan) \subseteq qChan$. Sometimes we abbreviate a sequence of distinct variables $q_1, ..., q_n$ into $\tilde{q}$.

The terms in qCCS are given by:

$$\begin{aligned} P, Q \quad ::= \quad & \textbf{nil} \ \mid\ \tau.P \ \mid\ c?x.P \ \mid\ c!e.P \ \mid\ \mathtt{c}?q.P \ \mid\ \mathtt{c}!q.P \ \mid\ \mathcal{E}[\tilde{q}].P \ \mid\ M[\tilde{q}; x].P \\ & \mid\ P + Q \ \mid\ P \,||\, Q \ \mid\ P[f] \ \mid\ P \backslash L \ \mid\ \textbf{if}\ b\ \textbf{then}\ P \ \mid\ A(\tilde{q}; \tilde{x}) \end{aligned}$$

where f is a relabelling function and $L \subseteq cChan \cup qChan$ is a set of channels. Most of the constructors are standard as in CCS [28]. We briefly explain a few new constructors. The process $\mathtt{c}?q.P$ receives a quantum datum along quantum channel $\mathtt{c}$ and evolves into P. The process $\mathtt{c}!q.P$ sends out a quantum datum along quantum channel $\mathtt{c}$ before evolving into P. The new symbols $\mathcal{E}$ and M represent respectively a trace-preserving super-operator and a non-degenerate projective measurement applying on the Hilbert space associated with the systems $\tilde{q}$.

Free classical variables can be defined in the usual way, except for the fact that the variable x in the quantum measurement $M[\tilde{q}; x]$ is bound. A process P is closed if it contains no free classical variable, i.e. $fv(P) = \emptyset$.

The set of free quantum variables for process P, denoted by $qv(P)$ can be inductively defined as follows.

$$
\begin{array}{rclrcl}
qv(\textsf{nil}) & = & \emptyset & qv(\tau.P) & = & qv(P) \\
qv(c?x.P) & = & qv(P) & qv(c!e.P) & = & qv(P) \\
qv(\mathtt{c}?q.P) & = & qv(P) - \{q\} & qv(\mathtt{c}!q.P) & = & qv(P) \cup \{q\} \\
qv(\mathcal{E}[\tilde{q}].P) & = & qv(P) \cup \tilde{q} & qv(M[\tilde{q}; x].P) & = & qv(P) \cup \tilde{q} \\
qv(P + Q) & = & qv(P) \cup qv(Q) & qv(P \mid\mid Q) & = & qv(P) \cup qv(Q) \\
qv(P[f]) & = & qv(P) & qv(P \backslash L) & = & qv(P) \\
qv(\textbf{if } b \textbf{ then } P) & = & qv(P) & qv(A(\tilde{q}; \tilde{x})) & = & \tilde{q}.
\end{array}
$$

For a process to be legal, we require that

1. $q \notin qv(P)$ in the process $\mathtt{c}!q.P$;
2. $qv(P) \cap qv(Q) = \emptyset$ in the process $P \mid\mid Q$;
3. Each constant $A(\tilde{q}; \tilde{x})$ has a defining equation $A(\tilde{q}; \tilde{x}) := P$, where P is a term with $qv(P) \subseteq \tilde{q}$ and $fv(P) \subseteq \tilde{x}$.

The first condition says that a quantum system will not be referenced after it has been sent out. This is a requirement of quantum no-cloning theorem. The second condition says that parallel composition $\mid\mid$ models separate parties that never reference a quantum system simultaneously.

Throughout the paper we implicitly assume the convention that processes are identified up to α-conversion, bound variables differ from each other and they are different from free variables.

We now turn to the operational semantics of qCCS. For each quantum variable q we assume a 2-dimensional Hilbert space $\mathcal{H}_q$. For any nonempty subset $S \subseteq qVar$ we write $\mathcal{H}_S$ for the tensor product space $\bigotimes_{q \in S} \mathcal{H}_q$. In particular, $\mathcal{H} = \mathcal{H}_{qVar}$ is the state space of the whole environment consisting of all the quantum variables, which is a countably infinite dimensional Hilbert space.

Let P be a closed quantum process and ρ a density operator on $\mathcal{H}$, the pair $\langle P, \rho \rangle$ is called a *configuration*. We write *Con* for the set of all configurations, ranged over by $\mathcal{C}$ and $\mathcal{D}$. We interpret qCCS as a pLTS whose states are all the configurations definable in the language, and whose arrows are determined by the rules in Figure 1; we have omitted the obvious symmetric counterparts to the rules *(C-Com)*, *(Q-Com)*, *(Int)* and *(Sum)*. The set of actions Act takes the form

$$\{c?v, c!v \mid c \in cChan, v \in \mathtt{Real}\} \cup \{\mathtt{c}?r, \mathtt{c}!r \mid \mathtt{c} \in qChan, r \in qVar\}$$

The symbol τ denotes invisible actions. We write Act_τ for $\mathsf{Act} \cup \{\tau\}$, which is ranged over by α. We use $cn(\alpha)$ for the set of channel names in action α. So, for example, $cn(\mathtt{c}?x) = \{\mathtt{c}\}$ and $cn(\tau) = \emptyset$.

In the first eight rules in Figure 1, the targets of arrows are point distributions, and we use the slightly abbreviated form $\mathcal{C} \xrightarrow{\alpha} \mathcal{C}'$ to mean $\mathcal{C} \xrightarrow{\alpha} \overline{\mathcal{C}'}$.

The rules use the obvious extension of the function $\mid\mid$ on terms to configurations and distributions. To be precise, $\mathcal{C} \mid\mid P$ is the configuration $\langle Q \mid\mid P, \rho \rangle$ where $\mathcal{C} = \langle Q, \rho \rangle$, and $\Delta \mid\mid P$ is the distribution defined by:

$$(\Delta \mid\mid P)(\langle Q, \rho \rangle) = \begin{cases} \Delta(\langle Q', \rho \rangle) & \text{if } Q = Q' \mid\mid P \\ 0 & \text{otherwise.} \end{cases}$$

Similar extension applies to $\Delta[f]$ and $\Delta \backslash L$.

(Tau)

$$\langle \tau.P, \rho\rangle \xrightarrow{\tau} \langle P, \rho\rangle$$

(C-Inp)

$$\frac{v \in \texttt{Real}}{\langle c?x.P, \rho\rangle \xrightarrow{c?v} \langle P[v/x], \rho\rangle}$$

(C-Outp)

$$\frac{v = [\![e]\!]}{\langle c!e.P, \rho\rangle \xrightarrow{c!v} \langle P, \rho\rangle}$$

(C-Com)

$$\frac{\langle P_1, \rho\rangle \xrightarrow{c?v} \langle P_1', \rho\rangle \qquad \langle P_2, \rho\rangle \xrightarrow{c!v} \langle P_2', \rho\rangle}{\langle P_1 \,||\, P_2, \rho\rangle \xrightarrow{\tau} \langle P_1' \,||\, P_2', \rho\rangle}$$

(Q-inp)

$$\frac{r \notin qv(\texttt{c}?q.P)}{\langle \texttt{c}?q.P, \rho\rangle \xrightarrow{\texttt{c}?r} \langle P[r/q], \rho\rangle}$$

(Q-Outp)

$$\langle \texttt{c}!q.P, \rho\rangle \xrightarrow{\texttt{c}!q} \langle P, \rho\rangle$$

(Q-Com)

$$\frac{\langle P_1, \rho\rangle \xrightarrow{\texttt{c}?r} \langle P_1', \rho\rangle \qquad \langle P_2, \rho\rangle \xrightarrow{\texttt{c}!r} \langle P_2', \rho\rangle}{\langle P_1 \,||\, P_2, \rho\rangle \xrightarrow{\tau} \langle P_1' \,||\, P_2', \rho\rangle}$$

(Oper)

$$\langle \mathcal{E}[\tilde{q}].P, \rho\rangle \xrightarrow{\tau} \langle P, \mathcal{E}_{\tilde{q}}(\rho)\rangle$$

(Meas)

$$\frac{M = \sum_{i\in I} \lambda_i E^i \qquad p_i = tr(E^i_{\tilde{q}}\rho)}{\langle M[\tilde{q}; x].P, \rho\rangle \xrightarrow{\tau} \sum_{i\in I} p_i \langle P[\lambda_i/x], E^i_{\tilde{q}}\rho E^i_{\tilde{q}}/p_i\rangle}$$

(Int)

$$\frac{\langle P_1, \rho\rangle \xrightarrow{\alpha} \Delta \qquad qbv(\alpha) \cap qv(P_2) = \emptyset}{\langle P_1 \,||\, P_2, \rho\rangle \xrightarrow{\alpha} \Delta \,||\, P_2}$$

(Sum)

$$\frac{\langle P_1, \rho\rangle \xrightarrow{\alpha} \Delta}{\langle P_1 + P_2, \rho\rangle \xrightarrow{\alpha} \Delta}$$

(Rel)

$$\frac{\langle P, \rho\rangle \xrightarrow{\alpha} \Delta}{\langle P[f], \rho\rangle \xrightarrow{f(\alpha)} \Delta[f]}$$

(Res)

$$\frac{\langle P, \rho\rangle \xrightarrow{\alpha} \Delta \qquad cn(\alpha) \cap L = \emptyset}{\langle P\backslash L, \rho\rangle \xrightarrow{\alpha} \Delta\backslash L}$$

(Cho)

$$\frac{\langle P, \rho\rangle \xrightarrow{\alpha} \Delta \qquad [\![b]\!] = \texttt{true}}{\langle \textbf{if } b \textbf{ then } P, \rho\rangle \xrightarrow{\alpha} \Delta}$$

(Cons)

$$\frac{\langle P[\tilde{v}/\tilde{x}, \tilde{r}/\tilde{q}], \rho\rangle \xrightarrow{\alpha} \Delta \qquad A(\tilde{x}, \tilde{q}) := P}{\langle A(\tilde{v}, \tilde{r}), \rho\rangle \xrightarrow{\alpha} \Delta}$$

Figure 1: Operational semantics of qCCS

5 Open bisimulations

Let $\mathcal{C} = \langle P, \rho\rangle$. We use the notation $qv(\mathcal{C}) := qv(P)$ for free quantum variables and $\mathrm{ptr}(\mathcal{C}) := \mathrm{tr}_{qv(P)}(\rho)$ for partial traces. Let $\Delta = \sum_{i\in I} p_i \cdot \overline{\langle P_i, \rho_i\rangle}$. We write $\mathcal{E}(\Delta)$ for the distribution $\sum_{i\in I} p_i \cdot \overline{\langle P_i, \mathcal{E}(\rho_i)\rangle}$.

Definition 5.1. *A relation $\mathcal{R} \subseteq Con \times Con$ is a* strong open simulation *if $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$ implies that $qv(\mathcal{C}) = qv(\mathcal{D})$, $\mathrm{ptr}(\mathcal{C}) = \mathrm{ptr}(\mathcal{D})$, and for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$*

- *whenever $\mathcal{E}(\mathcal{C}) \xrightarrow{\alpha} \Delta$, there is some distribution Θ with $\mathcal{E}(\mathcal{D}) \xrightarrow{\alpha} \Theta$ and $\Delta\ \mathcal{R}^\dagger\ \Theta$.*

A relation $\mathcal{R}$ is a strong open bisimulation *if both $\mathcal{R}$ and $\mathcal{R}^{-1}$ are strong open simulations.*

The above definition is inspired by the work of Sangiorgi [36], where a notion of bisimulation is defined for the π-calculus by treating name instantiation in an "open" style. Here we deal with super-operator application in an "open" style, but the instantiation of variables is in an "early" style because the operational semantics given in Figure 1 is essentially an early semantics. For more variants of semantics, see e.g. [35].

In this paper we are mainly interested in a notion of weak open bisimulation which is like strong open bisimulation but internal transitions are abstracted away.

Definition 5.2. *A relation $\mathcal{R} \subseteq Con \times Con$ is a* weak open simulation *if $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$ implies that $qv(\mathcal{C}) = qv(\mathcal{D})$, $\mathrm{ptr}(\mathcal{C}) = \mathrm{ptr}(\mathcal{D})$, and for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$*

- *whenever $\mathcal{E}(\mathcal{C}) \xrightarrow{\alpha} \Delta$, there is some distribution Θ with $\mathcal{E}(\mathcal{D}) \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta \mathcal{R}^\dagger \Theta$.*

A relation $\mathcal{R}$ is a weak open bisimulation *if both $\mathcal{R}$ and $\mathcal{R}^{-1}$ are weak open simulations. We let $\approx_o$ be the largest weak open bisimulation. In the sequel we will simply use open bisimulation to refer to weak open bisimulation.*

Two quantum processes P and Q are bisimilar, denoted by $P \approx_o Q$, if for any quantum state $\rho \in \mathcal{D}(\mathcal{H})$ and any indexed set $\tilde{v}$ of classical values, we have

$$\langle P\{\tilde{v}/\tilde{x}\}, \rho\rangle \approx_o \langle Q\{\tilde{v}/\tilde{x}\}, \rho\rangle.$$

Here $\tilde{x}$ is the set of free classical variables contained in P and Q.

5.1 A useful proof technique

In Definition 5.2 super-operator application and transitions are considered at the same time. In fact, we can separate the two issues and approach the concept of open bisimulation in an incremental way, which turns out to be very useful when proving that two configurations are open bisimilar.

Definition 5.3. *A relation $\mathcal{R} \subseteq Con \times Con$ is closed under super-operator application if $\mathcal{C} \mathcal{R} \mathcal{D}$ implies $\mathcal{E}(\mathcal{C}) \mathcal{R} \mathcal{E}(\mathcal{D})$ for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$.*

Definition 5.4. *A relation $\mathcal{R} \subseteq Con \times Con$ is a* ground simulation *if $\mathcal{C} \mathcal{R} \mathcal{D}$ implies that $qv(\mathcal{C}) = qv(\mathcal{D})$,* $\mathrm{ptr}(\mathcal{C}) = \mathrm{ptr}(\mathcal{D})$*, and*

- *whenever $\mathcal{C} \xrightarrow{\alpha} \Delta$, there is some distribution Θ with $\mathcal{D} \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta \mathcal{R}^\dagger \Theta$.*

A relation $\mathcal{R}$ is a ground bisimulation *if both $\mathcal{R}$ and $\mathcal{R}^{-1}$ are ground simulations.*

Proposition 5.5. *Suppose that a relation $\mathcal{R}$*

1. *is a ground bisimulation, and*
2. *is closed under all super-operator application.*

Then $\mathcal{R}$ is an open bisimulation.

Proof. Suppose that $\mathcal{C} \mathcal{R} \mathcal{D}$. Since $\mathcal{R}$ is a ground bisimulation, we have $qv(\mathcal{C}) = qv(\mathcal{D})$ and $\mathrm{ptr}(\mathcal{C}) = \mathrm{ptr}(\mathcal{D})$. Since $\mathcal{R}$ is closed under all super-operator application, we have $\mathcal{E}(\mathcal{C}) \mathcal{R} \mathcal{E}(\mathcal{D})$ for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$. If $\mathcal{E}(\mathcal{C}) \xrightarrow{\alpha} \Delta$, then there exists some distribution Θ such that $\mathcal{E}(\mathcal{D}) \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta \mathcal{R}^\dagger \Theta$ because $\mathcal{R}$ is a ground bisimulation. Similarly, any transtion from $\mathcal{E}(\mathcal{D})$ can also be matched up by $\mathcal{E}(\mathcal{C})$. Therefore, $\mathcal{R}$ is an open bisimulation. $\square$

The above proposition provides us a useful proof technique: in order to show that two configurations $\mathcal{C}$ and $\mathcal{D}$ are open bisimilar, it sufficies to exhibit a binary relation including the pair $(\mathcal{C}, \mathcal{D})$, and then to check that the relation is a ground bisimulation and is closed under all super-operator application. This is analogous to a proof technique of open bisimulation for the π-calculus [36], where name instantiation is playing the same role as super-operator application here.

Proposition 5.6. *$\approx_o$ is the largest ground bisimulation that is closed under all super-operator application.*

Proof. By definition $\approx_o$ is closed under all super-operator application. It is is obviously a ground bisimulation. Moreover, it is the largest one because of Proposition 5.5. $\square$

5.2 Equivalence and congruence

As a sanity check, we prove that $\approx_o$ is an equivalence relation. This is based on the following transfer property.

Proposition 5.7. *Suppose $\Delta \approx_o{}^\dagger \Theta$ and $\Delta \xrightarrow{\alpha} \Delta'$ in a pLTS. Then there exists some distribution Θ' such that $\Theta \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta'$ and $\Delta' \approx_o{}^\dagger \Theta'$.*

Proof. Suppose $\Delta \approx_o{}^\dagger \Theta$ and $\Delta \xrightarrow{\alpha} \Delta'$. By Corollary 3.7, there is a finite index set I such that (i) $\Delta = \sum_{i\in I} p_i \cdot \overline{\mathcal{C}_i}$, (ii) $\Theta = \sum_{i\in I} p_i \cdot \overline{\mathcal{D}_i}$, and (iii) $\mathcal{C}_i \approx_o \mathcal{D}_i$ for each $i \in I$. By the condition $\Delta \xrightarrow{\alpha} \Delta'$, (i) and Proposition 3.5, we can decompose Δ' into $\sum_{i\in I} p_i \cdot \Delta'_i$ for some Δ'_i such that $\overline{\mathcal{C}_i} \xrightarrow{\alpha} \Delta'_i$. By Lemma 3.3 again, for each $i \in I$, there is an index set J_i such that $\Delta'_i = \sum_{j\in J_i} q_{ij} \cdot \Delta'_{ij}$ and $\mathcal{C}_i \xrightarrow{\alpha} \Delta'_{ij}$ for each $j \in J_i$ and $\sum_{j\in J_i} q_{ij} = 1$. By (iii) there is some Θ'_{ij} such that $\mathcal{D}_i \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta'_{ij}$ and $\Delta'_{ij} \approx_o{}^\dagger \Theta'_{ij}$. Let $\Theta' = \sum_{i\in I, j\in J_i} p_i q_{ij} \cdot \Theta'_{ij}$. Since $\stackrel{\hat{\alpha}}{\Longrightarrow}$ is linear by Proposition 3.6, we know that $\Theta = \sum_{i\in I} p_i \sum_{j\in J_i} q_{ij} \mathcal{D}_i \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta'$. By the linearity of $\approx_o{}^\dagger$, we notice that $\Delta' = (\sum_{i\in I} p_i \sum_{j\in J_i} q_{ij} \cdot \Delta'_{ij}) \approx_o{}^\dagger \Theta'$. □

Corollary 5.8. *Suppose $\Delta \approx_o{}^\dagger \Theta$ and $\Delta \stackrel{\hat{\alpha}}{\Longrightarrow} \Delta'$. Then there is some Θ' with $\Theta \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta'$ and $\Delta' \approx_o{}^\dagger \Theta'$.*

Proof. By Proposition 5.7 it is not difficult to show that

(*) If $\Delta \approx_o{}^\dagger \Theta$ and $\Delta \stackrel{\hat{\tau}}{\Longrightarrow} \Delta'$ then there is some Θ' with $\Theta \stackrel{\hat{\tau}}{\Longrightarrow} \Theta'$ and $\Delta' \approx_o{}^\dagger \Theta'$.

Suppose $\Delta \stackrel{\hat{\alpha}}{\Longrightarrow} \Delta'$ and $\Delta \approx_o{}^\dagger \Theta$. If α is τ then the required Θ' follows by an application of property (*). Otherwise, by definition we know $\Delta \stackrel{\hat{\tau}}{\Longrightarrow} \Delta_1$, $\Delta_1 \xrightarrow{\alpha} \Delta_2$ and $\Delta_2 \stackrel{\hat{\tau}}{\Longrightarrow} \Delta'$. An application of property (*) gives a Θ_1 such that $\Theta \stackrel{\hat{\tau}}{\Longrightarrow} \Theta_1$ and $\Delta_1 \approx_o{}^\dagger \Theta_1$. An application of Proposition 5.7 gives a Θ_2 such that $\Theta_1 \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta_2$ and $\Delta_2 \approx_o{}^\dagger \Theta_2$. Finally another application of property (*) gives $\Theta_2 \stackrel{\hat{\tau}}{\Longrightarrow} \Theta'$ such that $\Delta' \approx_o{}^\dagger \Theta'$. The result now follows from the transitivity of $\stackrel{\hat{\tau}}{\Longrightarrow}$. □

Theorem 5.9. *$\approx_o$ is an equivalence relation.*

Proof. It is trivial to see that $\approx_o$ is reflexive and symmetric. For transitivity, we show that $\approx_o \cdot \approx_o$ is an open bisimulation relation. Since this is a symmetric relation, we only need to show that it is an open simulation. Suppose $\mathcal{C}_1 \approx_o \mathcal{C}_2$ and $\mathcal{C}_2 \approx_o \mathcal{C}_3$. If $\mathcal{C}_1 \xrightarrow{\alpha} \Delta_1$, then there is some $\mathcal{C}_2 \stackrel{\hat{\alpha}}{\Longrightarrow} \Delta_2$ such that $\Delta_1 \approx_o{}^\dagger \Delta_2$, since $\mathcal{C}_1 \approx_o \mathcal{C}_2$. From the condition $\mathcal{C}_2 \approx_o \mathcal{C}_3$ and Corollary 5.8 it follows that $\mathcal{C}_3 \stackrel{\hat{\alpha}}{\Longrightarrow} \Delta_3$ and $\Delta_2 \approx_o{}^\dagger \Delta_3$. By Proposition 3.8 we see that $\Delta_1 (\approx_o \cdot \approx_o)^\dagger \Delta_3$ as required. □

As a relation between configurations, $\approx_o$ is preserved by all static constructors.

Proposition 5.10. *If $\langle P, \rho\rangle \approx_o \langle Q, \sigma\rangle$ then*

1. *$\langle P\|R, \rho\rangle \approx_o \langle Q\|R, \sigma\rangle$;*
2. *$\langle P[f], \rho\rangle \approx_o \langle Q[f], \sigma\rangle$;*
3. *$\langle P\backslash L, \rho\rangle \approx_o \langle Q\backslash L, \sigma\rangle$;*
4. *$\langle \textbf{if } b \textbf{ then } P, \rho\rangle \approx_o \langle \textbf{if } b \textbf{ then } Q, \sigma\rangle$.*

Proof. We only prove (1) as an example. Let

$$\mathcal{R} = \{(\langle P\|R, \rho\rangle, \langle Q\|R, \sigma\rangle) \mid \langle P, \rho\rangle \approx_o \langle Q, \sigma\rangle\}.$$

It suffices to show that $\mathcal{R}$ is an open bisimulation. Suppose $\langle P\|R, \rho\rangle \mathcal{R} \langle Q\|R, \sigma\rangle$ where $\langle P, \rho\rangle \approx_o \langle Q, \sigma\rangle$. By the definition of $\approx_o$ we have that $qv(P) = qv(Q)$ and $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$. Thus $qv(P\|R) = qv(Q\|R)$ and we infer that

$$\mathrm{tr}_{qv(P\|R)}(\rho) \;=\; \mathrm{tr}_{qv(P\|R)\backslash qv(P)}\mathrm{tr}_{qv(P)}(\rho) \;=\; \mathrm{tr}_{qv(Q\|R)\backslash qv(Q)}\mathrm{tr}_{qv(Q)}(\sigma) \;=\; \mathrm{tr}_{qv(Q\|R)}(\sigma).$$

By Proposition 5.6, we know that $\langle P, \mathcal{E}(\rho)\rangle \approx_o \langle Q, \mathcal{E}(\sigma)\rangle$ for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(P)}})$, from which it follows that $\langle P \mid\mid R, \mathcal{E}(\rho)\rangle \ \mathcal{R}\ \langle Q \mid\mid R, \mathcal{E}(\sigma)\rangle$ for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(P||R)}})$. In other words, $\mathcal{R}$ is closed under super-operator application. Below we show that it is also a ground bisimulation.

Suppose$\langle P\|R, \rho\rangle \xrightarrow{\alpha} \Delta$ for some α and Δ. There are three cases to consider.

1. The transition is caused by R solely; that is, $\langle R, \rho\rangle \xrightarrow{\alpha} \sum_i p_i \cdot \overline{\langle R_i, \mathcal{E}_i(\rho)\rangle}$, and $\Delta = \sum_i p_i \cdot \overline{\langle P\|R_i, \mathcal{E}_i(\rho)\rangle}$. Then
$$\langle Q\|R, \sigma\rangle \xrightarrow{\alpha} \Theta = \sum_i p_i \cdot \overline{\langle Q\|R_i, \mathcal{E}_i(\sigma)\rangle}.$$
Furthermore, by Proposition 5.6, we have $\langle P, \mathcal{E}_i(\rho)\rangle \approx_o \langle Q, \mathcal{E}_i(\sigma)\rangle$, and then $\Delta \ \mathcal{R}^\dagger\ \Theta$ by definition.

2. The transition is caused by P solely; that is, $\langle P, \rho\rangle \xrightarrow{\alpha} \Delta_1 = \sum_i p_i \cdot \overline{\langle P_i, \rho_i\rangle}$, and $\Delta = \sum_i p_i \cdot \overline{\langle P_i\|R, \rho_i\rangle}$. Since $\langle P, \rho\rangle \approx_o \langle Q, \sigma\rangle$. Then $\langle Q, \sigma\rangle \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta_1$ such that $\Delta_1 \approx_o{}^\dagger\ \Theta_1$. By Proposition 3.5, we have the decomposition $\Theta_1 = \sum_i p_i \cdot \Theta_i$ with $\overline{\langle P_i, \rho_i\rangle} \approx_o{}^\dagger\ \Theta_i$ for each i. So we have
$$\langle Q\|R, \sigma\rangle \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta = \sum_i p_i \cdot \Theta_i\|R$$
and $\Delta \ \mathcal{R}^\dagger\ \Theta$ by definition.

3. The transition is caused by a communication between P and R. Without loss of generality, we assume that
$$\langle P, \rho\rangle \xrightarrow{\mathtt{c}?q} \langle P', \rho\rangle, \quad \langle R, \rho\rangle \xrightarrow{\mathtt{c}!q} \langle R', \rho\rangle,$$
and $\Delta = \langle P'\|R', \rho\rangle$. By a simple induction on the rules in Figure 1, it is easy to see that $\langle R, \eta\rangle \xrightarrow{\mathtt{c}!q} \langle R', \eta\rangle$ for any $\eta \in \mathcal{D}(\mathcal{H})$.

   From the assumption that $\langle P, \rho\rangle \approx_o \langle Q, \sigma\rangle$, we have
$$\langle Q, \sigma\rangle \stackrel{\mathtt{c}?q}{\Longrightarrow} \sum_{i\in I} p_i \cdot \overline{\langle Q_i, \sigma_i\rangle}$$
such that for any $i \in I$, it holds that $\langle P', \rho\rangle \approx_o \langle Q_i, \sigma_i\rangle$ and
$$\langle Q\|R, \sigma\rangle \stackrel{\tau}{\Longrightarrow} \Theta = \sum_{i\in I} p_i \cdot \overline{\langle Q_i\|R', \sigma_i\rangle}.$$
Furthermore, for any $i \in I$, we have
$$(\langle P'\|R', \rho\rangle, \langle Q_i\|R', \sigma_i\rangle) \in \mathcal{R}$$
by definition. That is, $\Delta \ \mathcal{R}^\dagger\ \Theta$ as required.

The symmetric form when $\langle Q\|R, \mathcal{E}(\sigma)\rangle \xrightarrow{\alpha} \Theta$ can be similarly proved. So $\mathcal{R}$ is a ground bisimulation on Con. It follows from Proposition 5.5 that $\mathcal{R}$ is also an open bisimulation. □

Note that we do not have a counterpart of the above proposition for dynamic constructors such as prefix. As a counterexample, consider the following two configurations taken from [10]:
$$\langle P, \rho\rangle \qquad \text{and} \qquad \langle Q, \rho\rangle$$
where $P = M_{0,1}[q; x].\mathbf{nil}$ with $M_{0,1} = \lambda_0[|0\rangle] + \lambda_1[|1\rangle]$ being the 1-qubit measurement according to the computational basis, $Q = I[q].\mathbf{nil}$, and $\rho = [|0\rangle]_q \otimes \sigma$ with $\sigma \in \mathcal{D}(\mathcal{H}_{\overline{q}})$. We have that $\langle P, \rho\rangle \approx_o \langle Q, \rho\rangle$, but $\langle H[q].P, \rho\rangle \not\approx_o \langle H[q].Q, \rho\rangle$ when H is the Hadamard operator.

Nevertheless, as a relation between processes, $\approx_o$ is preserved by almost all constructors of qCCS.

Theorem 5.11. *The relation $\approx_o$ between processes is preserved by all the constructors of qCCS except for summation.*

Proof. Similar to the proof of Theorem 6.17 in [10], which shows the congruence property of a notion of weak bisimulation. □

5.3 An extensional equivalence

We formally define three criteria, namely barb-preservation, reduction-closedness and composionality, in order to judge whether two processes are equivalent. This yields an extensional equivalence that turns out to coincide with open bisimilarity.

Definition 5.12 (Barbs). *For $\Delta \in \mathcal{D}(Con)$ and $c \in cChan$ let*

$$V_c(\Delta) = \sum\{\Delta(\mathcal{C}) \mid \mathcal{C} \xrightarrow{c!v} \text{ for some } v\}.$$

We write $\mathcal{C} \Downarrow_c^{\geq p}$ whenever $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ for some Δ with $V_c(\Delta) \geq p$.

Definition 5.13. *A relation $\mathcal{R}$ is*

- barb-preserving *if $\mathcal{C} \mathrel{\mathcal{R}} \mathcal{D}$ implies that $\mathcal{C} \Downarrow_c^{\geq p}$ iff $\mathcal{D} \Downarrow_c^{\geq p}$ for any classical channel c;*
- reduction-closed *if $\mathcal{C} \mathrel{\mathcal{R}} \mathcal{D}$ implies*
  - *whenever $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$, there exists Θ such that $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$ and $\Delta \mathrel{\mathcal{R}^\dagger} \Theta$,*
  - *whenever $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$, there exists Δ such that $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ and $\Delta \mathrel{\mathcal{R}^\dagger} \Theta$;*
- compositional *if $\mathcal{C} \mathrel{\mathcal{R}} \mathcal{D}$ implies $(\mathcal{C}||R) \mathrel{\mathcal{R}} (\mathcal{D}||R)$ for any process R with $qv(R)$ disjoint from $qv(\mathcal{C}) \cup qv(\mathcal{D})$, and $\mathcal{R}$ is closed under super-operator application.*

Definition 5.14 (Reduction barbed congruence). *Let* reduction barbed congruence*, denoted by $\approx_r$, be the largest relation over configurations which is barb-preserving, reduction-closed and compositional, and furthermore, if $\mathcal{C} \approx_r \mathcal{D}$ then $qv(\mathcal{C}) = qv(\mathcal{D})$ and $\mathrm{ptr}(\mathcal{C}) = \mathrm{ptr}(\mathcal{D})$.*

Theorem 5.15 (Soundness). *If $\mathcal{C} \approx_o \mathcal{D}$ then $\mathcal{C} \approx_r \mathcal{D}$.*

Proof. By Corollary 5.8 and Proposition 5.10 we know that $\approx_o$ is reduction closed and compositional. It remains to show that $\approx_o$ is barb-preserving.

Suppose $\mathcal{C} \approx_o \mathcal{D}$ and $\mathcal{C} \Downarrow_c^{\geq p}$, for any classical channel c and probability p; we need to show that $\mathcal{D} \Downarrow_c^{\geq p}$. We see from $\mathcal{C} \Downarrow_c^{\geq p}$ that $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ for some Δ with $V_c(\Delta) \geq p$. By Corollary 5.8, the relation $\approx_o$ is reduction-closed. Hence, there exists Θ such that $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$ and $\Delta \approx_o{}^\dagger \Theta$. The latter means that

$$\Delta = \sum_{i \in I} p_i \cdot \overline{\mathcal{C}_i} \qquad \mathcal{C}_i \approx_o \mathcal{D}_i \qquad \Theta = \sum_{i \in I} p_i \cdot \overline{\mathcal{D}_i} \tag{5}$$

By the second part of (5), if $\mathcal{C}_i \xrightarrow{c!v}$ for some action $c!v$, then $\mathcal{D}_i \stackrel{c!v}{\Longrightarrow}$, that is $\mathcal{D}_i \stackrel{\hat{\tau}}{\Longrightarrow} \Theta_i \xrightarrow{c!v}$ for some distribution Θ_i. Let I_c be the index set $\{i \in I \mid \mathcal{C}_i \xrightarrow{c!v} \text{ for some } v\}$, and Θ' be the distribution

$$(\sum_{i \in I_c} p_i \cdot \Theta_i) + (\sum_{i \in I \setminus I_c} p_i \cdot \overline{\mathcal{D}_i}).$$

By the linearity and reflexivity of $\stackrel{\hat{\tau}}{\Longrightarrow}$, Proposition 3.6, we have $\Theta \stackrel{\hat{\tau}}{\Longrightarrow} \Theta'$. It follows from $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta \stackrel{\hat{\tau}}{\Longrightarrow} \Theta'$ that $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta'$. It remains to show that $V_c(\Theta') \geq p$.

Note that for each $i \in I_c$ we have $\Theta_i \xrightarrow{c!v}$ for some action $c!v$, which means that $V_c(\Theta_i) = 1$. It follows that

$$\begin{array}{rcl} V_c(\Theta') & = & \sum_{i \in I_c} p_i \cdot V_c(\Theta_i) + \sum_{i \in I \setminus I_c} p_i \cdot V_c(\overline{\mathcal{D}_i}) \\ & \geq & \sum_{i \in I_c} p_i \cdot V_c(\Theta_i) \\ & = & \sum_{i \in I_c} p_i \\ & = & V_c(\Delta) \\ & \geq & p \end{array}$$

$\square$

In order to obtain completeness, the converse of Theorem 5.15, we make use of a proof technique that involves examing the barbs of processes in certain contexts; the following technical lemma enhances this technique.

Lemma 5.16. *If $\Delta||c!0 \approx_r{}^\dagger \Theta||c!0$ where c is a fresh classical channel, then $\Delta \approx_r{}^\dagger \Theta$.*

Proof. Consider the relation

$$\mathcal{R}= \{(\mathcal{C}, \mathcal{D}) \mid \mathcal{C}||c!0 \approx_r \mathcal{D}||c!0 \text{ for some fresh channel } c\}$$

We show that $\mathcal{R} \subseteq \approx_r$. Suppose $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$. Then there is a fresh channel c such that $\mathcal{C}||c!0 \approx_r \mathcal{D}||c!0$. Let $\mathcal{C} = \langle P, \rho\rangle$ and $\mathcal{D} = \langle Q, \sigma\rangle$. By the definition of $\approx_r$ we have $qv(P||c!0) = qv(Q||c!0)$ and $\mathrm{ptr}(\mathcal{C}||c!0) = \mathrm{ptr}(\mathcal{D}||c!0)$, i.e. $\mathrm{tr}_{qv(P||c!0)}(\rho) = \mathrm{tr}_{qv(Q||c!0)}(\sigma)$. Notice that

$$qv(P) \ = \ qv(P||c!0) \ = \ qv(Q||c!0) \ = \ qv(Q).$$

It follows that

$$\mathrm{ptr}(\mathcal{C}) = \mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(P||c!0)}(\rho) = \mathrm{tr}_{qv(Q||c!0)}(\sigma) = \mathrm{ptr}(\mathcal{D}).$$

Below we check that $\mathcal{R}$ is compositional, barb-preserving and reduction-closed.

1. $\mathcal{R}$ is compositional. For any process R with $qv(R)$ disjoint from $qv(\mathcal{C})$ and c fresh for R, since $\approx_r$ is compositional, we have $(\mathcal{C}||c!0||R) \approx_r (\mathcal{D}||c!0||R)$, which means $(\mathcal{C}||R)\ \mathcal{R}\ (\mathcal{D}||R)$. By the compositionality of $\approx_r$ we also have $\mathcal{E}(\mathcal{C} \mid\mid c!0) \approx_r \mathcal{E}(\mathcal{D} \mid\mid c!0)$ for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C}||c!0)}})$. Since $qv(\mathcal{C}) = qv(\mathcal{C} \mid\mid c!0)$, we have $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$. Note that

   $$\mathcal{E}(\mathcal{C}) \mid\mid c!0 \ = \ \mathcal{E}(\mathcal{C} \mid\mid c!0) \ \approx_r \ \mathcal{E}(\mathcal{D} \mid\mid c!0) \ = \ \mathcal{E}(\mathcal{D}) \mid\mid c!0.$$

   It follows that $\mathcal{E}(\mathcal{C})\ \mathcal{R}\ \mathcal{E}(\mathcal{D})$ and thus $\mathcal{R}$ is closed under super-operator application.

2. $\mathcal{R}$ is barb-preserving. Suppose $\mathcal{C} \Downarrow_{c_1}^{\geq p}$ for some channel c_1 and probability p. Let c_2 be some fresh channel. We construct the process T by letting

   $$T \ = \ c_1?x_1.c?x.c_2!0$$

   for any x_1 and x. Since $\approx_r$ is compositional, we have $(\mathcal{C} \mid\mid c!0 \mid\mid T) \approx_r (\mathcal{D} \mid\mid c!0 \mid\mid T)$. Note that $(\mathcal{C} \mid\mid c!0 \mid\mid T) \Downarrow_{c_2}^{\geq p}$, which implies $(\mathcal{D} \mid\mid c!0 \mid\mid T) \Downarrow_{c_2}^{\geq p}$. Since c is fresh for $\mathcal{D}$, the latter has no potential to communicate at channel c. Therefore, it must be the case that $\mathcal{D} \Downarrow_{c_1}^{\geq p}$.

3. $\mathcal{R}$ is reduction-closed. Suppose $\mathcal{C} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ for some distribution Δ. Then $\mathcal{C}||c!0 \stackrel{\hat{\tau}}{\Longrightarrow} \Delta||c!0$. Since $(\mathcal{C}||c!0) \approx_r (\mathcal{D}||c!0)$, there is some Γ such that $\mathcal{D}||c!0 \stackrel{\hat{\tau}}{\Longrightarrow} \Gamma$ and $(\Delta||c!0) \approx_r{}^\dagger \Gamma$. Note that c is fresh for $\mathcal{D}$, thus there is no communication between $\mathcal{D}$ and $c!0$. Therefore, it must be the case that $\Gamma = \Theta||c!0$ for some Θ such that $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$. Thus, $(\Delta||c!0) \approx_r{}^\dagger (\Theta||c!0)$, i.e. $\Delta\ \mathcal{R}^\dagger\ \Theta$.

□

Theorem 5.17 (Completeness)**.** *If $\mathcal{C} \approx_r \mathcal{D}$ then $\mathcal{C} \approx_o \mathcal{D}$.*

Proof. Since $\approx_r$ is closed under any super-operator application, by Proposition 5.5 it suffices to show that $\approx_r$ is a ground bisimulation. By the symmetry of $\approx_r$, we only need to show that $\approx_r$ is a ground simulation. Suppose $\mathcal{C} = \langle P, \rho\rangle$, $\mathcal{D} = \langle Q, \sigma\rangle$ and $\mathcal{C} \approx_r \mathcal{D}$. By definition, we have $qv(P) = qv(Q)$ and $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$. Suppose $\mathcal{C} \xrightarrow{\alpha} \Delta$. We distinguish several cases.

1. $\alpha \equiv \tau$. Since $\approx_r$ is compositional, we have $(\mathcal{C} \mid\mid c!0) \approx_r (\mathcal{D} \mid\mid c!0)$ for some fresh channel c. Since $\approx_r$ is reduction-closed, the reduction $\mathcal{C} \mid\mid c!0 \stackrel{\hat{\tau}}{\Longrightarrow} \Delta \mid\mid c!0$ is matched by some Γ such that $\mathcal{D} \mid\mid c!0 \stackrel{\hat{\tau}}{\Longrightarrow} \Gamma$ and $\Delta \mid\mid c!0 \approx_r{}^\dagger \Gamma$. Since c is fresh, there is no communication between $\mathcal{D}$ and $c!0$, so it must be the case that Γ has the form $\Theta \mid\mid c!0$ with $\mathcal{D} \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$. It follows from Lemma 5.16 and $\Delta \mid\mid c!0 \approx_r{}^\dagger \Theta \mid\mid c!0$ that $\Delta \approx_r{}^\dagger \Theta$.

2. $\alpha \equiv c!v$. Let T be the process defined by

$$T \ := \ c_1!0 + c?x.\mathbf{if}\ x = v\ \mathbf{then}\ (c_2!0 + \tau.c_3!0)$$

where c_1, c_2 and c_3 are fresh channels. Then $\mathcal{C}||T \stackrel{\hat{\tau}}{\Longrightarrow} \Delta||c_3!v$.

Since $\mathcal{C} \approx_r \mathcal{D}$ we know $\mathcal{C}||T \approx_r \mathcal{D}||T$ by the compositionality of $\approx_r$. Since $\approx_r$ is reduction-closed, there is some Γ such that $\mathcal{D}||T \stackrel{\hat{\tau}}{\Longrightarrow} \Gamma$ and $\Delta||c_3!0 \approx_r{}^\dagger \Gamma$. Since $\approx_r$ is barb-preserving we have $\Gamma \not\Downarrow^{>0}_{c_1}$, $\Gamma \not\Downarrow^{>0}_{c_2}$ and $\Gamma \Downarrow^{\geq 1}_{c_2}$. Here we use the notation $\Gamma \not\Downarrow^{>0}_{c_1}$ to mean that $\Gamma \Downarrow^{\geq p}_{c_1}$ does not hold for any $p > 0$. It must be the case that $\Gamma \equiv \Theta||c_3!0$ for some Θ with $\mathcal{D} \stackrel{c!v}{\Longrightarrow} \Theta$. By Lemma 5.16 and $\Delta||c_3!0 \approx_r{}^\dagger \Theta||c_3!0$, we have $\Delta \approx_r{}^\dagger \Theta$.

3. $\alpha \equiv \mathsf{c}?q$. Let T be the process defined by

$$T \ := \ c_1!0 + \mathsf{c}!r.c_2!0$$

where c_1 and c_2 are fresh channels. Then $\mathcal{C}||T \stackrel{\hat{\tau}}{\Longrightarrow} \Delta \mid\mid c_2!0$. Since $\mathcal{C} \approx_r \mathcal{D}$ we know $\mathcal{C}||T \approx_r \mathcal{D}||T$ by the compositionality of $\approx_r$. Since $\approx_r$ is reduction-closed, there is some Γ such that $\mathcal{D}||T \stackrel{\hat{\tau}}{\Longrightarrow} \Gamma$ and $\Delta||c_2!0 \approx_r \Gamma$. Since $\approx_r$ is barb-preserving we have $\Gamma \not\Downarrow^{>0}_{c_1}$ and $\Gamma \Downarrow^{\geq 1}_{c_2}$. It follows that $\mathcal{D} \stackrel{\mathsf{c}?q}{\Longrightarrow} \Theta$ and $\Gamma \equiv \Theta \mid\mid c_2!0$, with implicit assumption of α-conversion. By Lemma 5.16 and $\Delta \mid\mid c_2!0 \approx_r{}^\dagger \Theta \mid\mid c_2!0$, we have $\Delta \approx_r{}^\dagger \Theta$.

The case when $\alpha \equiv c?x$ is similar.

4. $\alpha \equiv \mathsf{c}!q$. Let T be the process defined by

$$T \ := \ c_1!0 + \mathsf{c}?r.(c_2!0 + I[r].c_3!0)$$

where c_1, c_2 and c_3 are fresh channels. Then $\mathcal{C}||T \stackrel{\hat{\tau}}{\Longrightarrow} \Delta \mid\mid (c_2!0 + I[q].c_3!0)$. Since $\mathcal{C} \approx_r \mathcal{D}$ we know $\mathcal{C}||T \approx_r \mathcal{D}||T$ by the compositionality of $\approx_r$. Since $\approx_r$ is reduction-closed, there is some Γ such that $\mathcal{D}||T \stackrel{\hat{\tau}}{\Longrightarrow} \Gamma$ and

$$\Delta||(c_2!0 + I[q].c_3!0) \approx_r{}^\dagger \Gamma. \tag{6}$$

Since $\approx_r$ is barb-preserving we have $\Gamma \not\Downarrow^{>0}_{c_1}$ and $\Gamma \Downarrow^{\geq 1}_{c_2}$. It follows that $\mathcal{D} \stackrel{\mathsf{c}!q'}{\Longrightarrow} \Theta$ for some $q' \in qVar$, and $\Gamma \equiv \Theta \mid\mid (c_2!0 + I[q'].c_3!0)$. Note that $\Delta||(c_2!0 + I[q].c_3!0) \stackrel{\tau}{\longrightarrow} \Delta||c_3!0$. To match this action, we have $\Gamma \stackrel{\hat{\tau}}{\Longrightarrow} \Gamma'$ for some Γ' such that $\Delta||c_3!0 \approx_r{}^\dagger \Gamma'$. As a consequence, we have $\Gamma' \Downarrow^{\geq 1}_{c_3}$ but $\Gamma' \not\Downarrow^{>0}_{c_2}$, so $\Gamma' \equiv \Theta' \mid\mid c_3!0$ for some Θ' with $\Theta \stackrel{\hat{\tau}}{\Longrightarrow} \Theta'$, which implies $\mathcal{D} \stackrel{\mathsf{c}!q'}{\Longrightarrow} \Theta'$. Now by Lemma 5.16 and $\Delta \mid\mid c_3!0 \approx_r{}^\dagger \Theta' \mid\mid c_3!0$, we derive $\Delta \approx_r{}^\dagger \Theta'$.

Finally, we claim that $q = q'$. Otherwise from Eq.(6), we know $q' \in qv(\Delta)$ but $q' \notin qv(\Theta)$. That contradicts the fact that $\Delta||c_3!0 \approx_r{}^\dagger \Gamma'$ as $qv(\Theta') \subseteq qv(\Theta)$.

$\square$

5.4 Modal characterisation

We extend the Hennessy-Milner logic by adding a probabilistic choice modality to express the bebaviour of distributions, as in [7], and a super-operator modality to express trace-preserving super-operator application, as well as atomic formulae involving projectors for dealing with density operators.

Definition 5.18. *The class $\mathcal{L}$ of modal formulae over* Act*, ranged over by ϕ, is defined by the following grammar:*

$$\begin{array}{rcl} \phi & := & E^{\geq p}_{\widetilde{q}} \mid \bigwedge_{i\in I} \phi_i \mid \langle\alpha\rangle\psi \mid \neg\phi \mid \mathcal{E}.\phi \\ \psi & := & \bigoplus_{i\in I} p_i \cdot \phi_i \end{array}$$

where $\alpha \in \mathsf{Act}_\tau$*,* $\mathcal{E}$ *is a super-operator, and* E *is a projector associated with a certain subspace of* $\mathcal{H}_{\widetilde{q}}$*. We call* ϕ *a* configuration formula *and* ψ *a* distribution formula*. Note that a distribution formula* ψ *only appears as the continuation of a diamond modality* $\langle\alpha\rangle\psi$*.*

The satisfaction relation $\models \subseteq S \times \mathcal{L}$ *is defined by*

- $\mathcal{C} \models E_{\tilde{q}}^{\geq p}$ *if* $qv(\mathcal{C}) \cap \tilde{q} = \emptyset$ *and* $\mathrm{tr}(E_{\tilde{q}}\rho) \geq p$ *where* $\mathcal{C} = \langle P, \rho\rangle$*.*
- $\mathcal{C} \models \bigwedge_{i\in I} \phi_i$ *if* $\mathcal{C} \models \phi_i$ *for all* $i \in I$*.*
- $\mathcal{C} \models \langle\alpha\rangle\psi$ *if for some* $\Delta \in \mathcal{D}(Con)$*,* $\mathcal{C} \stackrel{\hat{\alpha}}{\Longrightarrow} \Delta$ *and* $\Delta \models \psi$*.*
- $\mathcal{C} \models \neg\phi$ *if it is not the case that* $\mathcal{C} \models \phi$*.*
- $\mathcal{C} \models \mathcal{E}.\phi$ *if* $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$ *and* $\mathcal{E}(\mathcal{C}) \models \phi$*.*
- $\Delta \models \bigoplus_{i\in I} p_i \cdot \phi_i$ *if there are* $\Delta_i \in \mathcal{D}(Con)$*, for all* $i \in I, \mathcal{D} \in \lceil\Delta_i\rceil$*, with* $\mathcal{D} \models \phi_i$*, such that* $\Delta = \sum_{i\in I} p_i \cdot \Delta_i$*.*

With a slight abuse of notation, we write $\Delta \models \psi$ above to mean that Δ satisfies the distribution formula ψ. A logical equivalence arises from the logic naturally: we write $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$ if $\mathcal{C} \models \phi \Leftrightarrow \mathcal{D} \models \phi$ for all $\phi \in \mathcal{L}$.

It turns out that $\mathcal{L}$ is adequate with respect to open bisimilarity.

Theorem 5.19. *Let* $\mathcal{C}$ *and* $\mathcal{D}$ *be any two configurations in a pLTS. Then* $\mathcal{C} \approx_o \mathcal{D}$ *if and only if* $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$*.*

Proof. ($\Rightarrow$) Suppose $\mathcal{C} \approx_o \mathcal{D}$, we show that $\mathcal{C} \models \phi \Leftrightarrow \mathcal{D} \models \phi$. Since $\approx_o$ is symmetric, it suffices to prove that $\mathcal{C} \models \phi$ implies $\mathcal{D} \models \phi$ by structural induction on ϕ.

- Let $\mathcal{C} \models E_{\tilde{q}}^{\geq p}$. Then $qv(\mathcal{C}) \cap \tilde{q} = \emptyset$ and $\mathrm{tr}(E_{\tilde{q}}\rho) \geq p$. Since $\mathcal{C} \approx_o \mathcal{D}$, we have $qv(\mathcal{C}) = qv(\mathcal{D})$ and $\mathrm{ptr}(\mathcal{C}) = \mathrm{ptr}(\mathcal{D})$. Thus $qv(\mathcal{D}) \cap \tilde{q} = \emptyset$. Let $\mathcal{C} = \langle P, \rho\rangle$ and $\mathcal{D} = \langle Q, \sigma\rangle$. We can infer that

$$\begin{array}{rcl}
\mathrm{tr}(E_{\tilde{q}}\sigma) & = & \mathrm{tr}_{\overline{qv(Q)}}\mathrm{tr}_{qv(Q)}(E_{\tilde{q}}\sigma) \\
& = & \mathrm{tr}_{\overline{qv(Q)}}E_{\tilde{q}}(\mathrm{tr}_{qv(Q)}(\sigma)) \\
& = & \mathrm{tr}_{\overline{qv(P)}}E_{\tilde{q}}(\mathrm{tr}_{qv(P)}(\rho)) \\
& = & \mathrm{tr}_{\overline{qv(P)}}\mathrm{tr}_{qv(P)}(E_{\tilde{q}}\rho) \\
& = & \mathrm{tr}(E_{\tilde{q}}\rho) \\
& \geq & p.
\end{array}$$

  It follows that $\mathcal{D} \models E_{\tilde{q}}^{\geq p}$.

- Let $\mathcal{C} \models \bigwedge_{i\in I} \phi_i$. Then $\mathcal{C} \models \phi_i$ for each $i \in I$. So by induction $\mathcal{D} \models \phi_i$, and we have $\mathcal{D} \models \bigwedge_{i\in I} \phi_i$.
- Let $\mathcal{C} \models \neg\phi$. So $\mathcal{C} \not\models \phi$, and by induction we have $\mathcal{D} \not\models \phi$. Thus $\mathcal{D} \models \neg\phi$.
- Let $\mathcal{C} \models \langle\alpha\rangle \bigoplus_{i\in I} p_i \cdot \phi_i$. Then $\mathcal{C} \stackrel{\hat{\alpha}}{\Longrightarrow} \Delta$ and $\Delta \models \bigoplus_{i\in I} p_i \cdot \phi_i$ for some Δ. So $\Delta = \sum_{i\in i} p_i \cdot \Delta_i$ and for all $i \in I$ and $\mathcal{C}' \in \lceil\Delta_i\rceil$ we have $\mathcal{C}' \models \phi_i$. Since $\mathcal{C} \approx_o \mathcal{D}$, by Corollary 5.8 there is some Θ with $\mathcal{D} \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta \approx_o{}^\dagger \Theta$. Since the lifted relation is left-decomposable, we have that $\Theta = \sum_{i\in I} p_i \cdot \Theta_i$ and $\Delta_i \approx_o{}^\dagger \Theta_i$. It follows that for each $\mathcal{D}' \in \lceil\Theta_i\rceil$ there is some $\mathcal{C}' \in \lceil\Delta_i\rceil$ with $\mathcal{C}' \approx_o \mathcal{D}'$. So by induction we have $\mathcal{D}' \models \phi_i$ for all $\mathcal{D}' \in \lceil\Theta_i\rceil$ with $i \in I$. Therefore, we have $\Theta \models \bigoplus_{i\in I} p_i \cdot \phi_i$. It follows that $\mathcal{D} \models \langle\alpha\rangle \bigoplus_{i\in I} p_i \cdot \phi_i$.
- Let $\mathcal{C} \models \mathcal{E}.\phi$. Then $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$ and $\mathcal{E}(\mathcal{C}) \models \phi$. Since $\mathcal{C} \approx_o \mathcal{D}$, we have $\mathcal{E}(\mathcal{C}) \approx_o \mathcal{E}(\mathcal{D})$ by Proposition 5.6 and $qv(\mathcal{C}) = qv(\mathcal{D})$. By induction, we have $\mathcal{E}(\mathcal{D}) \models \phi$. It follows that $\mathcal{D} \models \mathcal{E}.\phi$.

($\Leftarrow$) Suppose $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$. We first show that $qv(\mathcal{C}) = qv(\mathcal{D})$ and $\mathrm{ptr}(\mathcal{C}) = \mathrm{ptr}(\mathcal{D})$. For any $\tilde{q}$, if $\tilde{q} \cap qv(\mathcal{C}) = \emptyset$ then $\mathcal{C} \models I_{\tilde{q}}^{\geq 1}$. Since $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$ we have $\mathcal{D} \models I_{\tilde{q}}^{\geq 1}$, and thus $\tilde{q} \cap qv(\mathcal{D}) = \emptyset$. It follows that $qv(\mathcal{C}) \supseteq qv(\mathcal{D})$. By the symmetry of $=^{\mathcal{L}}$, this implies $qv(\mathcal{C}) = qv(\mathcal{D})$. Now let $\mathcal{C} = \langle P, \rho\rangle$ and $\mathcal{D} = \langle Q, \sigma\rangle$. Suppose for a contradiction that $\mathrm{tr}_{qv(P)}\rho \neq \mathrm{tr}_{qv(P)}\sigma$. Then there exists a projection E on $\tilde{q}$ with $\tilde{q} \cap qv(P) = \emptyset$ and $\mathrm{tr}(E_{\tilde{q}}\sigma) < \mathrm{tr}(E_{\tilde{q}}\rho)$. Let $p = \mathrm{tr}(E_{\tilde{q}}\rho)$. Then $\langle P, \rho\rangle \models E_{\tilde{q}}^{\geq p}$ while $\langle Q, \sigma\rangle \not\models E_{\tilde{q}}^{\geq p}$, contradicting the assumption that $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$.

Next, we show that the relation $=^{\mathcal{L}}$ is a ground bisimulation. Suppose $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$ and $\mathcal{C} \xrightarrow{\alpha} \Delta$. We have to show that there is some Θ with $\mathcal{D} \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta\ (=^{\mathcal{L}})^{\dagger}\ \Theta$. Consider the set

$$T := \{\Theta \mid \mathcal{D} \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta \wedge \Theta = \sum_{\mathcal{C}' \in \lceil\Delta\rceil} \Delta(\mathcal{C}') \cdot \Theta_{\mathcal{C}'} \wedge \exists \mathcal{C}' \in \lceil\Delta\rceil, \exists \mathcal{D}' \in \lceil\Theta_{\mathcal{C}'}\rceil : \mathcal{C}' \neq^{\mathcal{L}} \mathcal{D}'\} \tag{7}$$

For each $\Theta \in T$, there must be some $\mathcal{C}'_\Theta \in \lceil\Delta\rceil$ and $\mathcal{D}'_\Theta \in \lceil\Theta_{\mathcal{C}'_\Theta}\rceil$ such that (i) either there is a formula ϕ_Θ with $\mathcal{C}'_\Theta \models \phi_\Theta$ but $\mathcal{D}'_\Theta \not\models \phi_\Theta$ (ii) or there is a formula ϕ'_Θ with $\mathcal{D}'_\Theta \models \phi'_\Theta$ but $\mathcal{C}'_\Theta \not\models \phi'_\Theta$. In the latter case we set $\phi_\Theta = \neg\phi'_\Theta$ and return back to the former case. So for each $\mathcal{C}' \in \lceil\Delta\rceil$ it holds that $\mathcal{C}' \models \bigwedge_{\{\Theta \in T \mid \mathcal{C}'_\Theta = \mathcal{C}'\}} \phi_\Theta$ and for each $\Theta \in T$ with $\mathcal{C}'_\Theta = \mathcal{C}'$ there is some $\mathcal{D}'_\Theta \in \lceil\Theta_{\mathcal{C}'}\rceil$ with $\mathcal{D}'_\Theta \not\models \bigwedge_{\{\Theta \in T \mid \mathcal{C}'_\Theta = \mathcal{C}'\}} \phi_\Theta$. Let

$$\phi := \langle\alpha\rangle \bigoplus_{\mathcal{C}' \in \lceil\Delta\rceil} \Delta(\mathcal{C}') \cdot \bigwedge_{\{\Theta \in T \mid \mathcal{C}'_\Theta = \mathcal{C}'\}} \phi_\Theta. \tag{8}$$

It is clear that $\mathcal{C} \models \phi$, hence $\mathcal{D} \models \phi$ by $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$. It follows that there must be a Θ^* with $\mathcal{D} \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta^*$, $\Theta^* = \sum_{\mathcal{C}' \in \lceil\Delta\rceil} \Delta(\mathcal{C}') \cdot \Theta^*_{\mathcal{C}'}$ and for each $\mathcal{C}' \in \lceil\Delta\rceil, \mathcal{D}' \in \lceil\Theta^*_{\mathcal{C}'}\rceil$ we have $\mathcal{D}' \models \bigwedge_{\{\Theta \in T \mid \mathcal{C}'_\Theta = \mathcal{C}'\}} \phi_\Theta$. This means that $\Theta^* \notin T$ and hence for each $\mathcal{C}' \in \lceil\Delta\rceil, \mathcal{D}' \in \lceil\Theta^*_{\mathcal{C}'}\rceil$ we have $\mathcal{C}' =^{\mathcal{L}} \mathcal{D}'$. It follows that $\Delta\ (=^{\mathcal{L}})^{\dagger}\ \Theta^*$. By symmetry all transitions of $\mathcal{D}$ can be matched up by transitions of $\mathcal{C}$.

Finally, we prove that the relation $=^{\mathcal{L}}$ is closed under super-operator application. That is, for any $\mathcal{E} \in \mathcal{SO}(\mathcal{H}_{\overline{qv(\mathcal{C})}})$ we need to show that $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$ implies $\mathcal{E}(\mathcal{C}) =^{\mathcal{L}} \mathcal{E}(\mathcal{D})$. Suppose $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$ and let ϕ be any formula such that $\mathcal{E}(\mathcal{C}) \models \phi$. We have $\mathcal{C} \models \mathcal{E}.\phi$. It follows from $\mathcal{C} =^{\mathcal{L}} \mathcal{D}$ that $qv(\mathcal{C}) = qv(\mathcal{D})$ and $\mathcal{D} \models \mathcal{E}.\phi$. Therefore, we obtain $\mathcal{E}(\mathcal{D}) \models \phi$. By symmetry if ϕ is satisfied by $\mathcal{E}(\mathcal{D})$ then it is also satisfied by $\mathcal{E}(\mathcal{C})$. In other words, we have $\mathcal{E}(\mathcal{C}) =^{\mathcal{L}} \mathcal{E}(\mathcal{D})$.

Now by appealing to Proposition 5.5 we see that $=^{\mathcal{L}}$ is an open bisimulation, thus $=^{\mathcal{L}} \subseteq \approx_o$. □

Note that the set T in (7) is infinite in general as $\mathcal{D}$ may have infinitely many different derivatives, hence we have to use infinite conjunction in (8). This is the reason that we cannot restrict ourselves to finite or binary conjunction in Definition 5.18.

6 Examples

BB84, the first quantum key distribution protocol developed by Bennett and Brassard in 1984 [2], provides a provably secure way to create a private key between two parties, say, Alice and Bob. Its security relies on the basic property of quantum mechanics that information gain about a quantum state is only possible at the expense of changing the state, if the states to be distinguished are not orthogonal. The basic BB84 protocol goes as follows:

(1) Alice randomly creates two strings of bits $\tilde{B}_a$ and $\tilde{K}_a$, each with size n.

(2) Alice prepares a string of qubits $\tilde{q}$, with size n, such that the ith qubit of $\tilde{q}$ is $|x_y\rangle$ where x and y are the ith bits of $\tilde{B}_a$ and $\tilde{K}_a$, respectively, and $|0_0\rangle = |0\rangle$, $|0_1\rangle = |1\rangle$, $|1_0\rangle = |+\rangle$, and $|1_1\rangle = |-\rangle$. Here the symbols $|+\rangle$ and $|-\rangle$ have their usual meaning:

$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \qquad \text{and} \qquad |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}.$$

(3) Alice sends the qubit string $\tilde{q}$ to Bob.

(4) Bob randomly generates a string of bits $\tilde{B}_b$ with size n.

(5) Bob measures each qubit received from Alice according to a basis determined by the bits he generated: if the ith bit of $\tilde{B}_b$ is k then he measures with $\{|k_0\rangle, |k_1\rangle\}$, $k = 0, 1$. Let the measurement results be $\tilde{K}_b$, which is also a string of bits with size n.

(6) Bob sends his choice of measurement bases $\tilde{B}_b$ back to Alice, and upon receiving the information, Alice sends her bases $\tilde{B}_a$ to Bob.

(7) Alice and Bob determine at which positions the bit strings $\tilde{B}_a$ and $\tilde{B}_b$ are equal. They discard the bits in $\tilde{K}_a$ and $\tilde{K}_b$ where the corresponding bits of $\tilde{B}_a$ and $\tilde{B}_b$ do not match.

After the execution of the basic BB84 protocol above, the remaining bits of $\tilde{K}_a$ and $\tilde{K}_b$, denoted by $\tilde{K}'_a$ and $\tilde{K}'_b$ respectively, should be the same, provided that the channels used are perfect, and no eavesdropper exists.

To detect a potentially existing eavesdropper Eve, Alice and Bob proceed as follows:

(8) Alice randomly chooses $\lceil k/2 \rceil$, where k is the size of $\tilde{K}'_a$, bits of $\tilde{K}'_a$, denoted by $\tilde{K}''_a$, and sends Bob $\tilde{K}''_a$ and their indexes in the original string $\tilde{K}'_a$.

(9) Upon receiving the information from Alice, Bob sends back to Alice his substring $\tilde{K}''_b$ of $\tilde{K}'_b$ according to the indexes received from Alice.

(10) Alice and Bob check if the strings $\tilde{K}''_a$ and $\tilde{K}''_b$ are equal. If yes, then the remaining substrings $\tilde{K}^f_a$ (resp. $\tilde{K}^f_b$) of $\tilde{K}'_a$ (resp. $\tilde{K}'_b$) by deleting $\tilde{K}''_a$ (resp. $\tilde{K}''_b$) are the secure keys shared by Alice and Bob. Otherwise, an eavesdropper is detected, and the protocol halts without generating any secure keys.

For simplicity, we omit the processes of information reconciliation and privacy amplification. Now we describe the above protocol in our language of qCCS. To ease the notations, we assume a special measurement $Ran[\tilde{q}; \tilde{x}]$ which can create a string of n random bits, independent of the initial states of the $\tilde{q}$ system, and store it to $\tilde{x}$. In effect, $Ran[\tilde{q}; \tilde{x}] = Set^n_+[\tilde{q}].M^n_{0,1}[\tilde{q}; \tilde{x}].Set^n_0[\tilde{q}]$. Then the basic BB84 protocol can be defined as

$$\begin{aligned}
Alice &\stackrel{def}{=} Ran[\tilde{q}; \tilde{B}_a].Ran[\tilde{q}; \tilde{K}_a].Set_{\tilde{K}_a}[\tilde{q}].H_{\tilde{B}_a}[\tilde{q}].\mathsf{A2B}!\tilde{q}.WaitA(\tilde{B}_a, \tilde{K}_a) \\
WaitA(\tilde{B}_a, \tilde{K}_a) &\stackrel{def}{=} b2a?\tilde{B}_b.a2b!\tilde{B}_a.key_a!cmp(\tilde{K}_a, \tilde{B}_a, \tilde{B}_b).\mathbf{nil} \\
Bob &\stackrel{def}{=} \mathsf{A2B}?\tilde{q}.Ran[\tilde{q}'; \tilde{B}_b].M_{\tilde{B}_b}[\tilde{q}; \tilde{K}_b].b2a!\tilde{B}_b.WaitB(\tilde{B}_b, \tilde{K}_b) \\
WaitB(\tilde{B}_b, \tilde{K}_b) &\stackrel{def}{=} a2b?\tilde{B}_a.key_b!cmp(\tilde{K}_b, \tilde{B}_a, \tilde{B}_b).\mathbf{nil} \\
BB84 &\stackrel{def}{=} (Alice\|Bob)\backslash\{a2b, b2a, \mathsf{A2B}\}
\end{aligned}$$

where Set^n_+ is the super-operator which sets each of the n qubits it applies on to $|+\rangle$, $M_{\tilde{y}}[\tilde{q}; \tilde{K}_b]$ is the quantum measurement on $\tilde{q}$ according to the basis determined by $\tilde{y}$, i.e., for each $1 \leq k \leq n$, it measures q_k with respect to the basis $\{|0\rangle, |1\rangle\}$ (reps. $\{|+\rangle, |-\rangle\}$) if $y(k) = 0$ (resp. 1), and stores the result into $\tilde{K}_b(k)$. $M^n_{0,1}$ is the same as $M_{0\cdots0}$, and $H_{\tilde{y}}[\tilde{q}]$ has a similar meaning with $M_{\tilde{y}}[\tilde{q}; \tilde{K}_b]$. We also abuse the notion slightly by writing $\mathcal{E}_{\tilde{B}}[\tilde{q}].P$ when we mean $\sum_{\tilde{x}=0^n}^{1^n}(\mathbf{if}\ \tilde{B} = \tilde{x}\ \mathbf{then}\ \mathcal{E}_{\tilde{x}}[\tilde{q}].P)$ where 0^n is the all zero string of size n. The function cmp takes a triple of strings $\tilde{x}, \tilde{y}, \tilde{z}$ with the same size as inputs, and returns the substring of $\tilde{x}$ where the corresponding bits of $\tilde{y}$ and $\tilde{z}$ match. When $\tilde{y}$ and $\tilde{z}$ match nowhere, we let $cmp(\tilde{x}, \tilde{y}, \tilde{z}) = \epsilon$, the empty string.

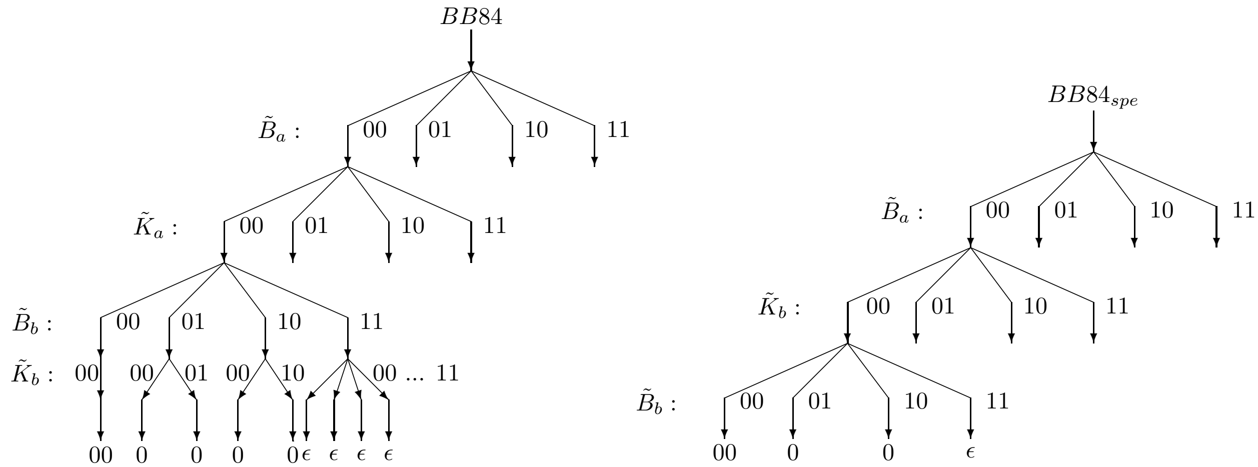

Figure 2: pLTSs for $BB84$ and $BB84_{spe}$

To show the correctness of this basic form of BB84 protocol, we have two choices. The first one is to employ the concept of bisimulation. Let

$$\begin{aligned} BB84_{spc} \quad &\overset{def}{=} \quad Ran[\tilde{q}; \tilde{B}_a].Ran[\tilde{q}; \tilde{K}_b].Ran[\tilde{q}'; \tilde{B}_b]. \\ &\quad\quad (key_a!cmp(\tilde{K}_b, \tilde{B}_a, \tilde{B}_b).\mathbf{nil} \| key_b!cmp(\tilde{K}_b, \tilde{B}_a, \tilde{B}_b).\mathbf{nil}). \end{aligned}$$

The pLTSs of $BB84$ and $BB84_{spe}$ for the special case of $n = 2$ can be depicted as in Figure 2, where for simplicity, we only specify the branch where $\tilde{B}_a = \tilde{K}_a = 00$. Each arrow in the graph denotes a sequence of τ actions, and all probabilistic distributions are uniform. The strings at the bottom line are the outputs of the protocol. Then it can be easily checked from the pLTSs that $BB84 \approx_o BB84_{spe}$. The key is, for each extra branch in $BB84$ caused by the measurement of Bob (the $\tilde{K}_b$ line), the final states are bisimilar; they all output the same string.

The second choice is to use logic formulae. Let

$$\begin{aligned} TestBB84 \quad &\overset{def}{=} \quad (BB84 \| key_a?\tilde{K}'_a.key_b?\tilde{K}'_b. \\ &\quad\quad (\mathbf{if}\ \tilde{K}'_a = \tilde{K}'_b\ \mathbf{then}\ suc!0.\mathbf{nil}\ \mathbf{else}\ fail!0)) \backslash \{key_a, key_b\}, \end{aligned}$$

and

$$\psi_p = \langle suc!0 \rangle true \wedge \neg \langle \tau \rangle (p \cdot \langle fail!0 \rangle true + (1-p) \cdot true)$$

where $true$ is the abbreviation of $\bigwedge_{i \in \emptyset} \phi_i$. It is not difficult to show $TestBB84 \models \psi_p$ for any $p > 0$.

Now we proceed to describe the protocol where an eavesdropper can be detected.

$$\begin{aligned}
Alice' &\stackrel{def}{=} (Alice \| key_a?\tilde{K}'_a.Pstr_{|\tilde{K}'_a|}[\tilde{q}_a;\tilde{x}].a2b!\tilde{x}.a2b!SubStr(\tilde{K}'_a,\tilde{x}).b2a?\tilde{K}''_b. \\
&\qquad (\textbf{if } SubStr(\tilde{K}'_a,\tilde{x}) = \tilde{K}''_b \textbf{ then } key'_a!RemStr(\tilde{K}'_a,\tilde{x}).\textbf{nil} \\
&\qquad\qquad \textbf{else } alarm_a!0.\textbf{nil})))\backslash\{key_a\}
\end{aligned}$$

$$\begin{aligned}
Bob' &\stackrel{def}{=} (Bob \| key_b?\tilde{K}'_b.a2b?\tilde{x}.a2b?\tilde{K}''_a.b2a!SubStr(\tilde{K}'_b,\tilde{x}). \\
&\qquad (\textbf{if } SubStr(\tilde{K}'_b,\tilde{x}) = \tilde{K}''_a \textbf{ then } key'_b!RemStr(\tilde{K}'_b,\tilde{x}).\textbf{nil} \\
&\qquad\qquad \textbf{else } alarm_b!0.\textbf{nil}))\backslash\{key_b\}
\end{aligned}$$

$$BB84' \stackrel{def}{=} Alice' \| Bob'$$

where $|\tilde{x}|$ is the size of $\tilde{x}$, the function $SubStr(\tilde{K}'_a,\tilde{x})$ returns the substring of $\tilde{K}'_a$ at the indexes specified by $\tilde{x}$, and $RemStr(\tilde{K}'_a,\tilde{x})$ returns the remaining substring of $\tilde{K}'_a$ by deleting $SubStr(\tilde{K}'_a,\tilde{x})$. The special measurement $Pstr_m$, which is similar to Ran, randomly generates a $\lceil m/2 \rceil$-sized string of indexes from $1,\ldots,m$.

For the capacity of a potential eavesdropper Eve, we assume that she has complete control of the quantum channel, but can only listen on the classical channels between Alice and Bob. That is, she can do any quantum operations on the communicated qubits from Alice and Bob, one of the extreme cases being keeping the qubits from Alice while creating and sending to Bob some fresh ones, with the same size, prepared by herself. But for classical communication, Eve can only copy and resend the bits without altering them, since Alice and Bob can choose to send them through a broadcasting channel. Note that perfect copying of the qubits transmitted through the quantum channel from Alice to Bob is prohibited by the basic laws of quantum mechanics, since the potential quantum states sent, $|0\rangle, |1\rangle, |+\rangle$, and $|-\rangle$ in this protocol, are nonorthogonal. With these natural assumptions, an eavesdropper Eve can be described as:

$$\begin{aligned}
Eve &\stackrel{def}{=} \mathsf{A2E}?\tilde{q}.\mathcal{E}[\tilde{q}'',\tilde{q}].M^n_{0,1}[\tilde{q}'';\tilde{K}_e].\mathsf{E2B}!\tilde{q}.WaitE(\tilde{K}_e) \\
WaitE(\tilde{K}_e) &\stackrel{def}{=} b2e?\tilde{B}_b.e2a!\tilde{B}_b.a2e?\tilde{B}_a.e2b!\tilde{B}_a.a2e?\tilde{x}.e2b!\tilde{x}. \\
&\qquad a2e?\tilde{K}''_a.e2b!\tilde{K}''_a.b2e?\tilde{K}''_b.e2a!\tilde{K}''_b.key'_e!gkey(\tilde{K}_e,\tilde{B}_e,\tilde{B}_a,\tilde{B}_b,\tilde{K}''_a,\tilde{K}''_b,\tilde{x}).\textbf{nil}
\end{aligned}$$

where $\mathcal{E}$ is a super-operator, and $gkey$ is the function Eve used to generate her guess of the key from the classical information transmitted between Alice and Bob. Then a practical running BB84 protocol, with the existence of an eavesdropper, goes as follows

$$BB84_E \stackrel{def}{=} (Alice'[f_a] \| Eve \| Bob'[f_b])\backslash\{a2e, b2e, e2a, e2b, \mathsf{A2E}, \mathsf{E2B}\}$$

where f_a and f_b are relabelling functions such that $f_a(a2b) = a2e, f_a(b2a) = e2a$, $f_a(\mathsf{A2B}) = \mathsf{A2E}$, and $f_b(a2b) = e2b, f_b(b2a) = b2e, f_b(\mathsf{A2B}) = \mathsf{E2B}$.

To get a taste of the security of $BB84'$, we consider a special case where Eve's strategy is to simply measure the qubits sent by Alice, according to randomly guessed bases, to get the keys. She then prepares and sends to Bob a fresh sequence of qubits, employing the same method Alice used to encode keys, but using her own guess of bases and the keys she obtained. That is, we define

$$Eve' \stackrel{def}{=} \mathsf{A2E}?\tilde{q}.Ran[\tilde{q}'';\tilde{B}_e].M_{\tilde{B}_e}[\tilde{q};\tilde{K}_e].Set_{\tilde{K}_e}[\tilde{q}].H_{\tilde{B}_e}[\tilde{q}].\mathsf{E2B}!\tilde{q}.WaitE(\tilde{K}_e)$$

Now let $BB84'_E$ be the protocol obtained from $BB84_E$ by replacing Eve by Eve$'$, and letting the function $gkey$ simply return its first parameter. Let

$$\begin{aligned}
TestBB84' &\stackrel{def}{=} (BB84'_E \| key'_a?\tilde{x}.key'_b?\tilde{y}.key'_e?\tilde{z}.(\textbf{if } \tilde{x} \neq \tilde{y} \textbf{ then } fail!0.\textbf{nil} \\
&\qquad\qquad \textbf{else } key_e!\tilde{z}.skey!\tilde{x}.\textbf{nil}))\backslash\{key'_a, key'_b, key'_e\}.
\end{aligned}$$

It is generally very complicated to prove the security of the full $BB84$ protocol, even for the simplified Eve' presented above. Here we choose to reduce $TestBB84'$ to a simpler process which is easier for further verification. To be specific, we can show that $TestBB84'$ is bisimilar to the following process:

$$
\begin{aligned}
TB \stackrel{def}{=} \; & Ran[\tilde{q}; \tilde{B}_a].Ran[\tilde{q}; \tilde{K}_a].Ran[\tilde{q}''; \tilde{B}_e].Ran'_{\tilde{B}_a,\tilde{B}_e,\tilde{K}_a}[\tilde{q}; \tilde{K}_e].Ran[\tilde{q}'; \tilde{B}_b]. \\
& Ran'_{\tilde{B}_e,\tilde{B}_b,\tilde{K}_e}[\tilde{q}; \tilde{K}_b].Pstr_{|\tilde{K}_{ab}|}[\tilde{q}_a; \tilde{x}]. \\
& (\mathbf{if}\ \tilde{K}_{ab} = \tilde{K}_{ba}\ \mathbf{then}\ key_e!\tilde{K}_e.skey!RemStr(\tilde{K}_{ab}, \tilde{x}).\mathbf{nil} \\
& \qquad\qquad \mathbf{else}\ (\mathbf{if}\ \tilde{K}^{\tilde{x}}_{ab} \neq \tilde{K}^{\tilde{x}}_{ba}\ \mathbf{then}\ alarm_a!0.\mathbf{nil} \| alarm_b!0.\mathbf{nil} \\
& \qquad\qquad\qquad \mathbf{else}\ fail!0.\mathbf{nil}))
\end{aligned}
$$

where to ease the notations, we let $\tilde{K}_{ab} = cmp(\tilde{K}_a, \tilde{B}_a, \tilde{B}_b)$, $\tilde{K}_{ba} = cmp(\tilde{K}_b, \tilde{B}_a, \tilde{B}_b)$, $\tilde{K}^{\tilde{x}}_{ab} = SubStr(\tilde{K}_{ab}, \tilde{x})$, and $\tilde{K}^{\tilde{x}}_{ba} = SubStr(\tilde{K}_{ba}, \tilde{x})$. Similar to Ran, the special measurement Ran' here, which takes three parameters, delivers a string of n bits. For example, $Ran_{\tilde{B}_a,\tilde{B}_e,\tilde{K}_a}[\tilde{q}; \tilde{K}_e]$ will first generate a string of $n - |\tilde{K}_{ae}|$ random bits $\tilde{x}$, replace with $\tilde{x}$ the substring of $\tilde{K}_a$ at the positions where $\tilde{B}_a$ and $\tilde{B}_e$ do not match, and store the string after the replacement in $\tilde{K}_e$.

7 Conclusion and related work

In our opinion, bisimulations should be considered as a proof methodology for demonstrating behavioural equivalence between systems, rather than providing the definition of the extensional behavioural equivalence itself. We have adapted the well-known *reduction barbed congruence* used for a variety of process calculi [20, 32, 11, 5], to obtain a touchstone extensional behavioural equivalence for quantum processes considered in [10]. In the literature there are also minor variations on the formulation of reduction barbed congruence, often called *contextual equivalence* or *barbed congruence*. See [11, 35] for a discussion of the differences.

We have defined a notion of open bisimulations, which provides both a sound and complete coinductive proof methodology for establishing the equivalence between qCCS processes. The operational semantics of this language is given in terms of probabilistic labelled transition systems. Moreover, we have generalised Hennessy-Milner logic to express the behaviour of quantum processes. In the resulting quantum logic, logical equivalence coincides with open bisimilarity.

To conclude this paper, we would like to compare the open bisimulation defined here with other bisimulations for quantum processes already proposed in the literature. Jorrand and Lalire [25, 27] defined a branching bisimulation for their QPAlg, which identifies quantum processes whose associated graphs have the same branching structure. However, their bisimulation cannot always distinguish different quantum operations, as quantum states are only compared when they are input or output. More seriously, the derived bisimilarity is not a congruence; it is not preserved by restriction. Bisimulation defined in [9] indeed distinguishes different quantum operations but it works well only for finite processes, since quantum states are compared after all actions have been performed. Again, it is not preserved by restriction, and whether it is preserved by parallel composition still remains open, although the positive answer is affirmed in two special cases. In [41], a congruent (strong) bisimulation was proposed for a special model where no classical datum is involved. However, as many important quantum communication protocols such as superdense coding and teleportation cannot be described in that model, the scope of its application is very limited. Furthermore, as all quantum operations are regarded as visible in [41], the bisimulation is too strong; it distinguishes two different sequences of quantum operations even when they have the same effect as a whole.

The first general (works for general models where both classical and quantum data are involved, and recursive definition is allowed), weak (quantum operations are regarded as invisible, so that they can be combined arbitrarily), and congruent bisimulation for quantum processes was defined in [10]. It differentiates quantum input, to match which an arbitrarily chosen super-operator should be considered, from other actions. The open bisimulation in this paper makes a step further by treating the super-operator application in an 'open' style: applying super-operators before an action to be matched is selected. This makes it possible to separate ground bisimulation and the closedness under super-operator application, and by doing so, we are able to provide not only a neater and simpler definition, but also a powerful technique for proving bisimilarity.

It is easy to prove that the bisimulation in [10] is both a ground bisimulation and closed under super-operator application. Then by Proposition 5.5, it is also an open bisimulation; in other words, the bisimilarity presented in the current paper is coarser than that defined in [10]. Whether or not they are actually the same is an interesting question, and we leave it for further investigation.

References

[1] Jos C. M. Baeten and W. P. Weijland. *Process Algebra*, volume 18 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1990.

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computer, Systems and Signal Processing*, pages 175–179, 1984.

[3] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Physical Review Letters*, 70:1895–1899, 1993.

[4] C.H. Bennett and S.J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.

[5] Yuxin Deng and Matthew Hennessy. On the semantics of markov automata. In *Proceedings of the 38th International Colloquium on Automata, Languages and Programming*, volume 6756 of *Lecture Notes in Computer Science*, pages 307–318. Springer, 2011.

[6] Yuxin Deng and Catuscia Palamidessi. Axiomatizations for probabilistic finite-state behaviors. *Theoretical Computer Science*, 373(1-2):92–114, 2007.

[7] Yuxin Deng, Rob van Glabbeek, Matthew Hennessy, and Carroll Morgan. Testing finitary probabilistic processes (extended abstract). In *Proceedings of the 20th International Conference on Concurrency Theory*, volume 5710 of *Lecture Notes in Computer Science*, pages 274–288. Springer, 2009.

[8] Yuxin Deng, Rob van Glabbeek, Carroll Morgan, and Chenyi Zhang. Scalar outcomes suffice for finitary probabilistic testing. In *Proceedings of the 16th European Symposium on Programming*, volume 4421 of *Lecture Notes in Computer Science*, pages 363–378. Springer, 2007.

[9] Y Feng, R Duan, Z Ji, and M Ying. Probabilistic bisimulations for quantum processes. *Information and Computation*, 205(11):1608–1639, 2007.

[10] Yuan Feng, Runyao Duan, and Mingsheng Ying. Bisimulation for quantum processes. In *Proceedings of the 38th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 523–534. ACM, 2011.

[11] Cédric Fournet and Georges Gonthier. A hierarchy of equivalences for asynchronous calculi. *Journal of Logic and Algebraic Programming*, 63(1):131–173, 2005.

[12] S. J. Gay and R. Nagarajan. Communicating quantum processes. In J. Palsberg and M. Abadi, editors, *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 145–157, 2005.

[13] SJ Gay and R Nagarajan. Types and typechecking for communicating quantum processes. *Mathematical Structures in Computer Science*, 16(03):375–406, 2006.

[14] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. ACM STOC*, pages 212–219, 1996.

[15] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 78(2):325, 1997.

[16] M. Hennessy. A proof system for communicating processes with value-passing. *Formal Aspects of Computer Science*, 3:346–366, 1991.

[17] M. Hennessy and A. Ingólfsdóttir. A theory of communicating processes value-passing. *Information and Computation*, 107(2):202–236, 1993.

[18] Matthew Hennessy and Robin Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the ACM*, 32(1):137–161, 1985.

[19] C. A. R. Hoare. *Communicating Sequential Processes*. Prentice Hall, 1985.

[20] Kohei Honda and Mario Tokoro. On asynchronous communication semantics. In P. Wegner M. Tokoro, O. Nierstrasz, editor, *Proceedings of the ECOOP '91 Workshop on Object-Based Concurrent Computing*, volume 612 of *LNCS 612*. Springer-Verlag, 1992.

[21] A. Jeffrey and J. Rathke. Contextual equivalence for higher-order pi-calculus revisited. *Logical Methods in Computer Science*, 1(1:4), 2005.

[22] Bengt Jonsson, C. Ho-Stuart, and Wang Yi. Testing and refinement for nondeterministic and probabilistic processes. In *Proceedings of the 3rd International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems*, volume 863 of *Lecture Notes in Computer Science*, pages 418–430. Springer, 1994.

[23] Bengt Jonsson and Wang Yi. Compositional testing preorders for probabilistic processes. In *Proceedings of the 10th Annual IEEE Symposium on Logic in Computer Science*, pages 431–441. Computer Society Press, 1995.

[24] Bengt Jonsson and Wang Yi. Testing preorders for probabilistic processes can be characterized by simulations. *Theoretical Computer Science*, 282(1):33–51, 2002.

[25] P. Jorrand and M. Lalire. Toward a quantum process algebra. In P. Selinger, editor, *Proceedings of the 2nd International Workshop on Quantum Programming Languages, 2004*, page 111, 2004.

[26] K. Kraus. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Springer, 1983.

[27] Marie Lalire. Relations among quantum processes: Bisimilarity and congruence. *Mathematical Structures in Computer Science*, 16(3):407–428, 2006.

[28] R. Milner. *Communication and Concurrency*. Prentice-Hall, 1989.

[29] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, parts i and ii. *Information and Computation*, 100:1–77, 1992.

[30] M. Nielsen and I. Chuang. *Quantum computation and quantum information*. Cambridge univer- sity press, 2000.

[31] Martin L. Puterman. *Markov Decision Processes*. Wiley, 1994.

[32] Julian Rathke and Pawel Sobocinski. Deriving structural labelled transitions for mobile ambients. In *Proceedings of the 19th International Conference on Concurrency Theory*, volume 5201 of *Lecture Notes in Computer Science*, pages 462–476. Springer, 2008.

[33] Julian Rathke and Pawel Sobocinski. Making the unobservable, unobservable. *Electronic Notes in Computer Science*, 229(3):131–144, 2009.

[34] D. Sangiorgi, N. Kobayashi, and E. Sumii. Environmental bisimulations for higher-order languages. In *Proceedings of the 22nd IEEE Symposium on Logic in Computer Science*, pages 293–302. IEEE Computer Society, 2007.

[35] D. Sangiorgi and D. Walker. *The π-calculus: a Theory of Mobile Processes*. Cambridge University Press, 2001.

[36] Davide Sangiorgi. A theory of bisimulation for the pi-calculus. *Acta Informatica*, 33(1):69–97, 1996.

[37] Roberto Segala. Modeling and verification of randomized distributed real-time systems. Technical Report MIT/LCS/TR-676, PhD thesis, MIT, Dept. of EECS, 1995.

[38] Roberto Segala and Nancy A. Lynch. Probabilistic simulations for probabilistic processes. *Nordic Journal of Computing*, 2(2):250–273, 1995.

[39] P. W. Shor. Algorithms for quantum computation: discrete log and factoring. In *Proceedings of the 35th IEEE FOCS*, pages 124–134, 1994.

[40] J. von Neumann. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Princeton University Press, 1955.

[41] M Ying, Y Feng, R Duan, and Z Ji. An algebra of quantum processes. *ACM Transactions on Computational Logic (TOCL)*, 10(3):1–36, 2009.