Symbolic bisimulation for quantum processes

YUAN FENG
University of Technology, Sydney, Australia, and Tsinghua University, China
YUXIN DENG
Shanghai Jiao Tong University, China
and MINGSHENG YING
University of Technology, Sydney, Australia, and Tsinghua University, China

With the previous notions of bisimulation presented in the literature, to check if two quantum processes are bisimilar, we have to instantiate their free quantum variables with arbitrary quantum states, and verify the bisimilarity of the resulting configurations. This makes checking bisimilarity infeasible from an algorithmic point of view, because quantum states constitute a continuum. In this paper, we introduce a *symbolic* operational semantics for quantum processes directly at the quantum operation level, which allows us to describe the bisimulation between quantum processes without resorting to quantum states. We show that the symbolic bisimulation defined here is equivalent to the open bisimulation for quantum processes in previous work, when strong bisimulations are considered. An algorithm for checking symbolic ground bisimilarity is presented. We also give a modal logical characterisation for quantum bisimilarity based on an extension of Hennessy-Milner logic to quantum processes.

Categories and Subject Descriptors: D.3.1 [**Programming Languages**]: Formal Definitions and Theory; F.3.1 [**Logics and Meanings of Programs**]: Specifying and Verifying and Reasoning about Programs

General Terms: Languages, Theory, Verification

Additional Key Words and Phrases: Bisimulation, Symbolic bisimulation, quantum processes

ACM Reference Format:
Yuan Feng, Yuxin Deng, and Mingsheng Ying, 2013. Symbolic bisimulation for quantum processes. ACM Trans. Comput. Logic 0, 0, Article 0 (0), 32 pages.
DOI = 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

1. INTRODUCTION

An important issue in quantum process algebra is to discover a quantum generalisation of bisimulation preserved by various process constructs, in particular, parallel composition, where one of the major differences between classical and quantum systems, namely quantum entanglement, is present. Jorrand and Lalire [Jorrand and

This work was supported by Australian ARC grants DP110103473, DP130102764, and FT100100218. Y. F. and M. Y. are also supported by the Overseas Team Program of Academy of Mathematics and Systems Science, Chinese Academy of Sciences. Y.D. was partially supported by the National Natural Science Foundation of China (61173033, 61033002) and the NSFC-ANR joint project (61261130589). Authors' addresses: Y. F. and M. Y.: Centre of Quantum Computation & Intelligent Systems (QCIS), Faculty of Information Technology, University of Technology, Sydney, City Campus, 15 Broadway, Ultimo, NSW 2007, Australia, and State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China. Y. D.: Department of Computer Science and Engineering, School of Electronics and Informatics, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China. Email addresses: Y. F., Yuan.Feng@uts.edu.au; Y. D., deng-yx@cs.sjtu.edu.cn; M. Y., Mingsheng.Ying@uts.edu.au.

DOI 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

Lalire 2004; Lalire 2006] defined a branching bisimulation for their *Quantum Process Algebra* (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 communicated. Moreover, the derived bisimilarity is not a congruence; it is not preserved by restriction. Bisimulation defined in [Feng et al. 2007] indeed distinguishes different quantum operations but it works well only for finite processes. Again, it is not preserved by restriction. In [Ying et al. 2009], a congruent bisimulation was proposed for a special model where no classical datum is involved. However, as many important quantum communication protocols such as super-dense coding and teleportation cannot be described in that model, the scope of its application is very limited.

A general notion of bisimulation for the quantum process algebra qCCS developed by the authors was found in [Feng et al. 2011; 2012], which enjoys the following nice features: (1) it is applicable to general models where both classical and quantum data are involved, and recursion is allowed; (2) it is preserved by all the standard process constructs, including parallel composition; and (3) quantum operations are regarded as invisible, so that they can be combined arbitrarily. Independently, a bisimulation congruence in *Communicating Quantum Processes* (CQP), developed by Gay and Nagarajan [Gay and Nagarajan 2005], was established by Davidson [Davidson 2011]. Later on, motivated by [Sangiorgi 1996], an open bisimulation for quantum processes was defined in [Deng and Feng 2012] that makes it possible to separate ground bisimulation and the closedness under super-operator applications, thus providing not only a neater and simpler definition, but also a new technique for proving bisimilarity. It is worth noting that a group from University of Tokyo and NTT Corporation [Kubota et al. 2012] has already implemented a software tool to decide bisimilarity of qCCS configurations, and used it to check the security of BB84 quantum key distribution protocol [Bennett and Brassard 1984].

The various bisimulations defined in the literature, however, have a common shortcoming: they all resort to the instantiation of quantum variables by quantum states. As a result, to check whether or not two processes are bisimilar, we have to accompany them with arbitrarily chosen quantum states, and check if the resultant configurations are bisimilar. Note that all quantum states constitute a continuum. The verification of bisimilarity is actually infeasible from an algorithmic point of view. The aim of the present paper is to tackle this problem with the powerful symbolic bisimulation technique [Hennessy and Lin 1995; Burch et al. 1992]. This paper only considers qCCS, but the ideas and techniques developed here apply to other quantum process algebras.

As a quantum extension of value-passing CCS, qCCS has both (possibly infinite) classical data domain and (doomed-to-be infinite) quantum data domain. The possibly infinite classical data set can be dealt with by symbolic bisimulation [Hennessy and Lin 1995] for classical process algebras directly. However, in qCCS, we are also faced with the additional difficulty caused by the infinity of all quantum states. The current paper solves this problem by introducing super-operator valued distributions, which allows us to fold the operational semantics of qCCS into a symbolic version and provides us with a notion, also called symbolic bisimulation for simplicity, where to check the bisimilarity of two quantum processes, only a finite number of process-superoperator pairs need to be considered, without appealing to quantum states. To be specific, we propose

— a symbolic operational semantics of qCCS in which quantum processes are described directly by the super-operators they can perform. It also incorporates a symbolic treatment for classical data.

— a notion of (strong) symbolic bisimulation, based on the symbolic operational semantics, as well as an efficient algorithm to check its ground version. Note that previous bisimulations proposed in the literature are all weak ones where internal actions are abstracted. However, for technical reasons, we only consider strong bisimulation in this paper.
— the coincidence of symbolic bisimulation with the open bisimulation defined in [Deng and Feng 2012], when strong bisimulation is considered.
— a modal characterisation of symbolic bisimulation by a quantum logic as an extension of Hennessy-Milner logic.

The remainder of the paper is organised as follows. In Section 2, we review some basic notions from linear algebra and quantum mechanics. The syntax and (ordinary) operational semantics of qCCS are presented in Section 3. We also review the definition of open bisimulation presented in [Deng and Feng 2012]. Section 4 collects some definitions and properties of the semiring of completely positive super-operators. The notion of super-operator valued distributions, which serves as an extension of probabilistic distributions, is also defined. Section 5 is the main part of this paper where we present a symbolic operational semantics of qCCS which describes the execution of quantum processes without resorting to concrete quantum states. Based on it, symbolic bisimulation between quantum processes, which also incorporates a symbolic treatment for classical data, motivated by symbolic bisimulation for classical processes, is presented and shown to be equivalent to the open bisimulation in Section 3. Section 6 is devoted to proposing an algorithm to check symbolic ground bisimulation, which is applicable to reasoning about the correctness of many existing quantum communication protocols. In Section 7 we propose a modal logic which turns out to be both sound and complete with respect to the symbolic bisimulation. We outline the main results in Section 8 and point out some directions for further study. In particular, we suggest the potential application of our results in model checking quantum communication protocols.

2. PRELIMINARIES

For the convenience of the reader, we briefly recall some basic notions from linear algebra and quantum theory which are needed in this paper. For more details, we refer to [Nielsen and Chuang 2000].

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 *normalised* 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 normalised 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* states that the set of all normalised

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 $\mathcal{H}$. The *trace* of A 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 the trace function is actually independent of the orthonormal basis selected. It is also easy to check that the 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 respect 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 respect to $\mathcal{H}_2$. Partial trace functions are also independent of the orthonormal basis selected.

Traditionally, a linear operator $\mathcal{E}$ on $\mathcal{L}(\mathcal{H})$ is called a $super\text{-}operator$ on $\mathcal{H}$. A super-operator is said to be *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* [Kraus 1983] of completely positive super-operators states that a super-operator $\mathcal{E}$ is completely positive if and only if there is some set of operators $\{E_i : i \in I\}$ with appropriate dimension such that

$$\mathcal{E}(A) = \sum_{i \in I} E_i A E_i^\dagger$$

for any $A \in \mathcal{L}(\mathcal{H})$. The operators E_i are called Kraus operators of $\mathcal{E}$. We abuse the notation slightly by denoting $\mathcal{E} = \{E_i : i \in I\}$. A super-operator $\mathcal{E}$ is said to be *trace-nonincreasing* if $\mathrm{tr}(\mathcal{E}(A)) \leq \mathrm{tr}(A)$ for any positive $A \in \mathcal{L}(\mathcal{H})$, and *trace-preserving* if the equality always holds. Equivalently, a super-operator is trace-nonincreasing completely positive (resp. trace-preserving completely positive) if and only if its Kraus operators E_i satisfy $\sum_i E_i^\dagger E_i \leq I$ (resp. $\sum_i E_i^\dagger E_i = I$). In this paper, we will use some

well-known (unitary) super-operators listed as follows: the quantum control-not super-operator $\mathcal{CN} = \{C_N\}$ performed on two qubits where

$$C_N = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

the 1-qubit Hadamard super-operator $\mathcal{H} = \{H\}$, and Pauli super-operators $\sigma^0 = \{I_2\}, \sigma^1 = \{X\}, \sigma^2 = \{Z\}$, and $\sigma^3 = \{Y\}$ where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

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

We also use the notations $\mathcal{X}, \mathcal{Z}$, and $\mathcal{Y}$ to denote σ^1, σ^2, and σ^3, respectively.

2.2. Basic quantum mechanics

According to von Neumann's formalism of quantum mechanics [von Neumann 1955], 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 normalised 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 a density operator is a 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. As a pure state can be regarded as a special mixed state, in this paper we use the term *quantum state* to denote a mixed state, or equivalently, a density operator. 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 the tensor product of the reduced states on its component systems. A well-known example is the 2-qubit state

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

which appears repeatedly in our examples in this paper. This kind of state is called an *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 the classical world, and is the key to many quantum information processing tasks such as teleportation [Bennett et al. 1993] and super-dense coding [Bennett and Wiesner 1992].

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

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

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 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 with a fixed state is provided, non-degenerate measurements together with unitary operators are sufficient to implement general measurements.

3. QCCS: SYNTAX AND SEMANTICS

In this section, we briefly review the syntax and semantics of a quantum extension of value-passing CCS [Milner 1989; Hennessy and Ingólfsdóttir 1993], called qCCS, studied in [Feng et al. 2007; Ying et al. 2009; Feng et al. 2011; 2012], and the definition of open bisimulation between qCCS processes presented in [Deng and Feng 2012].

3.1. Syntax

We assume three types of data in qCCS: Bool for booleans, real numbers Real for classical data, and qubits Qbt for quantum data. Let $cVar$, ranged over by $x, y, \ldots$, be the set of classical variables, and $qVar$, ranged over by $q, r, \ldots$, the set of quantum variables. It is assumed that $cVar$ and $qVar$ are both countably infinite. We assume a set Exp of classical data expressions over `Real`, which includes $cVar$ as a subset and is ranged over by $e, e', \ldots$, and a set of boolean-valued expressions $BExp$, ranged over by $b, b', \ldots$, with the usual set of boolean operators `tt`, `ff`, $\neg$, $\wedge$, $\vee$, 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. Let $cChan$ be the set of classical channel names, ranged over by $c, d, \ldots$, and $qChan$ the set of quantum channel names, ranged over by $\mathtt{c}, \mathtt{d}, \ldots$. Let

$Chan = cChan \cup qChan$. A relabelling function f is a one to one function from $Chan$ to $Chan$ such that $f(cChan) \subseteq cChan$ and $f(qChan) \subseteq qChan$.

We often abbreviate the indexed set $\{q_1, \ldots, q_n\}$ to $\widetilde{q}$ when $q_1, \ldots, q_n$ are distinct quantum variables and the dimension n is understood. Sometimes we also use $\widetilde{q}$ to denote the string $q_1 \ldots q_n$. We assume a set of process constant schemes, ranged over by $A, B, \ldots$. Assigned to each process constant scheme A there are two non-negative integers $ar_c(A)$ and $ar_q(A)$. If $\widetilde{x}$ is a tuple of classical variables with $|\widetilde{x}| = ar_c(A)$, and $\widetilde{q}$ a tuple of distinct quantum variables with $|\widetilde{q}| = ar_q(A)$, then $A(\widetilde{x}, \widetilde{q})$ is called a process constant. When $ar_c(A) = ar_q(A) = 0$, we also denote by A the (unique) process constant produced by A.

Based on these notations, the syntax of qCCS terms can be given by the Backus-Naur form as

$$\begin{aligned} t &::= \mathbf{nil} \mid A(\widetilde{e}, \widetilde{q}) \mid \alpha.t \mid t + t \mid t \| t \mid t\backslash L \mid t[f] \mid \mathbf{if}\ b\ \mathbf{then}\ t \\ \alpha &::= \tau \mid c?x \mid c!e \mid \mathsf{c}?q \mid \mathsf{c}!q \mid \mathcal{E}[\widetilde{q}] \mid M[\widetilde{q}; x] \end{aligned}$$

where $c \in cChan$, $x \in cVar$, $\mathsf{c} \in qChan$, $q \in qVar$, $\widetilde{q} \subseteq qVar$, $e \in Exp$, $\widetilde{e} \subseteq Exp$, τ is the silent action, $A(\widetilde{x}, \widetilde{q})$ is a process constant, f is a relabelling function, $L \subseteq Chan$, $b \in BExp$, and $\mathcal{E}$ and M are respectively a trace-preserving super-operator and a non-degenerate projective measurement applying on the Hilbert space associated with the systems $\widetilde{q}$. In this paper, we assume all super-operators are completely positive.

To exclude quantum processes which are not physically implementable, we also require $q \notin qv(t)$ in $\mathsf{c}!q.t$ and $qv(t) \cap qv(u) = \emptyset$ in $t \| u$, where for a process term t, $qv(t)$ is the set of its free quantum variables inductively defined as follows:

$$\begin{aligned} qv(\mathbf{nil}) &= \emptyset & qv(\tau.t) &= qv(t) \\ qv(c?x.t) &= qv(t) & qv(c!e.t) &= qv(t) \\ qv(\mathsf{c}?q.t) &= qv(t) - \{q\} & qv(\mathsf{c}!q.t) &= qv(t) \cup \{q\} \\ qv(\mathcal{E}[\widetilde{q}].t) &= qv(t) \cup \widetilde{q} & qv(M[\widetilde{q}; x].t) &= qv(t) \cup \widetilde{q} \\ qv(t + u) &= qv(t) \cup qv(u) & qv(t \| u) &= qv(t) \cup qv(u) \\ qv(t[f]) &= qv(t) & qv(t\backslash L) &= qv(t) \\ qv(\mathbf{if}\ b\ \mathbf{then}\ t) &= qv(t) & qv(A(\widetilde{e}, \widetilde{q})) &= \widetilde{q}. \end{aligned}$$

The notion of free classical variables in quantum processes, denoted by $fv(\cdot)$, can be defined in the usual way with the only modification that the quantum measurement prefix $M[\widetilde{q}; x]$ has binding power on x. A quantum process term t is closed if $fv(t) = \emptyset$. We let $\mathcal{T}$, ranged over by $t, u, \cdots$, be the set of all qCCS terms, and $\mathcal{P}$, ranged over by $P, Q, \cdots$, the set of closed terms. To complete the definition of qCCS syntax, we assume that for each process constant $A(\widetilde{x}, \widetilde{q})$, there is a defining equation

$$A(\widetilde{x}, \widetilde{q}) \stackrel{def}{=} t$$

where $fv(t) \subseteq \widetilde{x}$ and $qv(P) \subseteq \widetilde{q}$. Throughout the paper we implicitly assume that process terms are identified up to α-conversion.

The process constructs we give here are quite similar to those in classical CCS, and they also have similar intuitive meanings: **nil** stands for a process which does not perform any action; $c?x$ and $c!e$ are respectively classical input and classical output, while $\mathsf{c}?q$ and $\mathsf{c}!q$ are their quantum counterparts. $\mathcal{E}[\widetilde{q}]$ denotes the action of performing the super-operator $\mathcal{E}$ on the qubits $\widetilde{q}$ while $M[\widetilde{q}; x]$ measures the qubits $\widetilde{q}$ according to M and the measurement outcome is substituted for the classical variable x. $+$ models nondeterministic choice: $t + u$ behaves like either t or u depending on the choice of the environment. $\|$ denotes the usual parallel composition. The operators $\backslash L$ and $[f]$ model restriction and relabelling, respectively: $t\backslash L$ behaves like t as long as any action through the channels in L is forbidden, and $t[f]$ behaves like t where each channel

name is replaced by its image under the relabelling function f. Finally, **if** b **then** t is the standard conditional choice where t can be executed only if b is $\mathtt{tt}$.

An evaluation ψ is a function from $cVar$ to Real; it can be extended in an obvious way to functions from Exp to Real and from $BExp$ to $\{\mathtt{tt}, \mathtt{ff}\}$, and finally, from $\mathcal{T}$ to $\mathcal{P}$. For simplicity, we still use ψ to denote these extensions. Let $\psi\{v/x\}$ be the evaluation which differs from ψ only in that it maps x to v.

3.2. Transitional semantics

For each quantum variable $q \in qVar$, we assume a 2-dimensional Hilbert space $\mathcal{H}_q$ to be the state space of the q-system. For any $S \subseteq qVar$, we denote

$$\mathcal{H}_S = \bigotimes_{q \in S} \mathcal{H}_q.$$

In particular, $\mathcal{H} = \mathcal{H}_{qVar}$ is the state space of the whole environment consisting of all the quantum variables. Note that $\mathcal{H}$ is a countably-infinite dimensional Hilbert space.

Suppose P is a closed quantum process. A pair of the form $\langle P, \rho\rangle$ is called a configuration, where $\rho \in \mathcal{D}(\mathcal{H})$ is a density operator on $\mathcal{H}$ (As $\mathcal{H}$ is infinite dimensional, ρ should be understood as a density operator on some finite dimensional subspace of $\mathcal{H}$ which contains $\mathcal{H}_{qv(P)}$). The set of configurations is denoted Con, and ranged over by $\mathcal{C}, \mathcal{D}, \cdots$. Let

$$Act_c \;=\; \{\tau\} \cup \{c?v, c!v \mid c \in cChan, v \in \mathsf{Real}\} \cup \{\mathsf{c}?r, \mathsf{c}!r \mid \mathsf{c} \in qChan, r \in qVar\}.$$

For each $\alpha \in Act_c$, we define the bound quantum variables $qbv(\alpha)$ of α as $qbv(\mathsf{c}?r) = \{r\}$ and $qbv(\alpha) = \emptyset$ if α is not a quantum input. The set of channel names used in action α is denoted by $cn(\alpha)$; that is, $cn(c?v) = cn(c!v) = \{c\}$, $cn(\mathsf{c}?r) = cn(\mathsf{c}!r) = \{\mathsf{c}\}$, and $cn(\tau) = \emptyset$. We also extend the relabelling function to Act_c in an obvious way.

Let $Dist(Con)$, ranged over by $\mu, \nu, \cdots$, be the set of all finite-supported probabilistic distributions over Con. Then the operational semantics of qCCS can be given by the probabilistic labelled transition system (pLTS) $\langle Con, Act_c, \longmapsto\rangle$, where $\longmapsto \subseteq Con \times Act_c \times Dist(Con)$ is the smallest relation satisfying the inference rules depicted in Fig. 1. The symmetric forms for rules Par_c, $C\text{-}Com_c$, $Q\text{-}Com_c$, and Sum_c are omitted.

In these rules, we abuse the notation slightly by writing $\mathcal{C} \stackrel{\alpha}{\longmapsto} \mathcal{D}$ if $\mathcal{C} \stackrel{\alpha}{\longmapsto} \mu$ where μ is the simple distribution such that $\mu(\mathcal{D}) = 1$. We also use the obvious extension of the function $\|$ on configurations to distributions. To be precise, if $\mu = \sum_{i\in I} p_i\langle P_i, \rho_i\rangle$ then $\mu\|Q$ denotes the distribution $\sum_{i\in I} p_i\langle P_i\|Q, \rho_i\rangle$. Similar extension applies to $\mu[f]$ and $\mu\backslash L$.

3.3. Open bisimulation

In this subsection, we recall the basic definitions and properties of open bisimulation introduced in [Deng and Feng 2012]. Let $\mathcal{R} \subseteq Con \times Con$ be a relation on configurations. We can lift $\mathcal{R}$ to a relation on $Dist(Con)$ by writing $\mu\mathcal{R}\nu$ if

(1) $\mu = \sum_{i\in I} p_i\mathcal{C}_i$,
(2) for each $i \in I$, $\mathcal{C}_i\mathcal{R}\mathcal{D}_i$ for some $\mathcal{D}_i$, and
(3) $\nu = \sum_{i\in I} p_i\mathcal{D}_i$.

Note that here the configurations $\mathcal{C}_i, i \in I$, are not necessarily distinct.

Definition 3.1. A symmetric relation $\mathcal{R} \subseteq Con \times Con$ is called a (strong) open bisimulation if for any $\langle P, \rho\rangle, \langle Q, \sigma\rangle \in Con$, $\langle P, \rho\rangle\mathcal{R}\langle Q, \sigma\rangle$ implies that

(1) $qv(P) = qv(Q)$, and $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$,

$$Tau_c \quad \frac{}{\langle \tau.P,\rho\rangle \overset{\tau}{\longmapsto} \langle P,\rho\rangle} \qquad C\text{-}Inp_c \quad \frac{v \in \mathsf{Real}}{\langle c?x.t,\rho\rangle \overset{c?v}{\longmapsto} \langle t\{v/x\},\rho\rangle}$$

$$C\text{-}Out_c \quad \frac{v = [\![e]\!]}{\langle c!e.P,\rho\rangle \overset{c!v}{\longmapsto} \langle P,\rho\rangle} \qquad Q\text{-}Inp_c \quad \frac{r \notin qv(\mathsf{c}?q.P)}{\langle \mathsf{c}?q.P,\rho\rangle \overset{\mathsf{c}?r}{\longmapsto} \langle P\{r/q\},\rho\rangle}$$

$$Q\text{-}Out_c \quad \frac{}{\langle \mathsf{c}!q.P,\rho\rangle \overset{\mathsf{c}!q}{\longmapsto} \langle P,\rho\rangle} \qquad Oper_c \quad \frac{}{\langle \mathcal{E}[\widetilde{r}].P,\rho\rangle \overset{\tau}{\longmapsto} \langle P,\mathcal{E}_{\widetilde{r}}(\rho)\rangle}$$

$$Meas_c \quad \frac{M = \sum_{i\in I}\lambda_i E^i,\ p_i = \mathrm{tr}(E^i_{\widetilde{r}}\rho)}{\langle M[\widetilde{r};x].P,\rho\rangle \overset{\tau}{\longmapsto} \sum_{i\in I} p_i\langle P\{\lambda_i/x\}, E^i_{\widetilde{r}}\rho E^i_{\widetilde{r}}/p_i\rangle} \qquad Par_c \quad \frac{\langle P_1,\rho\rangle \overset{\alpha}{\longmapsto} \mu,\ qbv(\alpha)\cap qv(P_2)=\emptyset}{\langle P_1\|P_2,\rho\rangle \overset{\alpha}{\longmapsto} \mu\|P_2}$$

$$C\text{-}Com_c \quad \frac{\langle P_1,\rho\rangle \overset{c?v}{\longmapsto} \langle P_1',\rho\rangle,\ \langle P_2,\rho\rangle \overset{c!v}{\longmapsto} \langle P_2',\rho\rangle}{\langle P_1\|P_2,\rho\rangle \overset{\tau}{\longmapsto} \langle P_1'\|P_2',\rho\rangle} \qquad Q\text{-}Com_c \quad \frac{\langle P_1,\rho\rangle \overset{\mathsf{c}?r}{\longmapsto} \langle P_1',\rho\rangle,\quad \langle P_2,\rho\rangle \overset{\mathsf{c}!r}{\longmapsto} \langle P_2',\rho\rangle}{\langle P_1\|P_2,\rho\rangle \overset{\tau}{\longmapsto} \langle P_1'\|P_2',\rho\rangle}$$

$$Sum_c \quad \frac{\langle P,\rho\rangle \overset{\alpha}{\longmapsto} \mu}{\langle P+Q,\rho\rangle \overset{\alpha}{\longmapsto} \mu} \qquad Rel_c \quad \frac{\langle P,\rho\rangle \overset{\alpha}{\longmapsto} \mu}{\langle P[f],\rho\rangle \overset{f(\alpha)}{\longmapsto} \mu[f]}$$

$$Cho_c \quad \frac{\langle P,\rho\rangle \overset{\alpha}{\longmapsto} \mu,\ [\![b]\!] = \mathtt{tt}}{\langle \mathbf{if}\ b\ \mathbf{then}\ P,\rho\rangle \overset{\alpha}{\longmapsto} \mu} \qquad Res_c \quad \frac{\langle P,\rho\rangle \overset{\alpha}{\longmapsto} \mu,\ cn(\alpha)\cap L=\emptyset}{\langle P\backslash L,\rho\rangle \overset{\alpha}{\longmapsto} \mu\backslash L}$$

$$Def_c \quad \frac{\langle t\{\widetilde{v}/\widetilde{x},\widetilde{r}/\widetilde{q}\},\rho\rangle \overset{\alpha}{\longmapsto} \mu,\ A(\widetilde{x},\widetilde{q}) \overset{def}{=} t}{\langle A(\widetilde{v},\widetilde{r}),\rho\rangle \overset{\alpha}{\longmapsto} \mu}$$

Fig. 1. Operational semantics of qCCS. We denote by $[\![e]\!]$ the evaluation of e, and $\mathcal{E}_{\widetilde{r}}$ the super-operator $\mathcal{E}$ acting on quantum system r.

(2) for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P)}}$ (Again, $\mathcal{E}$ should be understood as a super-operator on some finite dimensional subspace of $\mathcal{H}_{\overline{qv(P)}}$), whenever $\langle P,\mathcal{E}(\rho)\rangle \overset{\alpha}{\longmapsto} \mu$, there exists ν such that $\langle Q,\mathcal{E}(\sigma)\rangle \overset{\alpha}{\longmapsto} \nu$ and $\mu\mathcal{R}\nu$.

Definition 3.2.

(1) Two quantum configurations $\langle P,\rho\rangle$ and $\langle Q,\sigma\rangle$ are open bisimilar, denoted by $\langle P,\rho\rangle \dot{\sim} \langle Q,\sigma\rangle$, if there exists an open bisimulation $\mathcal{R}$ such that $\langle P,\rho\rangle\mathcal{R}\langle Q,\sigma\rangle$;
(2) Two quantum process terms t and u are open bisimilar, denoted by $t \dot{\sim} u$, if for any quantum state $\rho \in \mathcal{D}(\mathcal{H})$ and any evaluation ψ, $\langle t\psi,\rho\rangle \dot{\sim} \langle u\psi,\rho\rangle$.

To illustrate the operational semantics and open bisimulation presented in this section, we give a simple example.

Example 3.3. This example shows two alternative ways of setting a quantum system to the pure state $|0\rangle$. Let $P \overset{def}{=} Set^0[q].\mathcal{I}[q].\mathbf{nil}$ and

$$Q \overset{def}{=} M_{0,1}[q;x].(\mathbf{if}\ x=0\ \mathbf{then}\ \mathcal{I}[q].\mathbf{nil}\ +\mathbf{if}\ x=1\ \mathbf{then}\ \mathcal{X}[q].\mathbf{nil}),$$

where $Set^0 = \{|0\rangle\langle 0|, |0\rangle\langle 1|\}$, $M_{0,1}$ is the 1-qubit measurement according to the computational basis $\{|0\rangle,|1\rangle\}$, $\mathcal{I}$ is the identity super-operator, and $\mathcal{X}$ is the Pauli-X super-operator. For any $\rho \in \mathcal{D}(\mathcal{H})$, the pLTSs rooted by $\langle P,\rho\rangle$ and $\langle Q,\rho\rangle$ respectively are depicted in Fig. 2 where

$$Q_0 \overset{def}{=} \mathbf{if}\ 0=0\ \mathbf{then}\ \mathcal{I}[q].\mathbf{nil}\ +\mathbf{if}\ 0=1\ \mathbf{then}\ \mathcal{X}[q].\mathbf{nil},$$
$$Q_1 \overset{def}{=} \mathbf{if}\ 1=0\ \mathbf{then}\ \mathcal{I}[q].\mathbf{nil}\ +\mathbf{if}\ 1=1\ \mathbf{then}\ \mathcal{X}[q].\mathbf{nil},$$

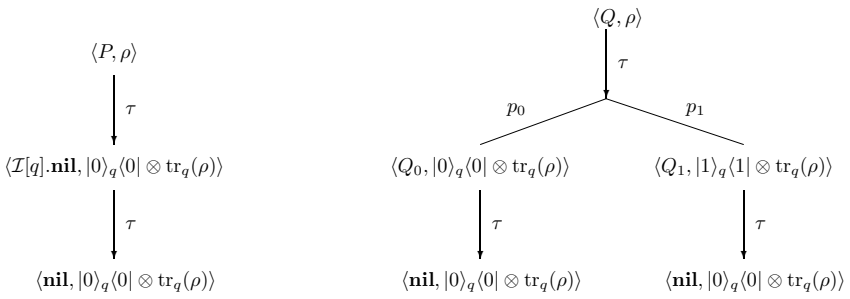


Fig. 2. pLTSs for the two ways of setting a quantum system to $|0\rangle$

and $p_i = \mathrm{tr}(|i\rangle\langle i|_q \cdot \rho)$. Note that both P and Q are free of quantum input. We can show $P \dot{\sim} Q$ easily by verifying that the relation $\mathcal{R} \cup \mathcal{R}^{-1}$, where

$$\begin{aligned}\mathcal{R} \;=\; \{&(\langle P, \rho\rangle, \langle Q, \rho\rangle), (\langle \mathcal{I}[q].\mathbf{nil}, \rho_0\rangle, \langle Q_0, \rho_0\rangle),\\ &(\langle \mathcal{I}[q].\mathbf{nil}, \rho_0\rangle, \langle Q_1, \rho_1\rangle), (\langle \mathbf{nil}, \rho_0\rangle, \langle \mathbf{nil}, \rho_0\rangle) : \rho \in \mathcal{D}(\mathcal{H})\}\end{aligned}$$

and $\rho_i = |i\rangle\langle i|_q \otimes \mathrm{tr}_q\rho$, is an open bisimulation.

4. SUPER-OPERATOR VALUED DISTRIBUTIONS

One of the aims of this paper is to propose a symbolic operational semantics for qCCS, in which the behaviour of a quantum process is described not by the effect on specific quantum states, but by the accumulated super-operators they can perform. To this end, we need to replace the probabilities occurring in quantum measurements by super-operators, and accordingly, extend the ordinary probabilistic distributions to super-operator valued distributions.

4.1. Semiring of super-operators

We denote by $\mathcal{S}(\mathcal{H})$ the set of super-operators on $\mathcal{H}$, ranged over by $\mathcal{A}, \mathcal{B}, \cdots$. Obviously, both $(\mathcal{S}(\mathcal{H}), 0_\mathcal{H}, +)$ and $(\mathcal{S}(\mathcal{H}), \mathcal{I}_\mathcal{H}, \circ)$ are monoids, where $\mathcal{I}_\mathcal{H}$ and $0_\mathcal{H}$ are the identity and null super-operators on $\mathcal{H}$, respectively, and $\circ$ is the composition of super-operators defined by $(\mathcal{A} \circ \mathcal{B})(\rho) = \mathcal{A}(\mathcal{B}(\rho))$ for any $\rho \in \mathcal{D}(\mathcal{H})$. We always omit the symbol $\circ$ and write $\mathcal{A}\mathcal{B}$ directly for $\mathcal{A} \circ \mathcal{B}$. Furthermore, the operation $\circ$ is (both left and right) distributive with respect to $+$:

$$\mathcal{A}(\mathcal{B}_1 + \mathcal{B}_2) = \mathcal{A}\mathcal{B}_1 + \mathcal{A}\mathcal{B}_2, \;\; (\mathcal{B}_1 + \mathcal{B}_2)\mathcal{A} = \mathcal{B}_1\mathcal{A} + \mathcal{B}_2\mathcal{A}.$$

Thus $(\mathcal{S}(\mathcal{H}), +, \circ)$ forms a semiring.

For any $\mathcal{A}, \mathcal{B} \in \mathcal{S}(\mathcal{H})$ and $V \subseteq qVar$, we write $\mathcal{A} \lesssim_V \mathcal{B}$ if for any $\rho \in \mathcal{D}(\mathcal{H})$, $\mathrm{tr}_{\overline{V}}(\mathcal{A}(\rho)) \sqsubseteq \mathrm{tr}_{\overline{V}}(\mathcal{B}(\rho))$, where $\overline{V}$ is the complement set of V in $qVar$, and $\sqsubseteq$ is the Löwner preorder defined on operators such as $A \sqsubseteq B$ if and only if $B - A$ is positive semi-definite. Let $\eqsim_V$ be $\lesssim_V \cap \gtrsim_V$. We usually abbreviate $\lesssim_\emptyset$ and $\eqsim_\emptyset$ to $\lesssim$ and $\eqsim$, respectively. It is easy to check that if $\mathcal{A}$ and $\mathcal{B}$ have Kraus operators $\{A_i : i \in I\}$ and $\{B_j : j \in J\}$ respectively, then $\mathcal{A} \lesssim \mathcal{B}$ if and only if $\sum_{i\in I} A_i^\dagger A_i \sqsubseteq \sum_{j\in J} B_j^\dagger B_j$. The following proposition is direct from definitions:

PROPOSITION 4.1. *Let $\mathcal{A}$ and $\mathcal{B} \in \mathcal{S}(\mathcal{H})$. Then*

(1) $\mathcal{A} \eqsim \mathcal{I}_\mathcal{H}$ if and only if $\mathcal{A}$ is trace-preserving, i.e., $\mathrm{tr}(\mathcal{A}(\rho)) = \mathrm{tr}(\rho)$ *for any* $\rho \in \mathcal{D}(\mathcal{H})$.
(2) $\mathcal{A} \eqsim 0_\mathcal{H}$ if and only if $\mathcal{A} = 0_\mathcal{H}$.

The next lemma, which is easy from definition, shows that the equivalence relation $\eqsim_V$ is preserved by the right application of composition.

LEMMA 4.2. *Let $\mathcal{A}, \mathcal{A}', \mathcal{B} \in \mathcal{S}(\mathcal{H})$ and $V \subseteq qVar$. If $\mathcal{A} \eqsim_V \mathcal{A}'$, then $\mathcal{A}\mathcal{B} \eqsim_V \mathcal{A}'\mathcal{B}$.*

However, $\eqsim$ is not preserved by composition from the left-hand side. A counter-example is when $\mathcal{A}$ is the X-Pauli super-operator, and $\mathcal{B}$ has one single Kraus operator $|0\rangle\langle 0|$. Then $\mathcal{A} \eqsim \mathcal{I}_\mathcal{H}$, but $\mathcal{B}\mathcal{A} \not\eqsim \mathcal{B}\mathcal{I}_\mathcal{H}$ since $\mathrm{tr}(\mathcal{B}\mathcal{A}(|0\rangle\langle 0|)) = 0$ while $\mathrm{tr}(\mathcal{B}\mathcal{I}_\mathcal{H}(|0\rangle\langle 0|)) = 1$. Nevertheless, we have the following property which is useful for later discussion.

LEMMA 4.3. *Let $\mathcal{A}, \mathcal{A}' \in \mathcal{S}(\mathcal{H})$ and $\mathcal{B} \in \mathcal{S}(\mathcal{H}_V)$ where $\emptyset \neq V \subseteq qVar$. If $\mathcal{A} \eqsim_V \mathcal{A}'$, then both $\mathcal{A}\mathcal{B} \eqsim_V \mathcal{A}'\mathcal{B}$ and $\mathcal{B}\mathcal{A} \eqsim_V \mathcal{B}\mathcal{A}'$.*

PROOF. Easy from the fact that $\mathrm{tr}_{\overline{V}}\mathcal{B}\mathcal{A}(\rho) = \mathcal{B}(\mathrm{tr}_{\overline{V}}\mathcal{A}(\rho))$ when $\mathcal{B} \in \mathcal{S}(\mathcal{H}_V)$. □

Let $\mathcal{S}_t(\mathcal{H}) \subseteq \mathcal{S}(\mathcal{H})$ be the set of trace-preserving super-operators, ranged over by $\mathcal{E}, \mathcal{F}, \cdots$. Obviously, $(\mathcal{S}_t(\mathcal{H}), \mathcal{I}_\mathcal{H}, \circ)$ is a sub-monoid of $\mathcal{S}(\mathcal{H})$ while $(\mathcal{S}_t(\mathcal{H}), 0_\mathcal{H}, +)$ is not. It is easy to check that for any $\mathcal{E}, \mathcal{F} \in \mathcal{S}_t(\mathcal{H})$ and $V \subseteq qVar$, $\mathcal{E} \lesssim_V \mathcal{F}$ if and only if $\mathcal{E} \eqsim_V \mathcal{F}$. So for trace-preserving super-operators, we usually use the more symmetric form $\eqsim_V$ instead of $\lesssim_V$.

4.2. Super-operator valued distributions

Let S be a countable set. A super-operator valued distribution, or simply distribution for short, Δ over S is a function from S to $\mathcal{S}(\mathcal{H})$ such that $\sum_{s\in S}\Delta(s) \eqsim \mathcal{I}_\mathcal{H}$. We denote by $\lceil\Delta\rceil$ the support set of Δ, *i.e.*, the set of s such that $\Delta(s) \neq 0_\mathcal{H}$. Let $\mathcal{D}ist_\mathcal{H}(S)$ be the set of finite-support super-operator valued distributions over S; that is,

$$\mathcal{D}ist_\mathcal{H}(S) \;=\; \{\Delta : S \to \mathcal{S}(\mathcal{H}) \mid \lceil\Delta\rceil \text{ is finite, and } \sum_{s\in\lceil\Delta\rceil}\Delta(s) \eqsim \mathcal{I}_\mathcal{H}\}.$$

Let $\Delta, \Xi, \cdots$ range over $\mathcal{D}ist_\mathcal{H}(S)$. Sometimes it is convenient to denote a distribution Δ by the explicit form $\sum_{i\in I}\mathcal{A}_i \bullet s_i$ where $\lceil\Delta\rceil = \{s_i \mid i \in I\}$ and $\Delta(s_i) = \mathcal{A}_i$ for each $i \in I$. When Δ is a simple distribution such that $\lceil\Delta\rceil = \{s\}$ for some s and $\Delta(s) = \mathcal{E}$, we abuse the notation slightly to denote Δ by $\mathcal{E} \bullet s$. We further abbreviate $\mathcal{I}_\mathcal{H} \bullet s$ to s. Note that there are infinitely many different simple distributions having the same support $\{s\}$.

Definition 4.4. Given $\{\Delta_i : i \in I\} \subseteq \mathcal{D}ist_\mathcal{H}(S)$ and $\{\mathcal{A}_i : i \in I\} \subseteq \mathcal{S}(\mathcal{H})$, $\sum_{i\in I}\mathcal{A}_i \eqsim \mathcal{I}_\mathcal{H}$, we define the combination, denoted by $\sum_{i\in I}\mathcal{A}_i \bullet \Delta_i$, to be a new distribution Δ such that

(1) $\lceil\Delta\rceil = \bigcup\{\lceil\Delta_i\rceil : i \in I, \mathcal{A}_i \neq 0_\mathcal{H}\}$,
(2) for any $s \in \lceil\Delta\rceil$, $\Delta(s) = \sum_{i\in I}\Delta_i(s)\mathcal{A}_i$.

Here and in the following of this paper, the index sets $I, J, K, \cdots$ are all assumed to be finite. By Lemma 4.2, it is easy to check that the above definition is well-defined. Furthermore, since $\eqsim$ is not preserved by left applications of composition, we cannot require $\Delta(s) = \sum_{i\in I}\mathcal{A}_i\Delta_i(s)$ in the second clause, although it seems more natural. As a result, we have $\mathcal{E} \bullet (\mathcal{F} \bullet s) = \mathcal{F}\mathcal{E} \bullet s$ and in general $\mathcal{F}\mathcal{E} \bullet s \neq \mathcal{E}\mathcal{F} \bullet s$.

Probability distributions can be regarded as special super-operator valued distributions by requiring that all super-operators appeared in the definitions above have the form $p\mathcal{I}_\mathcal{H}$ where $0 \leq p \leq 1$. Since in this case all super-operators commute, we always omit the bullet $\bullet$ in the expressions.

$$Act_s \quad \frac{\gamma = \tau, c?x, c!e, c?q, c!q}{(\!|\gamma.t, \mathcal{E}|\!) \xrightarrow{\mathtt{tt},\gamma} (\!|t, \mathcal{E}|\!)} \qquad Oper_s \quad \frac{}{(\!|\mathcal{F}[\widetilde{q}].t, \mathcal{E}|\!) \xrightarrow{\mathtt{tt},\tau} \mathcal{F}_{\widetilde{q}} \bullet (\!|t, \mathcal{F}_{\widetilde{q}}\mathcal{E}|\!)}$$

$$Meas_s \quad \frac{M = \sum_{i\in I} \lambda_i |\phi_i\rangle\langle\phi_i|}{(\!|M[\widetilde{q};x].t, \mathcal{E}|\!) \xrightarrow{\mathtt{tt},\tau} \sum_{i\in I} \mathcal{A}^{\phi_i}_{\widetilde{r}} \bullet (\!|t\{\lambda_i/x\}, Set^{\phi_i}_{\widetilde{r}}\mathcal{E}|\!)} \qquad Par_s \quad \frac{(\!|t, \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta}{(\!|t\|u, \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta\|u}, \ \begin{array}{l} bv(\gamma) \cap fv(u) = \emptyset \\ qbv(\gamma) \cap qv(u) = \emptyset \end{array}$$

$$C\text{-}Com_s \quad \frac{(\!|t, \mathcal{E}|\!) \xrightarrow{b_1,c?x} (\!|t', \mathcal{E}|\!), \quad (\!|u, \mathcal{E}|\!) \xrightarrow{b_2,c!e} (\!|u', \mathcal{E}|\!)}{(\!|t\|u, \mathcal{E}|\!) \xrightarrow{b_1\wedge b_2,\tau} (\!|t'\{e/x\}\|u', \mathcal{E}|\!)} \qquad Q\text{-}Com_s \quad \frac{(\!|t, \mathcal{E}|\!) \xrightarrow{b_1,c?q} (\!|t', \mathcal{E}|\!), \quad (\!|u, \mathcal{E}|\!) \xrightarrow{b_2,c!q} (\!|u', \mathcal{E}|\!)}{(\!|t\|u, \mathcal{E}|\!) \xrightarrow{b_1\wedge b_2,\tau} (\!|t'\|u', \mathcal{E}|\!)}$$

$$Sum_s \quad \frac{(\!|t, \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta}{(\!|t + u, \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta} \qquad Rel_s \quad \frac{(\!|t, \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta}{(\!|t[f], \mathcal{E}|\!) \xrightarrow{b,f(\gamma)} \Delta[f]}$$

$$Cho_s \quad \frac{(\!|t, \mathcal{E}|\!) \xrightarrow{b',\gamma} \Delta, \quad bv(\gamma) \cap fv(b) = \emptyset}{(\!|\mathbf{if}\ b\ \mathbf{then}\ t, \mathcal{E}|\!) \xrightarrow{b\wedge b',\gamma} \Delta} \qquad Res_s \quad \frac{(\!|t, \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta, \quad cn(\gamma) \cap L = \emptyset}{(\!|t\backslash L, \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta\backslash L}$$

$$Def_s \quad \frac{(\!|t\{\widetilde{e}/\widetilde{x}, \widetilde{r}/\widetilde{q}\}, \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta, \ A(\widetilde{x}, \widetilde{q}) \stackrel{def}{=} t}{(\!|A(\widetilde{e}, \widetilde{r}), \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta}$$

Fig. 3. Symbolic operational semantics of qCCS

5. SYMBOLIC BISIMULATION

5.1. Super-operator weighted transition systems

With the help of super-operator valued distributions defined in the previous section, we now extend the ordinary probabilistic labelled transition systems to super-operator weighted ones.

Definition 5.1. A super-operator weighted labelled transition system, or quantum labelled transition system (qLTS), is a triple $(S, Act, \longrightarrow)$, where

(1) S is a countable set of states,
(2) Act is a countable set of transition actions,
(3) $\longrightarrow$ is a subset of $S \times Act \times \mathcal{D}ist_{\mathcal{H}}(S)$.

For simplicity, we write $s \xrightarrow{\alpha} \Delta$ instead of $(s, \alpha, \Delta) \in \longrightarrow$. A pLTS may be viewed as a degenerate qLTS in which all super-operator valued distributions are probabilistic ones.

5.2. Symbolic transitional semantics of qCCS

To present the symbolic operational semantics of quantum processes, we need some more notations. Let

$$\begin{aligned} Act_s \ = \ & \{\tau\} \cup \{c?x, c!e \mid c \in cChan, x \in cVar, e \in Exp\} \\ & \cup \{\mathsf{c}?r, \mathsf{c}!r \mid \mathsf{c} \in qChan, r \in qVar\} \end{aligned}$$

and $BAct_s = BExp \times Act_s$. For each $\gamma \in Act_s$, the notions $qbv(\gamma)$, $cn(\gamma)$, and $fv(\gamma)$ are similarly defined as for Act_c. We also define $bv(\gamma)$, the set of bound classical variables in γ in an obvious way.

A pair of the form $(\!|t, \mathcal{E}|\!)$, where $t \in \mathcal{T}$ and $\mathcal{E} \in \mathcal{S}_t(\mathcal{H})$, is called a snapshot. The set of snapshots is denoted by SN and sometimes ranged over by $\mathfrak{t}, \mathfrak{u}, \cdots$. Then the symbolic semantics of qCCS is given by the qLTS $(SN, BAct_s, \longrightarrow)$ on snapshots, where

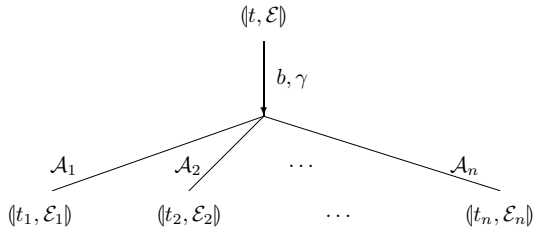
$\longrightarrow \subseteq SN \times BAct_s \times \mathcal{D}ist_{\mathcal{H}}(SN)$ is the smallest relation satisfying the rules defined in Fig. 3. In Rule $Meas_s$, for each $i \in I$, $\mathcal{A}^{\phi_i}_{\widetilde{r}} \in \mathcal{S}(\mathcal{H})$ and $Set^{\phi_i}_{\widetilde{r}} \in \mathcal{S}_t(\mathcal{H})$ are defined respectively as

$$\mathcal{A}^{\phi_i}_{\widetilde{r}} \ : \ \rho \mapsto |\phi_i\rangle_{\widetilde{r}}\langle\phi_i|\rho|\phi_i\rangle_{\widetilde{r}}\langle\phi_i| \tag{2}$$

$$Set^{\phi_i}_{\widetilde{r}} \ : \ \rho \mapsto \sum_{j\in I} |\phi_i\rangle_{\widetilde{r}}\langle\phi_j|\rho|\phi_j\rangle_{\widetilde{r}}\langle\phi_i|. \tag{3}$$

The symmetric forms for rules Par_s, $C\text{-}Com_s$, $Q\text{-}Com_s$, and Sum_s are omitted. Here again, the functions $\|$, $[f]$, and $\backslash L$ have been extended to super-operator valued distributions by denoting, say, $\Delta\|u$ the distribution $\sum_{i\in I}\mathcal{A}_i\bullet(\!|t_i\|u,\mathcal{E}_i|\!)$, if $\Delta = \sum_{i\in I}\mathcal{A}_i\bullet(\!|t_i,\mathcal{E}_i|\!)$.

The transition graph of a snapshot is depicted as usual where each transition $(\!|t,\mathcal{E}|\!) \xrightarrow{b,\gamma} \sum_{i=1}^{n}\mathcal{A}_i \bullet (\!|t_i,\mathcal{E}_i|\!)$ is depicted as



For simplicity, lines marked with $\mathcal{I}_{\mathcal{H}}$ are sometimes omitted.

Example 5.2. (Example 3.3 revisited) In this example, we revisit the two ways of setting a quantum system to pure state $|0\rangle$, presented in Example 3.3. According to the symbolic operational semantics presented in Fig. 3, the qLTSs rooted by $(\!|P,\mathcal{I}_{\mathcal{H}}|\!)$ and $(\!|Q,\mathcal{I}_{\mathcal{H}}|\!)$ respectively can be depicted as in Fig. 4, where $\mathcal{A}_i$ has the single Kraus operator $|i\rangle_q\langle i|$ for $i = 0, 1$.

At the first glance, it is tempting to think that symbolic semantics provides no advantage in describing quantum processes, as the qLTSs in Fig. 4 are almost the same as the pLTSs in Fig. 2 (indeed, the right-hand side qLTS in the former is even more complicated than the corresponding pLTS in the latter). However, pLTSs in Fig. 2 are depicted for a fixed quantum state ρ; to characterise the behaviours of a quantum process, infinitely many such pLTSs must be given, although typically they share the same structure. On the other hand, the qLTSs in Fig. 4 specify *all* possible behaviours of the processes, by means of the super-operators they can perform.

Example 5.3. This example shows the correctness of the super-dense coding protocol. Let $M = \sum_{i=0}^{3} i|\widetilde{i}\rangle\langle\widetilde{i}|$ be a 2-qubit measurement where $\widetilde{i}$ is the binary expansion of i. Let $\mathcal{CN}$ be the controlled-not operation and $\mathcal{H}$ the Hadamard operation. Then the quantum processes that participate in the super-dense coding protocol can be defined as follows:

$$Alice \stackrel{def}{=} \mathsf{c}_A?q_1.\sum_{0\le i\le 3}\left(\mathbf{if}\ x = i\ \mathbf{then}\ \sigma^i[q_1].\mathsf{e}!q_1.\mathbf{nil}\right),$$

$$Bob \stackrel{def}{=} \mathsf{c}_B?q_2.\mathsf{e}?q_1.\mathcal{CN}[q_1,q_2].\mathcal{H}[q_1].M[q_1,q_2;x].d!x.\mathbf{nil},$$

$$EPR \stackrel{def}{=} Set^{\Psi}[q_1,q_2].\mathsf{c}_B!q_2.\mathsf{c}_A!q_1.\mathbf{nil},$$

$$Sdc \stackrel{def}{=} c?x.(EPR\|Alice\|Bob)\backslash\{\mathsf{c}_A,\mathsf{c}_B,\mathsf{e}\}.$$

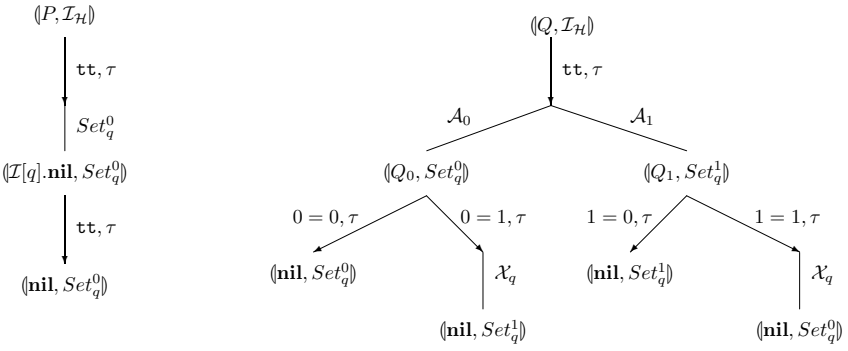


Fig. 4. qLTSs for two ways of setting a quantum system to $|0\rangle$

The specification of super-dense coding protocol can be defined as:

$$Sdc_{spec} \stackrel{def}{=} c?x.\tau^7.Set^x[q_1, q_2].d!x.\mathbf{nil}$$

where

$$Set^x[q_1, q_2].d!x.\mathbf{nil} = \sum_{i=0}^{3}(\mathbf{if}\ x = i\ \mathbf{then}\ Set^i[q_1, q_2].d!x.\mathbf{nil}),$$

and Set^i and Set^Ψ are the 2-qubit super-operators which set the target qubits to $|\widetilde{i}\rangle$ and $|\Psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, respectively. We insert seven τ's in the specification to match the internal actions of Sdc. The qLTSs rooted from $(\!|Sdc_{spec}, \mathcal{I}_{\mathcal{H}}|\!)$ and $(\!|Sdc, \mathcal{I}_{\mathcal{H}}|\!)$ respectively are depicted in Fig. 5 where $\widetilde{q} = \{q_1, q_2\}$, $\mathcal{A}_{\widetilde{i}}$ is the super-operator with the single Kraus operator $|\widetilde{i}\rangle\langle\widetilde{i}|$, $L = \{\mathtt{c}_A, \mathtt{c}_B, \mathtt{e}\}$,

$$Sdc^x \ = \ \left(\left(\sum_{i=0}^{3}(\mathbf{if}\ x = i\ \mathbf{then}\ \sigma^i[q_1].\mathtt{e}!q_1.\mathbf{nil})\right) \| Bob\right) \backslash L.$$

For simplicity, we only draw the transitions along the $x = 0$ branch.

To conclude this subsection, we prove some useful properties of symbolic transitions.

LEMMA 5.4. *If $(\!|t, \mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta$, then there exist super-operators $\{\mathcal{B}_i : i \in I\} \subseteq \mathcal{S}(\mathcal{H})$ and $\{\mathcal{F}_i : i \in I\} \subseteq \mathcal{S}_t(\mathcal{H})$, and process terms $\{t_i : i \in I\} \subseteq \mathcal{T}$ such that*

(1) $\sum_{i\in I} \mathcal{B}_i \eqsim \mathcal{I}_{\mathcal{H}}$,
(2) $\Delta = \sum_{i\in I} \mathcal{B}_i \bullet (\!|t_i, \mathcal{F}_i\mathcal{E}|\!)$,
(3) for any $\mathcal{G} \in \mathcal{S}_t(\mathcal{H})$, $(\!|t, \mathcal{G}|\!) \xrightarrow{b,\gamma} \sum_{i\in I} \mathcal{B}_i \bullet (\!|t_i, \mathcal{F}_i\mathcal{G}|\!)$.

Especially, if $|I| > 1$ then $\mathcal{B}_i$ and $\mathcal{F}_i$ take the forms as $\mathcal{A}_{\widetilde{r}}^{\phi_i}$ and $Set_{\widetilde{r}}^{\phi_i}$ in Eqs.(2) and (3), respectively.

PROOF. Easy from the definition of inference rules. □

The following lemmas show the relationship between transitions in ordinary semantics and in symbolic semantics. Let ψ be an evaluation, $\alpha \in Act_c$, and $\gamma \in Act_s$. We write $\alpha =_\psi \gamma$ if either $\alpha = c!v$, $\gamma = c!e$, and $\psi(e) = v$, or $\gamma = \alpha$ if neither of them is a classical output.

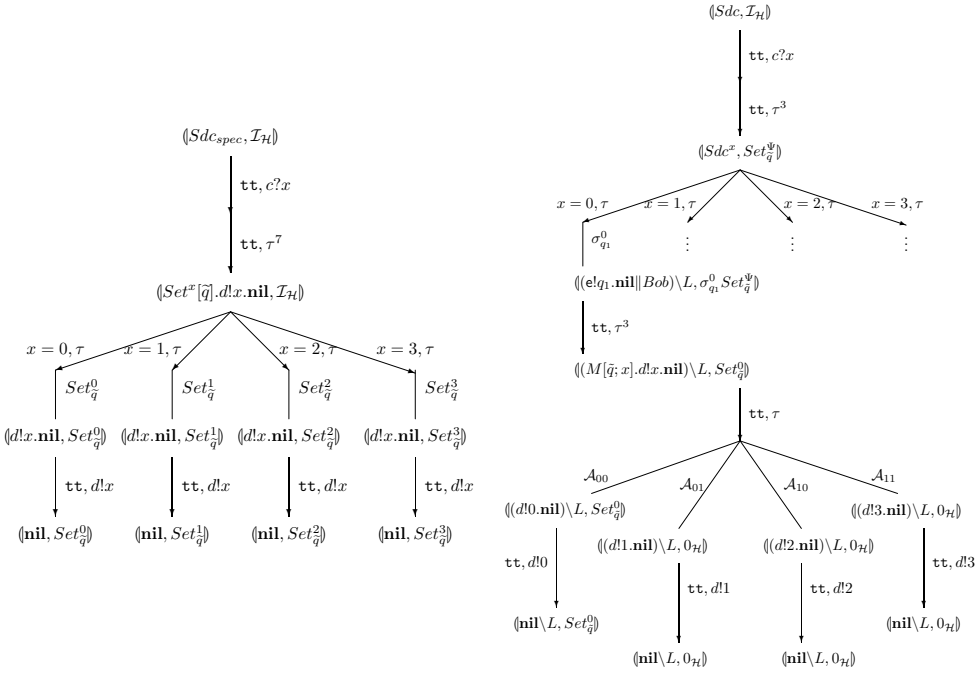


Fig. 5. qLTSs for $(\!|Sdc_{spec}, \mathcal{I}_{\mathcal{H}}|\!)$ and $(\!|Sdc, \mathcal{I}_{\mathcal{H}}|\!)$

LEMMA 5.5. *Suppose* $\langle t\psi, \rho\rangle \overset{\alpha}{\longmapsto} \mu$. *Then there exist* b, I, ψ', $\{\mathcal{A}_i : i \in I\} \subseteq \mathcal{S}(\mathcal{H})$, $\{\mathcal{E}_i : i \in I\} \subseteq \mathcal{S}_t(\mathcal{H})$, *and* $\{t_i : i \in I\} \subseteq \mathcal{T}$, *such that* $\sum_{i\in I} \mathcal{A}_i \eqsim \mathcal{I}_{\mathcal{H}}$, *and*

(1) $\psi(b) = \mathtt{tt}$,
(2) $\mu = \sum_{i\in I} \mathrm{tr}(\mathcal{A}_i(\rho))\langle t_i\psi', \mathcal{E}_i(\rho)\rangle$,
(3) for any $\mathcal{E} \in \mathcal{S}_t(\mathcal{H})$, $(\!|t, \mathcal{E}|\!) \overset{b,\gamma}{\longrightarrow} \sum_{i\in I} \mathcal{A}_i \bullet (\!|t_i, \mathcal{E}_i\mathcal{E}|\!)$, *where*
  (a) if $\alpha = c?v$ *then* $\gamma = c?x$ *for some* $x \notin fv(t)$, *and* $\psi' = \psi\{v/x\}$,
  (b) otherwise, $\gamma =_\psi \alpha$ *and* $\psi' = \psi$.

PROOF. We prove by induction on the depth of the inference by which the action $\langle t\psi, \rho\rangle \overset{\alpha}{\longmapsto} \mu$ is inferred. We argue by cases on the form of t.

(1) $t = c?x.t'$. Then $t\psi = c?x.u$ where u is the process term obtained from t' by instantiating all the free variables in $fv(t') - \{x\}$ according to ψ. By Rule $C\text{-}Inp_c$ we deduce that $\alpha = c?v$ for some $v \in \mathsf{Real}$ and $\mu = \langle P, \rho\rangle$ where $P = u\{v/x\} = t'\psi\{v/x\}$. By Rule Act_s, for any $\mathcal{E} \in \mathcal{S}_t(\mathcal{H})$, we have $(\!|t, \mathcal{E}|\!) \overset{\mathtt{tt}, c?x}{\longrightarrow} (\!|t', \mathcal{E}|\!)$. So we need only to take $b = \mathtt{tt}$, $|I| = 1$, $t_i = t'$, $\mathcal{A}_i = \mathcal{E}_i = \mathcal{I}_{\mathcal{H}}$.
(2) $t = c!e.t'$. Then $t\psi = c!\psi(e).(t'\psi)$, and by Rule $C\text{-}Out_c$ we deduce that $\alpha = c!\psi(e)$ and $\mu = \langle t'\psi, \rho\rangle$. By Rule Act_s, for any $\mathcal{E} \in \mathcal{S}_t(\mathcal{H})$, we have $(\!|t, \mathcal{E}|\!) \overset{\mathtt{tt}, c!e}{\longrightarrow} (\!|t', \mathcal{E}|\!)$. So we need only to take $b = \mathtt{tt}$, $|I| = 1$, $t_i = t'$, $\mathcal{A}_i = \mathcal{E}_i = \mathcal{I}_{\mathcal{H}}$ as well.
(3) $t = \mathtt{c}?q.t'$. Then $t\psi = \mathtt{c}?q.(t'\psi)$, and by Rule $Q\text{-}Inp_c$ we deduce that $\alpha = \mathtt{c}?r$ for some $r \notin qv(t)$ and $\mu = \langle (t'\psi)\{r/q\}, \rho\rangle$. By Rule Act_s and α-conversion, for any $\mathcal{E} \in \mathcal{S}_t(\mathcal{H})$,

we have $(\!|t,\mathcal{E}|\!) \xrightarrow{\mathtt{tt},c?r} (\!|t'\{r/q\},\mathcal{E}|\!)$. So we need only to take $b=\mathtt{tt}$, $|I|=1$, $t_i=t'\{r/q\}$, $\mathcal{A}_i=\mathcal{E}_i=\mathcal{I}_{\mathcal{H}}$.

(4) $t = M[\widetilde{q};x].t'$. Then $t\psi = M[\widetilde{q};x].u$ where u is the process term obtained from t' by instantiating all the free variables in $fv(t')-\{x\}$ according to ψ. Let $M=\sum_{i\in I}\lambda_i|\phi_i\rangle\langle\phi_i|$. By Rule $Meas_c$ we deduce that $\alpha=\tau$ and $\mu=\sum_{i\in I}\mathrm{tr}(\mathcal{A}_i(\rho))\langle P_i,\mathcal{E}_i(\rho)\rangle$ where $P_i=u\{\lambda_i/x\}=t'\{\lambda_i/x\}\psi$, $\mathcal{A}_i=\{|\phi_i\rangle\langle\phi_i|\}$, and $\mathcal{E}_i=\{|\phi_i\rangle\langle\phi_j| : j\in I\}$. Take $b=\mathtt{tt}$. By Rule $Meas_s$, for any $\mathcal{E}\in\mathcal{S}_t(\mathcal{H})$, we have $(\!|t,\mathcal{E}|\!) \xrightarrow{b,\tau} \sum_{i\in I}\mathcal{A}_i\bullet(\!|t'\{\lambda_i/x\},\mathcal{E}_i\mathcal{E}|\!)$.

(5) $t=t_1\|t_2$. Then $t\psi=t_1\psi\|t_2\psi$. There are two sub-cases to consider:

(a) The action is caused solely by one of the components, say $\langle t_1\psi,\rho\rangle \xmapsto{\alpha} \mu_1$. Then we have $qbv(\alpha)\cap qv(t_2\psi)=\emptyset$, and $\mu=\mu_1\|t_2\psi$. By induction, there exist $b,I,t_i,\mathcal{A}_i,\mathcal{E}_i,i\in I$, such that $\psi(b)=\mathtt{tt}$, $\mu_1=\sum_{i\in I}\mathrm{tr}(\mathcal{A}_i(\rho))\langle t_i\psi',\mathcal{E}_i(\rho)\rangle$, and for any $\mathcal{E}\in\mathcal{S}_t(\mathcal{H})$, $(\!|t_1,\mathcal{E}|\!) \xrightarrow{b,\gamma} \sum_{i\in I}\mathcal{A}_i\bullet(\!|t_i,\mathcal{E}_i\mathcal{E}|\!)$. Note that by α-conversion, when $\gamma=c?x$, we can always take x such that $x\notin fv(t_2)$, and consequently, $(t_i\|t_2)\psi'=t_i\psi'\|t_2\psi$. Finally, we have $(\!|t,\mathcal{E}|\!) \xrightarrow{b,\gamma} \sum_{i\in I}\mathcal{A}_i\bullet(\!|t_i\|t_2,\mathcal{E}_i\mathcal{E}|\!)$, using Rule Par_s.

(b) The action is caused by a (classical or quantum) communication. Here we only detail the case when $\langle t_1\psi,\rho\rangle \xmapsto{c?v} \langle P_1,\rho\rangle$, $\langle t_2\psi,\rho\rangle \xmapsto{c!v} \langle P_2,\rho\rangle$, $\alpha=\tau$, and $\mu=\langle P_1\|P_2,\rho\rangle$. Then by induction, there exist b_1, b_2, t_1', t_2' such that $\psi(b_1\wedge b_2)=\mathtt{tt}$, $P_1=t_1'\psi'$, $P_2=t_2'\psi$, and for any $\mathcal{E}\in\mathcal{S}_t(\mathcal{H})$, $(\!|t_1,\mathcal{E}|\!) \xrightarrow{b_1,c?x} (\!|t_1',\mathcal{E}|\!)$ and $(\!|t_2,\mathcal{E}|\!) \xrightarrow{b_2,c!e} (\!|t_2',\mathcal{E}|\!)$, where $x\notin fv(t_1)$, $\psi'=\psi\{v/x\}$, and $\psi(e)=v$. Thus

$$(t_1'\{e/x\}\|t_2')\psi=t_1'\{e/x\}\psi\|t_2'\psi=t_1'\psi\{v/x\}\|t_2'\psi=t_1'\psi'\|t_2'\psi=P_1\|P_2.$$

Finally, we have $(\!|t,\mathcal{E}|\!) \xrightarrow{b_1\wedge b_2,\tau} (\!|t_1'\{e/x\}\|t_2',\mathcal{E}|\!)$, using Rule $Q\text{-}Com_s$.

(6) Other cases. Similar to the cases we discussed above.

□

LEMMA 5.6. *Suppose* $(\!|t,\mathcal{E}|\!) \xrightarrow{b,\gamma} \Delta$. *Then there exist* I, $\{\mathcal{A}_i : i\in I\}\subseteq\mathcal{S}(\mathcal{H})$, $\{\mathcal{E}_i : i\in I\}\subseteq\mathcal{S}_t(\mathcal{H})$, *and* $\{t_i : i\in I\}\subseteq\mathcal{T}$, *such that* $\sum_{i\in I}\mathcal{A}_i\eqsim\mathcal{I}_{\mathcal{H}}$, *and*

(1) $\Delta=\sum_{i\in I}\mathcal{A}_i\bullet(\!|t_i,\mathcal{E}_i\mathcal{E}|\!)$,

(2) for any ψ *and* ρ, $\psi(b)=\mathtt{tt}$ *implies* $\langle t\psi,\rho\rangle \xmapsto{\alpha} \sum_{i\in I}\mathrm{tr}(\mathcal{A}_i(\rho))\langle t_i\psi',\mathcal{E}_i(\rho)\rangle$ *where*
  (a) if $\gamma=c?x$ *then* $\alpha=c?v$ *for some* $v\in\mathsf{Real}$, *and* $\psi'=\psi\{v/x\}$,
  (b) otherwise, $\gamma=_\psi\alpha$ *and* $\psi'=\psi$.

PROOF. Similar to Lemma 5.5. □

5.3. Symbolic bisimulation

Let $\mathcal{S}\subseteq SN\times SN$ be an equivalence relation. We lift $\mathcal{S}$ to $\mathcal{D}ist_{\mathcal{H}}(SN)\times\mathcal{D}ist_{\mathcal{H}}(SN)$ by defining $\Delta\mathcal{S}\Xi$ if for any equivalence class $T\in SN/\mathcal{S}$, $\Delta(T)\eqsim\Xi(T)$; that is, $\sum_{\mathfrak{t}\in T}\Delta(\mathfrak{t})\eqsim\sum_{\mathfrak{t}\in T}\Xi(\mathfrak{t})$. We write $\gamma=_b\gamma'$ if either $\gamma=c!e$, $\gamma'=c!e'$, and $b\to e=e'$, or $\gamma=\gamma'$ if neither of them is a classical output. The following definition is motivated by [Hennessy and Lin 1995].

Definition 5.7. Let $\mathfrak{S}=\{\mathcal{S}^b : b\in BExp\}$ be a family of equivalence relations on SN. $\mathfrak{S}$ is called a symbolic (strong open) bisimulation if for any $b\in BExp$, $(\!|t,\mathcal{E}|\!)\mathcal{S}^b(\!|u,\mathcal{F}|\!)$ implies that

(1) $qv(t)=qv(u)$ and $\mathcal{E}\eqsim_{\overline{qv(t)}}\mathcal{F}$, if b is satisfiable;

(2) for any $\mathcal{G} \in \mathcal{S}_t(\mathcal{H}_{\overline{qv(t)}})$, whenever $(\!|t, \mathcal{G}\mathcal{E}|\!) \xrightarrow{b_1,\gamma} \Delta$ with $bv(\gamma) \cap fv(b,t,u) = \emptyset$, there exists a collection of booleans B such that $b \wedge b_1 \rightarrow \bigvee B$ and $\forall\, b' \in B$, $\exists b_2, \gamma'$ with $b' \rightarrow b_2$, $\gamma =_{b'} \gamma'$, $(\!|u, \mathcal{G}\mathcal{F}|\!) \xrightarrow{b_2,\gamma'} \Xi$, and $(\mathcal{G}\mathcal{E} \bullet \Delta)\mathcal{S}^{b'}(\mathcal{G}\mathcal{F} \bullet \Xi)$.

One may wonder if it suffices to only require $\Delta\mathcal{S}^{b'}\Xi$ at the end of Clause (2), and deduce from it $(\mathcal{G}\mathcal{E} \bullet \Delta)\mathcal{S}^{b'}(\mathcal{G}\mathcal{F} \bullet \Xi)$ if necessary. This is not true. Although $\mathcal{G}\mathcal{E}$ and $\mathcal{G}\mathcal{F}$ are both trace-preserving super-operators, $\Delta\mathcal{S}^{b'}\Xi$ does not necessarily imply $(\mathcal{G}\mathcal{E} \bullet \Delta)\mathcal{S}^{b'}(\mathcal{G}\mathcal{F} \bullet \Xi)$. For example, let $\Delta = \mathcal{A} \bullet \mathfrak{t}$ and $\Xi = \mathcal{A} \bullet \mathfrak{u}$ with $\mathfrak{t}\mathcal{S}^{b'}\mathfrak{u}$. Then $\Delta\mathcal{S}^{b'}\Xi$. On the other hand, we have $\mathcal{G}\mathcal{E} \bullet \Delta = \mathcal{A}\mathcal{G}\mathcal{E} \bullet \mathfrak{t}$ and $\mathcal{G}\mathcal{F} \bullet \Xi = \mathcal{A}\mathcal{G}\mathcal{F} \bullet \mathfrak{u}$. They are not necessarily related by $\mathcal{S}^{b'}$, as in general, we have $\mathcal{A}\mathcal{G}\mathcal{E} \not\equiv \mathcal{A}\mathcal{G}\mathcal{F}$; please see the remark after Lemma 4.2 for details. Furthermore, this requirement is essential in proving the results, say, Lemma 5.21, in later sections.

Two configurations $(\!|t, \mathcal{E}|\!)$ and $(\!|u, \mathcal{F}|\!)$ are symbolically b-bisimilar, denoted by $(\!|t, \mathcal{E}|\!) \sim^b (\!|u, \mathcal{F}|\!)$, if there exists a symbolic bisimulation $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ such that $(\!|t, \mathcal{E}|\!)\mathcal{S}^b(\!|u, \mathcal{F}|\!)$. Two quantum process terms t and u are symbolically b-bisimilar, denoted by $t \sim^b u$, if $(\!|t, \mathcal{I}_{\mathcal{H}}|\!) \sim^b (\!|u, \mathcal{I}_{\mathcal{H}}|\!)$. When $b = \mathtt{tt}$, we simply write $t \sim u$.

Similar to [Deng and Feng 2012], we can separate the super-operator application and transitions in the definition of symbolic bisimulation. This will be very useful when proving bisimilarity.

Definition 5.8. A family of equivalence relations $\{\mathcal{S}^b : b \in BExp\}$ is called a symbolic *ground* bisimulation if for any $b \in BExp$, $(\!|t, \mathcal{E}|\!)\mathcal{S}^b(\!|u, \mathcal{F}|\!)$ implies that

(1) $qv(t) = qv(u)$ and $\mathcal{E} \eqsim_{\overline{qv(t)}} \mathcal{F}$, if b is satisfiable,

(2) whenever $(\!|t, \mathcal{E}|\!) \xrightarrow{b_1,\gamma} \Delta$ with $bv(\gamma) \cap fv(b,t,u) = \emptyset$, there exists a collection of booleans B such that $b \wedge b_1 \rightarrow \bigvee B$ and $\forall\, b' \in B$, $\exists b_2, \gamma'$ with $b' \rightarrow b_2$, $\gamma =_{b'} \gamma'$, $(\!|u, \mathcal{F}|\!) \xrightarrow{b_2,\gamma'} \Xi$, and $(\mathcal{E} \bullet \Delta)\mathcal{S}^{b'}(\mathcal{F} \bullet \Xi)$.

Given two configurations $(\!|t, \mathcal{E}|\!)$ and $(\!|u, \mathcal{F}|\!)$, we write $(\!|t, \mathcal{E}|\!) \sim_g^b (\!|u, \mathcal{F}|\!)$ if there is a symbolic ground bisimulation $\{\mathcal{S}^b : b \in BExp\}$ with $(\!|t, \mathcal{E}|\!)\mathcal{S}^b(\!|u, \mathcal{F}|\!)$.

Definition 5.9. A relation $\mathcal{S}$ on SN is said to be closed under super-operator application if $(\!|t, \mathcal{E}|\!)\mathcal{S}(\!|u, \mathcal{F}|\!)$ implies $(\!|t, \mathcal{G}\mathcal{E}|\!)\mathcal{S}(\!|u, \mathcal{G}\mathcal{F}|\!)$ for any $\mathcal{G} \in \mathcal{S}_t(\mathcal{H}_{\overline{qv(t)}})$. A family of relations is closed under super-operator application if each individual relation is.

PROPOSITION 5.10. *A family of equivalence relations $\{\mathcal{S}^b : b \in BExp\}$ is a symbolic bisimulation if and only if it is both a ground bisimulation and closed under super-operator application.*

PROOF. Similar to the corresponding result in [Deng and Feng 2012]. □

The above proposition provides an incremental way to proving bisimilarity, which is analogous to a proof technique of open bisimulation for the π-calculus [Sangiorgi 1996], where name instantiation is playing the same role as super-operator application here.

A process term is said to be *free of quantum input* if all of its descendants, including itself, can not perform quantum input actions.

LEMMA 5.11. *Let $(\!|t, \mathcal{E}|\!) \sim_g^b (\!|u, \mathcal{F}|\!)$, and t and u be free of quantum input. Then for any $\mathcal{G} \in \mathcal{S}_t(\mathcal{H}_{\overline{qv(t)}})$, $(\!|t, \mathcal{G}\mathcal{E}|\!) \sim_g^b (\!|u, \mathcal{G}\mathcal{F}|\!)$.*

PROOF. We need to show $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$, where

$$\begin{aligned}\mathcal{S}^b \;=\; &\{((\!|t, \mathcal{G}\mathcal{E}|\!), (\!|u, \mathcal{G}\mathcal{F}|\!)) : t \text{ and } u \text{ free of quantum input, } \mathcal{G} \in \mathcal{S}_t(\mathcal{H}_{\overline{qv(t)}}),\\ &\text{and } (\!|t, \mathcal{E}|\!) \sim_g^b (\!|u, \mathcal{F}|\!)\},\end{aligned}$$

is a symbolic ground bisimulation. This is easy by noting that for any descendant t' of t, $qv(t') \subseteq qv(t)$, and then $\mathcal{G} \in \mathcal{S}_t(\mathcal{H}_{\overline{qv(t')}})$ as well. Consequently, $\mathcal{G}$ commutes with all the super-operators performed by t and its descendants. □

THEOREM 5.12. *If t and u are both free of quantum input, then $(\!|t, \mathcal{E}|\!) \sim^b (\!|u, \mathcal{F}|\!)$ if and only if $(\!|t, \mathcal{E}|\!) \sim_g^b (\!|u, \mathcal{F}|\!)$.*

PROOF. Easy from Lemma 5.11 and proposition 5.10. □

To show the usage of symbolic bisimulation and the proof technique above, we revisit the examples presented in Section 5.2 to show that the proposed protocols indeed achieve the desired goals. Let $\widetilde{A} = \{A_i : i \in I\}$ be a set of disjoint subsets of snapshots. An equivalence relation $\mathcal{S}$ is said to be generated by $\widetilde{A}$ if its equivalence classes on the set of snapshots $\cup_{i\in I} A_i$ are given by the partition $\widetilde{A}$, and it is the identity relation on $SN - \cup_{i\in I} A_i$.

Example 5.13. (Example 5.2 revisited) This example is devoted to showing rigorously that the two ways of setting a quantum system to the pure state $|0\rangle$, presented in Examples 3.3 and 5.2, are indeed symbolic bisimilar. Let

$$\begin{aligned}A \;&=\; \{(\!|P, \mathcal{I}_{\mathcal{H}}|\!), (\!|Q, \mathcal{I}_{\mathcal{H}}|\!)\},\\ B \;&=\; \{(\!|\mathcal{I}[q].\mathbf{nil}, Set_q^0|\!), (\!|Q_0, Set_q^0|\!), (\!|Q_1, Set_q^1|\!)\}\end{aligned}$$

and $\mathcal{S}'$ be the equivalence relation generated by $\{A, B\}$. It is easy to check that the family $\{\mathcal{S}^b : b \in BExp\}$, where $\mathcal{S}^b = \mathcal{S}'$ for any $b \in BExp$, is a symbolic ground bisimulation. Thus $P \sim_g Q$. Furthermore, as both P and Q are free of quantum input, we have $P \sim Q$.

Example 5.14. (Superdense coding revisited) This example is devoted to proving rigorously that the protocol presented in Example 5.3 indeed sends two bits of classical information from Alice to Bob by transmitting a qubit. For that purpose, we need to show that $(\!|Sdc_{spec}, \mathcal{I}_{\mathcal{H}}|\!) \sim (\!|Sdc, \mathcal{I}_{\mathcal{H}}|\!)$. Indeed, let

$$\begin{aligned}A \;&=\; \{(\!|Sdc_{spec}, \mathcal{I}_{\mathcal{H}}|\!), (\!|Sdc, \mathcal{I}_{\mathcal{H}}|\!)\},\\ B^j \;&=\; \{(\!|t, \mathcal{E}|\!) : d((\!|t, \mathcal{E}|\!)) = j\},\\ C_i^k \;&=\; \{(\!|t, \mathcal{E}|\!) : (\!|t, \mathcal{E}|\!) \text{ along the branch of } x = i, \text{ and } d((\!|t, \mathcal{E}|\!)) = k\},\end{aligned}$$

where $d((\!|t, \mathcal{E}|\!))$ is the depth of the node $(\!|t, \mathcal{E}|\!)$ from the root of its corresponding qLTS, $0 < j \leq 4$, $0 \leq i \leq 3$, and $5 \leq k \leq 10$. Let $\mathcal{S}_1^{\mathtt{tt}}$ be the equivalence relation generated by $\{A, B^1, B^2, B^3, B^4\}$, and $\mathcal{S}_1^{x=i}$ generated by $\{C_i^k : 5 \leq k \leq 10\}$. For any $b \in BExp$, let $\mathcal{S}^b$ be $\mathcal{S}_1^{x=i}$ if $b \to x = i$, $\mathcal{S}_1^{\mathtt{tt}}$ if $b \to \mathtt{tt}$, and the identity relation otherwise. Then it is easy to check that $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ is a symbolic ground bisimulation. Again, as Sdc_{spec} and Sdc are both free of quantum input, we have $(\!|Sdc_{spec}, \mathcal{I}_{\mathcal{H}}|\!) \sim (\!|Sdc, \mathcal{I}_{\mathcal{H}}|\!)$.

5.4. Symbolic bisimilarity as a symbolic bisimulation

In the following, we show that symbolic bisimilarity is indeed a symbolic bisimulation. We denote by $\mathcal{S}^*$ the equivalence closure of a relation $\mathcal{S}$.

Definition 5.15. A relation family $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ is called decreasing, if for any $b, b' \in BExp$ with $b \to b'$, we have $\mathcal{S}^{b'} \subseteq \mathcal{S}^b$.

LEMMA 5.16. *Let $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ be a symbolic bisimulation. Then there exists a decreasing symbolic bisimulation $\mathfrak{U} = \{\mathcal{U}^b : b \in BExp\}$ such that for each $b \in BExp$, $\mathcal{S}^b \subseteq \mathcal{U}^b$.*

PROOF. Suppose $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ is a symbolic bisimulation. For each $b \in BExp$, let

$$\mathcal{U}_1^b = \bigcup \{\mathcal{S}^{b'} : b \to b'\} \text{ and } \mathcal{U}^b = (\mathcal{U}_1^b)^*.$$

Obviously, $\mathfrak{U} = \{\mathcal{U}^b : b \in BExp\}$ is decreasing. We have to show that $\mathfrak{U}$ is a symbolic bisimulation.

Let $b \in BExp$ and $(\!|t, \mathcal{E}|\!)\mathcal{U}^b(\!|u, \mathcal{F}|\!)$. Note that $\mathcal{U}_1^b$ is both reflexive and symmetric. So $\mathcal{U}^b$ is actually the transitive closure of $\mathcal{U}_1^b$, and there exist $n \geq 1$ and a sequence of snapshots $(\!|t_i, \mathcal{E}_i|\!)$, $0 \leq i \leq n$, such that $(\!|t, \mathcal{E}|\!) = (\!|t_0, \mathcal{E}_0|\!)$, $(\!|u, \mathcal{F}|\!) = (\!|t_n, \mathcal{E}_n|\!)$, and for each $0 \leq i \leq n-1$, $(\!|t_i, \mathcal{E}_i|\!)\mathcal{U}_1^b(\!|t_{i+1}, \mathcal{E}_{i+1}|\!)$. For the sake of simplicity, we assume $n = 2$. That is, there exists $(\!|s, \mathcal{G}|\!)$ such that $(\!|t, \mathcal{E}|\!)\mathcal{S}^{b_1}(\!|s, \mathcal{G}|\!)\mathcal{S}^{b_2}(\!|u, \mathcal{F}|\!)$ with $b \to b_1 \wedge b_2$. The general case is more tedious but similar.

First we check that if b is satisfiable, then $qv(t) = qv(s) = qv(u)$ and $\mathcal{E} \approx_{\overline{qv(t)}} \mathcal{G} \approx_{\overline{qv(t)}} \mathcal{F}$. Suppose $(\!|t, \mathcal{E}|\!) \xrightarrow{b_1', \gamma} \Delta$ with $bv(\gamma) \cap fv(b_1, t, u) = \emptyset$. By α-conversion, we may assume further that $bv(\gamma) \cap fv(s) = \emptyset$. From $(\!|t, \mathcal{E}|\!)\mathcal{S}^{b_1}(\!|s, \mathcal{G}|\!)$, there exists a collection of booleans $\{c_i : 1 \leq i \leq n\}$ such that $b_1 \wedge b_1' \to \bigvee c_i$ and for any i, $\exists c_i', \gamma_i$ with $c_i \to c_i'$, $\gamma =_{c_i} \gamma_i$, $(\!|s, \mathcal{G}|\!) \xrightarrow{c_i', \gamma_i} \Theta$, and $(\mathcal{E} \bullet \Delta)\mathcal{S}^{c_i}(\mathcal{G} \bullet \Theta)$. By α-conversion, we can again assume that for each i, $bv(\gamma_i) \cap fv(b_2, s, u) = \emptyset$. Now by the assumption that $(\!|s, \mathcal{G}|\!)\mathcal{S}^{b_2}(\!|u, \mathcal{F}|\!)$, there exists a collection of booleans $\{d_{ij} : 1 \leq j \leq n_i\}$ such that $b_2 \wedge c_i' \to \bigvee_j d_{ij}$ and for any d_{ij}, $\exists d_{ij}', \gamma_{ij}$ with $d_{ij} \to d_{ij}'$, $\gamma_{ij} =_{d_{ij}} \gamma_i$, $(\!|u, \mathcal{F}|\!) \xrightarrow{d_{ij}', \gamma_{ij}} \Xi$, and $(\mathcal{G} \bullet \Theta)\mathcal{S}^{d_{ij}}(\mathcal{F} \bullet \Xi)$.

Now let

$$B = \{b \wedge c_i \wedge d_{ij} : 1 \leq i \leq n, 1 \leq j \leq n_i\}.$$

From the fact that $b \to b_1 \wedge b_2$, it is easy to check that $b \wedge b_1' \to \bigvee B$. For any $c = b \wedge c_i \wedge d_{ij}$, we take $c' = d_{ij}'$ and $\gamma' = \gamma_{ij}$. Then $c \to c'$, $\gamma' =_c \gamma$, and $(\!|u, \mathcal{F}|\!) \xrightarrow{c', \gamma'} \Xi$ as required. Furthermore, by the fact that $c \to c_i$ and the definition of $\mathcal{U}^c$, we have $(\mathcal{E} \bullet \Delta)\mathcal{U}^c(\mathcal{G} \bullet \Theta)$ indeed. Similarly, $(\mathcal{G} \bullet \Theta)\mathcal{U}^c(\mathcal{F} \bullet \Xi)$. Thus $(\mathcal{E} \bullet \Delta)\mathcal{U}^c(\mathcal{F} \bullet \Xi)$ as required.

Furthermore, it is easy to check that for any $b \in BExp$, $\mathcal{U}^b$ is closed under super-operator application as each $\mathcal{S}^b$ is. Thus we have $\mathfrak{U}$ is a symbolic bisimulation. □

LEMMA 5.17. *Let decreasing families $\mathfrak{S}_i = \{\mathcal{S}_i^b : b \in BExp\}$, $i = 1, 2$, be symbolic bisimulations. Then the family $\mathfrak{S} = \{(\mathcal{S}_1^b \mathcal{S}_2^b)^* : b \in BExp\}$ is also a symbolic bisimulation.*

PROOF. Let $b \in BExp$ and $(\!|t, \mathcal{E}|\!)(\mathcal{S}_1^b \mathcal{S}_2^b)^*(\!|u, \mathcal{F}|\!)$. Suppose there exist $n \geq 1$ and a sequence of snapshots $(\!|t_i, \mathcal{E}_i|\!)$, $0 \leq i \leq n$, such that $(\!|t, \mathcal{E}|\!) = (\!|t_0, \mathcal{E}_0|\!)$, $(\!|u, \mathcal{F}|\!) = (\!|t_n, \mathcal{E}_n|\!)$, and for each $0 \leq i \leq n-1$, $(\!|t_i, \mathcal{E}_i|\!)\mathcal{S}_1^b\mathcal{S}_2^b(\!|t_{i+1}, \mathcal{E}_{i+1}|\!)$. Again, for the sake of simplicity, we assume $n = 1$. That is, there exists $(\!|s, \mathcal{G}|\!)$ such that $(\!|t, \mathcal{E}|\!)\mathcal{S}_1^b(\!|s, \mathcal{G}|\!)\mathcal{S}_2^b(\!|u, \mathcal{F}|\!)$. The rest of the poof follows almost the same lines of those in Lemma 5.16, by employing the assumption that $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are both decreasing. □

With the lemmas above, we can show that the family $\{\sim^b : b \in BExp\}$ is actually the largest symbolic bisimulation.

THEOREM 5.18.

(1) For each $b \in BExp$, $\sim^b$ is an equivalence relation.
(2) The family $\{\sim^b : b \in BExp\}$ is a symbolic bisimulation.

PROOF. (2) is direct from (1) and the definition of symbolic bisimulation. To prove (1), let $b \in BExp$. Obviously, $\sim^b$ is reflexive and symmetric. To show the transitivity of $\sim^b$, let $(\!|t, \mathcal{E}|\!) \sim^b (\!|u, \mathcal{F}|\!)$ and $(\!|u, \mathcal{F}|\!) \sim^b (\!|s, \mathcal{G}|\!)$. Then by definition, there exist symbolic bisimulations $\mathfrak{S}_i = \{\mathcal{S}_i^b : b \in BExp\}$, $i = 1, 2$, such that $(\!|t, \mathcal{E}|\!)\mathcal{S}_1^b(\!|u, \mathcal{F}|\!)$ and $(\!|u, \mathcal{F}|\!)\mathcal{S}_2^b(\!|s, \mathcal{G}|\!)$. By Lemma 5.16, we can assume without loss of generality that both $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are decreasing, thus $\mathfrak{S} = \{(\mathcal{S}_1^b\mathcal{S}_2^b)^* : b \in BExp\}$ is also a symbolic bisimulation, by Lemma 5.17. So $(\!|t, \mathcal{E}|\!) \sim^b (\!|s, \mathcal{G}|\!)$. □

To conclude this subsection, we present a property of symbolic bisimilarity which is useful for the next section.

THEOREM 5.19. *Let $(\!|t, \mathcal{E}|\!), (\!|u, \mathcal{F}|\!) \in SN$ and $b \in BExp$. Then $(\!|t, \mathcal{E}|\!) \sim^b (\!|u, \mathcal{F}|\!)$ if and only if*

(1) $qv(t) = qv(u)$ and $\mathcal{E} \eqsim_{\overline{qv(t)}} \mathcal{F}$, if b is satisfiable;
(2) for any $\mathcal{G} \in \mathcal{S}_t(\mathcal{H}_{\overline{qv(t)}})$, whenever $(\!|t, \mathcal{G}\mathcal{E}|\!) \xrightarrow{b_1,\gamma} \Delta$ with $bv(\gamma) \cap fv(b, t, u) = \emptyset$, then there exist a collection of booleans B such that $b \wedge b_1 \to \bigvee B$ and $\forall\, b' \in B$, $\exists b_2, \gamma'$ with $b' \to b_2$, $\gamma =_{b'} \gamma'$, $(\!|u, \mathcal{G}\mathcal{F}|\!) \xrightarrow{b_2,\gamma'} \Xi$, and $(\mathcal{G}\mathcal{E} \bullet \Delta) \sim^{b'} (\mathcal{G}\mathcal{F} \bullet \Xi)$;
(3) Symmetric condition of (2).

PROOF. Routine. □

5.5. Connection of symbolic and open bisimulations

Let $\Delta = \sum_{i\in I} \mathcal{A}_i \bullet (\!|t_i, \mathcal{E}_i|\!)$ be a distribution, ψ an evaluation, and $\rho \in \mathcal{D}(\mathcal{H})$. We write

$$(\Delta\psi)(\rho) = \sum_{i\in I} \mathrm{tr}(\mathcal{A}_i(\rho))\langle t_i\psi, \mathcal{E}_i(\rho)\rangle.$$

In particular, if $\mathfrak{t} = (\!|t, \mathcal{E}|\!)$ then $(\mathfrak{t}\psi)(\rho) = \langle t\psi, \mathcal{E}(\rho)\rangle$. The basic ideas of the proofs in this subsection are borrowed from [Hennessy and Lin 1995], with the help of Lemmas 5.5 and 5.6.

Let $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ be a symbolic bisimulation. Define

$$\mathcal{R}_{\mathfrak{S}} = \{((\mathfrak{t}\psi)(\rho), (\mathfrak{u}\psi)(\rho)) : \rho \in \mathcal{D}(\mathcal{H}) \text{ and } \exists b, \psi(b) = \mathtt{tt} \text{ and } \mathfrak{t}\mathcal{S}^b\mathfrak{u}\}.$$

We prove that $\mathcal{R}_{\mathfrak{S}}$ is an open bisimulation. To achieve this, the following lemma is needed.

LEMMA 5.20. *Let $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ be a symbolic bisimulation, $\rho \in \mathcal{D}(\mathcal{H})$, and $\psi(b) = \mathtt{tt}$. Then*

$$\Delta\, \mathcal{S}^b\, \Xi \textit{ implies } (\Delta\psi)(\rho)\, \mathcal{R}_{\mathfrak{S}}\, (\Xi\psi)(\rho).$$

PROOF. Suppose $\Delta = \sum_{i\in I} \mathcal{A}_i \bullet (\!|t_i, \mathcal{E}_i|\!)$, $\Xi = \sum_{j\in J} \mathcal{B}_j \bullet (\!|u_j, \mathcal{F}_j|\!)$ and $\Delta\, \mathcal{S}^b\, \Xi$. We decompose the set $\lceil\Delta\rceil \cup \lceil\Xi\rceil$ into disjoint subsets $S_1, \cdots, S_n$ such that any two snapshots are in the same S_k if and only if they are related by $\mathcal{S}^b$. For each $1 \le k \le n$, let

$$K_k = \{i \in I : (\!|t_i, \mathcal{E}_i|\!) \in S_k\} \cup \{j \in J : (\!|u_j, \mathcal{F}_j|\!) \in S_k\}.$$

Then

$$\sum_{i\in K_k\cap I} \mathcal{A}_i \eqsim \sum_{j\in K_k\cap J} \mathcal{B}_j. \tag{4}$$

For any $\rho \in \mathcal{D}(\mathcal{H})$ and ψ with $\psi(b) = \mathtt{tt}$,

$$(\Delta\psi)(\rho) = \sum_{i\in I} \mathrm{tr}(\mathcal{A}_i(\rho))\langle t_i\psi, \mathcal{E}_i(\rho)\rangle = \sum_{k=1}^{n} \sum_{i\in K_k\cap I} \mathrm{tr}(\mathcal{A}_i(\rho))\langle t_i\psi, \mathcal{E}_i(\rho)\rangle$$
$$= \sum_{k=1}^{n} \frac{1}{\sum_{j\in K_k\cap J}\mathrm{tr}(\mathcal{B}_j(\rho))} \sum_{i\in K_k\cap I}\sum_{j\in K_k\cap J} \mathrm{tr}(\mathcal{A}_i(\rho))\mathrm{tr}(\mathcal{B}_j(\rho))\langle t_i\psi, \mathcal{E}_i(\rho)\rangle.$$

Similarly, we have

$$(\Xi\psi)(\rho) = \sum_{j\in J} \mathrm{tr}(\mathcal{B}_j(\rho))\langle u_j\psi, \mathcal{F}_j(\rho)\rangle = \sum_{k=1}^{n} \sum_{j\in K_k\cap J} \mathrm{tr}(\mathcal{B}_j(\rho))\langle u_j\psi, \mathcal{F}_j(\rho)\rangle$$
$$= \sum_{k=1}^{n} \frac{1}{\sum_{i\in K_k\cap I}\mathrm{tr}(\mathcal{A}_i(\rho))} \sum_{i\in K_k\cap I}\sum_{j\in K_k\cap J} \mathrm{tr}(\mathcal{A}_i(\rho))\mathrm{tr}(\mathcal{B}_j(\rho))\langle u_j\psi, \mathcal{F}_j(\rho)\rangle.$$

Note that by definition, if $\mathfrak{t}\mathcal{S}^b\mathfrak{u}$ then $(\mathfrak{t}\psi)(\rho)\mathcal{R}_{\mathfrak{S}}(\mathfrak{u}\psi)(\rho)$. It follows that for an arbitrarily given k, we have $\langle t_i\psi, \mathcal{E}_i(\rho)\rangle\mathcal{R}_{\mathfrak{S}}\langle u_j\psi, \mathcal{F}_j(\rho)\rangle$ for any $i \in K_k \cap I$ and $j \in K_k \cap J$. Furthermore, by Eq.(4), we know $\sum_{i\in K_k\cap I}\mathrm{tr}(\mathcal{A}_i(\rho)) = \sum_{j\in K_k\cap J}\mathrm{tr}(\mathcal{B}_j(\rho))$. Thus $(\Delta\psi)(\rho)\,\mathcal{R}_{\mathfrak{S}}\,(\Xi\psi)(\rho)$ by definition. □

LEMMA 5.21. *Let $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ be a symbolic bisimulation. Then $\mathcal{R}_{\mathfrak{S}}$ is an open bisimulation.*

PROOF. Let $(\mathfrak{t}\psi)(\rho)\mathcal{R}_{\mathfrak{S}}(\mathfrak{u}\psi)(\rho)$ where $\mathfrak{t} = (\!|t, \mathcal{E}|\!)$ and $\mathfrak{u} = (\!|u, \mathcal{F}|\!)$. Then there exists b, such that $\psi(b) = \mathtt{tt}$ and $\mathfrak{t}\mathcal{S}^b\mathfrak{u}$. Thus we have

(1) $qv(t\psi) = qv(t) = qv(u) = qv(u\psi)$, and $\mathrm{tr}_{qv(t\psi)}\mathcal{E}(\rho) = \mathrm{tr}_{qv(t\psi)}\mathcal{F}(\rho)$ from $\mathcal{E} \eqsim_{\overline{qv(t)}} \mathcal{F}$.

(2) Suppose $\langle t\psi, \mathcal{E}(\rho)\rangle \stackrel{\alpha}{\longmapsto} \mu$. Then by Lemma 5.5, we have

$$(\!|t, \mathcal{E}|\!) \stackrel{b_1,\gamma}{\longrightarrow} \Delta' = \sum_{i\in I} \mathcal{A}_i \bullet (\!|t_i, \mathcal{E}_i\mathcal{E}|\!)$$

such that $\psi(b_1) = \mathtt{tt}$,

$$\mu = \sum_{i\in I} \mathrm{tr}(\mathcal{A}_i\mathcal{E}(\rho))\langle t_i\psi', \mathcal{E}_i\mathcal{E}(\rho)\rangle.$$

Furthermore, we have $\gamma = c?x$ for some $x \notin fv(t)$ and $\psi' = \psi\{v/x\}$ if $\alpha = c?v$, or $\gamma =_\psi \alpha$ and $\psi' = \psi$ otherwise. Note that if $\gamma = c?x$, we can always take x such that $x \notin fv(t, u, b, b_1)$ by α-conversion. Now by the assumption that $\mathfrak{t}\mathcal{S}^b\mathfrak{u}$, there exists a collection of booleans B such that $b \wedge b_1 \to \bigvee B$ and $\forall\, b' \in B$, $\exists b_2, \gamma'$ with $b' \to b_2$, $\gamma =_{b'} \gamma'$,

$$(\!|u, \mathcal{F}|\!) \stackrel{b_2,\gamma'}{\longrightarrow} \Xi' = \sum_{j\in J} \mathcal{B}_j \bullet (\!|u_j, \mathcal{F}_j\mathcal{F}|\!),$$

and $(\mathcal{E} \bullet \Delta')\mathcal{S}^{b'}(\mathcal{F} \bullet \Xi')$. Note that $\psi(b \wedge b_1) = \mathtt{tt}$ and $b \wedge b_1 \to \bigvee B$. We can always find a $b' \in B$ such that $\psi(b') = \mathtt{tt}$, thus $\psi(b_2) = \mathtt{tt}$ as well. Then by Lemma 5.6, we have

$$\langle u\psi, \mathcal{F}(\rho)\rangle \stackrel{\beta}{\longmapsto} \nu = \sum_{j\in J} \mathrm{tr}(\mathcal{B}_j\mathcal{F}(\rho))\langle u_j\psi'', \mathcal{F}_j\mathcal{F}(\rho)\rangle$$

where $\beta = c?v$ and $\psi'' = \psi\{v/x\}$ if $\gamma' = c?x$, or $\gamma' =_\psi \beta$ and $\psi'' = \psi$ otherwise. We claim that $\beta = \alpha$, and $\psi'' = \psi'$. There are three cases to consider:

(i) $\alpha = c?v$. Then $\gamma = c?x$ and $\psi' = \psi\{v/x\}$. So $\gamma' = c?x$ from $\gamma' =_{b'} \gamma$, which implies that $\beta = c?v = \alpha$, and $\psi'' = \psi\{v/x\} = \psi'$.
(ii) $\alpha = c!v$. Then $\gamma = c!e$, $\psi(e) = v$, and $\psi' = \psi$. So $\gamma' = c!e'$ with $b' \to e = e'$, which implies that $\beta = c!v'$ where $v' = \psi(e')$, and $\psi'' = \psi = \psi'$. Finally, from $\psi(b') = \mathtt{tt}$ we deduce $v' = v$.
(iii) For other cases, $\beta = \gamma' = \gamma = \alpha$, and $\psi'' = \psi = \psi'$.

Finally, by Lemma 5.20 we deduce $\mu\mathcal{R}_{\mathfrak{S}}\nu$ from the facts that $(\mathcal{E} \bullet \Delta')\mathcal{S}^{b'}(\mathcal{F} \bullet \Xi')$, $\mu = [(\mathcal{E} \bullet \Delta')\psi'](\rho)$, $\nu = [(\mathcal{F} \bullet \Xi')\psi'](\rho)$, and $\psi'(b') = \mathtt{tt}$.

(3) $\mathcal{R}_{\mathfrak{S}}$ is closed under super-operator application, as each $\mathcal{S}^b$ is.

□

COROLLARY 5.22. *Let $b \in BExp$, $t, u \in \mathcal{T}$, and $P, Q \in \mathcal{P}$. Then $t \sim^b u$ implies for any evaluation ψ, if $\psi(b) = \mathtt{tt}$ then $t\psi \dot{\sim} u\psi$.*

PROOF. Let $t \sim^b u$, and $\mathfrak{S} = \{\mathcal{S}^b : b \in BExp\}$ be a symbolic bisimulation such that $(\!|t, \mathcal{I}_{\mathcal{H}}|\!)\mathcal{S}^b(\!|u, \mathcal{I}_{\mathcal{H}}|\!)$. Then by Lemma 5.21, for any evaluation ψ and any ρ, $\psi(b) = \mathtt{tt}$ implies $\langle t\psi, \rho\rangle \dot{\sim} \langle u\psi, \rho\rangle$, thus $t\psi \dot{\sim} u\psi$ by definition. □

For any $b \in BExp$, define

$$\mathcal{S}^b_{\dot{\sim}} = \{(\mathfrak{t}, \mathfrak{u}) : \forall \psi, \psi(b) = \mathtt{tt} \text{ implies that for any } \rho \in \mathcal{D}(\mathcal{H}), (\mathfrak{t}\psi)(\rho) \dot{\sim} (\mathfrak{u}\psi)(\rho)\}.$$

We prove that $\mathfrak{S}_{\dot{\sim}} = \{\mathcal{S}^b_{\dot{\sim}} : b \in BExp\}$ is a symbolic bisimulation. Firstly, it is easy to check that for each b, $\mathcal{S}^b_{\dot{\sim}}$ is an equivalence relation. Then we can show the following lemma, which is parallel to Lemma 5.20.

LEMMA 5.23. *Let $b \in BExp$. If for any evaluation ψ,*

$$\psi(b) = \mathtt{tt} \textit{ implies that } \forall \rho \in \mathcal{D}(\mathcal{H}), (\Delta\psi)(\rho) \dot{\sim} (\Xi\psi)(\rho),$$

then $\Delta\, \mathcal{S}^b_{\dot{\sim}}\, \Xi$.

PROOF. Let $\Delta = \sum_{i\in I} \mathcal{A}_i \bullet (\!|t_i, \mathcal{E}_i|\!)$ and $\Xi = \sum_{j\in J} \mathcal{B}_j \bullet (\!|u_j, \mathcal{F}_j|\!)$. We prove this lemma by distinguishing two cases:

(1) Both $|I| > 1$ and $|J| > 1$. Similar to Lemma 5.20, we first decompose the set $\lceil\Delta\rceil \cup \lceil\Xi\rceil$ into disjoint subsets $S_1, \cdots, S_n$ such that any two snapshots are in the same S_k if and only if they are related by $\mathcal{S}^b_{\dot{\sim}}$. For each $1 \le k \le n$, let

$$K_k = \{i \in I : (\!|t_i, \mathcal{E}_i|\!) \in S_k\} \cup \{j \in J : (\!|u_j, \mathcal{F}_j|\!) \in S_k\} \tag{5}$$

and $\mathfrak{K} = \{K_k : 1 \le k \le n\}$. Note that by Lemma 5.4, there are two sets of pairwise orthogonal pure states $\{|\phi_i\rangle : i \in I\}$ and $\{|\phi'_j\rangle : j \in J\}$ in some $\mathcal{H}_{\tilde{q}}$ such that the Kraus operators of $\mathcal{A}_i$ and $\mathcal{E}_i$ are $\{|\phi_i\rangle\langle\phi_i|\}$ and $\{|\phi_i\rangle\langle\phi_{i'}| : i' \in I\}$, respectively, while the Kraus operators of $\mathcal{B}_j$ and $\mathcal{F}_j$ are $\{|\phi'_j\rangle\langle\phi'_j|\}$ and $\{|\phi'_j\rangle\langle\phi'_{j'}| : j' \in J\}$, respectively. Let $E_k = \sum_{i\in K_k\cap I} |\phi_i\rangle\langle\phi_i|$, and $F_k = \sum_{j\in K_k\cap J} |\phi'_j\rangle\langle\phi'_j|$. Then it suffices to show $E_k = F_k$, $1 \le k \le n$. In the following, we prove $E_1 = F_1$; other cases are similar.
For any ρ and ψ such that $\psi(b) = \mathtt{tt}$, we decompose the set $\lceil(\Delta\psi)(\rho)\rceil \cup \lceil(\Xi\psi)(\rho)\rceil$ into equivalence classes $R_1, \cdots, R_{m^\psi_\rho}$ according to $\dot{\sim}$. For each $1 \le l \le m^\psi_\rho$, let

$$L^{\psi,\rho}_l = \{i \in I : \langle t_i\psi, \mathcal{E}_i(\rho)\rangle \in R_l\} \cup \{j \in J : \langle u_j\psi, \mathcal{F}_j(\rho)\rangle \in R_l\}$$

and $\mathfrak{L}^{\psi,\rho} = \{L^{\psi,\rho}_l : 1 \le l \le R_{m^\psi_\rho}\}$. Note that by the definition of $\mathcal{S}^b_{\dot{\sim}}$, $\mathfrak{K}$ is a refinement of $\mathfrak{L}^{\psi,\rho}$ for any $\psi(b) = \mathtt{tt}$ and ρ. We assume without loss of generality that $L^{\psi,\rho}_1$ is the partition in $\mathfrak{L}^{\psi,\rho}$ which contains K_1, and $L^{\psi,\rho}_1 = K_1 \cup K^{\psi,\rho}_1$ where $K^{\psi,\rho}_1 = \bigcup_{k\in I_{\psi,\rho}} K_k$ and $I_{\psi,\rho}$ is a subset of $\{2, \cdots, n\}$.

As the effects of the super-operators $\mathcal{E}_i$ and $\mathcal{F}_j$ are simply erasing the original information at $\widetilde{q}$ and setting the partial states of $\widetilde{q}$ to be $|\phi_i\rangle$ and $|\phi'_j\rangle$, respectively, we have $\mathfrak{L}^{\psi,\rho} = \mathfrak{L}^{\psi,\sigma}$ (which means $m^{\psi}_{\rho} = m^{\psi}_{\sigma}$, and $L^{\psi,\rho}_l = L^{\psi,\sigma}_l$ for each l) for all σ with $\mathrm{tr}_{\widetilde{q}}\rho = \mathrm{tr}_{\widetilde{q}}\sigma$. Let $E^{\psi,\rho}_1 = \sum_{k\in I_{\psi,\rho}} E_k$ and $F^{\psi,\rho}_1 = \sum_{k\in I_{\psi,\rho}} F_k$. Note that $\mathrm{tr}(\mathcal{A}_i(\rho)) = \mathrm{tr}(|\phi_i\rangle_{\widetilde{q}}\langle\phi_i|\rho) = \mathrm{tr}(|\phi_i\rangle_{\widetilde{q}}\langle\phi_i|\rho_{\widetilde{q}})$ where $\rho_{\widetilde{q}}$ is the reduced state of ρ at the systems $\widetilde{q}$. Then for any $\rho' \in \mathcal{D}(\mathcal{H}_{\widetilde{q}})$,

$$\mathrm{tr}((E_1 + E^{\psi,\rho}_1)\rho') = \sum_{i\in L^{\psi,\sigma}_1\cap I} \mathrm{tr}(\mathcal{A}_i(\sigma)) = \sum_{j\in L^{\psi,\sigma}_1\cap J} \mathrm{tr}(\mathcal{B}_j(\sigma)) = \mathrm{tr}((F_1 + F^{\psi,\rho}_1)\rho')$$

where $\sigma = \rho' \otimes \mathrm{tr}_{\widetilde{q}}(\rho)$ is equal to ρ except at $\widetilde{q}$, and the second equality is from the assumption that $(\Delta\psi)(\sigma) \dot{\sim} (\Xi\psi)(\sigma)$. This implies $E_1 + E^{\psi,\rho}_1 = F_1 + F^{\psi,\rho}_1$.
Let $K = \bigcap_{\rho,\psi(b)=\mathtt{tt}} I_{\psi,\rho}$. We claim that $K = \emptyset$. Otherwise, there exists k such that $k \in I_{\psi,\rho}$ for any $\psi(b) = \mathtt{tt}$ and ρ. Then by the definition of $L^{\psi,\rho}_1$, we have $\langle t_i\psi, \mathcal{E}_i(\rho)\rangle \dot{\sim} \langle t_{i'}\psi, \mathcal{E}_{i'}(\rho)\rangle$ where $i \in K_1$ and $i' \in K_k$. Thus $(\!|t_i, \mathcal{E}_i|\!)\mathcal{S}^b_{\dot{\sim}}(\!|t_{i'}, \mathcal{E}_{i'}|\!)$, contradicting the fact that they belong to different equivalence classes of $\mathcal{S}^b_{\dot{\sim}}$.
Now for any pure state $|\phi\rangle$ such that $E_1|\phi\rangle = |\phi\rangle$, we have $E^{\psi,\rho}_1|\phi\rangle = 0$ for any ρ and $\psi(b) = \mathtt{tt}$, by the orthogonality of E_i's. Thus $F^{\psi,\rho}_1|\phi\rangle = |\phi\rangle - F_1|\phi\rangle$. Note that $F^{\psi',\rho'}_1 F^{\psi,\rho}_1 = \sum_{k\in I_{\psi,\rho}\cap I_{\psi',\rho'}} F_k = F^{\psi,\rho}_1 F^{\psi',\rho'}_1$ and $F^{\psi',\rho'}_1 F_1 = 0$. We have

$$\sum_{k\in I_{\psi,\rho}\cap I_{\psi',\rho'}} F_k|\phi\rangle = |\phi\rangle - F_1|\phi\rangle,$$

and finally, $\sum_{k\in K} F_k|\phi\rangle = |\phi\rangle - F_1|\phi\rangle$. Then $F_1|\phi\rangle = |\phi\rangle$ from the fact that $K = \emptyset$. Similarly, we can prove that for any $|\phi\rangle$, $F_1|\phi\rangle = |\phi\rangle$ implies $E_1|\phi\rangle = |\phi\rangle$. Thus $E_1 = F_1$.

(2) Either $|I| = 1$ or $|J| = 1$. Let us suppose $|I| = 1$, and $\Delta = (\!|t, \mathcal{E}|\!)$. We need to show that for each $j \in J$, $\mathcal{B}_j \neq 0_{\mathcal{H}}$ implies $(\!|t, \mathcal{E}|\!)\mathcal{S}^b_{\dot{\sim}}(\!|u_j, \mathcal{F}_j|\!)$. This is true because otherwise we can find $\psi(b) = \mathtt{tt}$, $j \in J$, and $\rho \in \mathcal{D}(\mathcal{H})$ such that $\mathrm{tr}(\mathcal{B}_j(\rho)) \neq 0$ but $\langle t\psi, \mathcal{E}(\rho)\rangle \dot{\nsim} \langle u_j\psi, \mathcal{F}_j(\rho)\rangle$. Thus $(\Delta\psi)(\rho) \dot{\nsim} (\Xi\psi)(\rho)$, a contradiction.

□

LEMMA 5.24. *The family* $\mathfrak{S}_{\dot{\sim}} = \{\mathcal{S}^b_{\dot{\sim}} : b \in BExp\}$ *is a symbolic bisimulation.*

PROOF. Let $b \in BExp$ and $\mathfrak{t}\mathcal{S}^b_{\dot{\sim}}\mathfrak{u}$. Then for any ψ, $\psi(b) = \mathtt{tt}$ implies that for any $\rho \in \mathcal{D}(\mathcal{H})$, $(\mathfrak{t}\psi)(\rho) \dot{\sim} (\mathfrak{u}\psi)(\rho)$. Let $\mathfrak{t} = (\!|t, \mathcal{E}|\!)$ and $\mathfrak{u} = (\!|u, \mathcal{F}|\!)$.

(1) If b is satisfiable, then $qv(t) = qv(t\psi) = qv(u\psi) = qv(u)$, and $\mathcal{E} \approx_{\overline{qv(t)}} \mathcal{F}$ from the fact that $\mathrm{tr}_{qv(t)}\mathcal{E}(\rho) = \mathrm{tr}_{qv(t)}\mathcal{F}(\rho)$ for any ρ.

(2) Suppose

$$(\!|t, \mathcal{E}|\!) \xrightarrow{b_1,\gamma} \Delta' = \sum_{i\in I} \mathcal{A}_i \bullet (\!|t_i, \mathcal{E}_i\mathcal{E}|\!) \tag{6}$$

with $bv(\gamma) \cap fv(b, t, u) = \emptyset$. We need to construct a set of booleans B such that $b \wedge b_1 \rightarrow \bigvee B$, and $\forall\, b' \in B$, $\exists b_2, \gamma'$ with $b' \rightarrow b_2$, $\gamma =_{b'} \gamma'$, $(\!|u, \mathcal{F}|\!) \xrightarrow{b_2,\gamma'} \Xi'$, and $(\mathcal{E} \bullet \Delta')\mathcal{S}^{b'}(\mathcal{F} \bullet \Xi')$. Let

$$U = \{\Theta : (\!|u, \mathcal{F}|\!) \xrightarrow{b(\Theta),\gamma(\Theta)} \Theta \text{ and } \gamma =_{\mathtt{ff}} \gamma(\Theta)\}.$$

Here similar to [Hennessy and Lin 1995], to ease the notations we only consider the case where for each Θ, there is at most one action, denoted by $(b(\Theta), \gamma(\Theta))$, such

that $(\!|u, \mathcal{F}|\!) \overset{b(\Theta),\gamma(\Theta)}{\longrightarrow} \Theta$. For each $\Theta \in U$, let b'_Θ be a boolean expression such that for any ψ,

$$\psi(b'_\Theta) = \mathtt{tt} \text{ if and only if for any } \rho, [(\mathcal{E} \bullet \Delta')\psi](\rho) \dot{\sim} [(\mathcal{F} \bullet \Theta)\psi](\rho). \tag{7}$$

Let $B = \{b_\Theta : \Theta \in U\}$, where $b_\Theta = b'_\Theta \wedge b''_\Theta \wedge b(\Theta)$ and b''_Θ is a boolean expression defined by

$$b''_\Theta \equiv \begin{cases} e = e' & \text{if } \gamma = c!e \text{ and } \gamma(\Theta) = c!e' \text{ are both classical output,} \\ \mathtt{tt} & \text{otherwise.} \end{cases} \tag{8}$$

Then obviously, $\gamma =_{b_\Theta} \gamma(\Theta)$. We check $b \wedge b_1 \to \bigvee B$. For any evaluation ψ such that $\psi(b \wedge b_1) = \mathtt{tt}$, we have by definition of $\mathcal{S}^b_{\dot{\sim}}$ that $\langle t\psi, \mathcal{E}(\rho)\rangle \dot{\sim} \langle u\psi, \mathcal{F}(\rho)\rangle$ for any ρ. On the other hand, by Lemma 5.6 and Eq.(6), for any v we have

$$\langle t\psi, \mathcal{E}(\rho)\rangle \overset{\alpha}{\longmapsto} \mu = \sum_{i\in I} \mathrm{tr}(\mathcal{A}_i\mathcal{E}(\rho))\langle t_i\psi', \mathcal{E}_i\mathcal{E}(\rho)\rangle$$

where $\alpha = c?v$ and $\psi' = \psi\{v/x\}$ if $\gamma = c?x$, and $\alpha =_\psi \gamma$ and $\psi' = \psi$ otherwise. To match this transition, we have

$$\langle u\psi, \mathcal{F}(\rho)\rangle \overset{\alpha}{\longmapsto} \nu$$

for some ν such that $\mu \dot{\sim} \nu$. Now from Lemma 5.5, there exists $\Xi' \in U$ such that $\psi(b(\Xi')) = \mathtt{tt}$,

$$(\!|u, \mathcal{F}|\!) \overset{b(\Xi'),\gamma(\Xi')}{\longrightarrow} \Xi' = \sum_{j\in J} \mathcal{B}_j \bullet (\!|u_j, \mathcal{F}_j\mathcal{F}|\!),$$

and

$$\nu = \sum_{j\in J} \mathrm{tr}(\mathcal{B}_j\mathcal{F}(\rho))\langle u_j\psi'', \mathcal{F}_j\mathcal{F}(\rho)\rangle.$$

Furthermore, we have $\gamma(\Xi') = c?y$ for some $y \notin fv(u)$ and $\psi'' = \psi\{v/y\}$ if $\alpha = c?v$, and $\alpha =_\psi \gamma(\Xi')$ and $\psi'' = \psi$ otherwise.
We claim that $\gamma =_\psi \gamma(\Xi')$, and $\psi'' = \psi'$. There are two cases to consider:

(i) $\gamma = c?x$. Then $\alpha = c?v$ and $\psi' = \psi\{v/x\}$, which implies that $\gamma(\Xi') = c?y$ for some $y \notin fv(u)$. By α-conversion and the fact that $x \notin fv(b, t, u)$, we can also take $y = x$. So $\gamma(\Xi') = \gamma$, and $\psi'' = \psi\{v/x\} = \psi'$.

(ii) For other cases, $\gamma(\Xi') =_\psi \alpha =_\psi \gamma$, and $\psi'' = \psi = \psi'$.

Now we have $\mu = [(\mathcal{E} \bullet \Delta')\psi'](\rho)$ and $\nu = [(\mathcal{F} \bullet \Xi')\psi'](\rho)$. Note that we can take $v = \psi(x)$ when $\gamma = c?x$ so that ψ and ψ' are always equal. Then we have $\psi(b'_{\Xi'}) = \mathtt{tt}$ from Eq.(7) and the arbitrariness of ρ. By Eq.(8) and the fact that $\gamma =_\psi \gamma(\Xi')$, we further derive that $\psi(b''_{\Xi'}) = \mathtt{tt}$. Therefore, $\psi(b_{\Xi'}) = \mathtt{tt}$, and so $\psi(\bigvee B) = \mathtt{tt}$.

For any $b_\Theta \in B$, we have $b_\Theta \to b(\Theta)$, $\gamma =_{b_\Theta} \gamma(\Theta)$, and $(\!|u, \mathcal{F}|\!) \overset{b(\Theta),\gamma(\Theta)}{\longrightarrow} \Theta$ by definition of B. Finally, for any evaluation ψ, if $\psi(b_\Theta) = \mathtt{tt}$ then $\psi(b'_\Theta) = \mathtt{tt}$, and from Eq.(7) we have $[(\mathcal{E} \bullet \Delta')\psi](\rho) \dot{\sim} [(\mathcal{F} \bullet \Xi')\psi](\rho)$ for any $\rho \in \mathcal{D}(\mathcal{H})$. Then $(\mathcal{E} \bullet \Delta')\mathcal{S}^{b_\Theta}_{\dot{\sim}} (\mathcal{F} \bullet \Theta)$ follows by Lemma 5.23.

□

COROLLARY 5.25. *If for any evaluation ψ, $\psi(b) = \mathtt{tt}$ implies $t\psi \dot{\sim} u\psi$, then $t \sim^b u$.*

PROOF. For any $\rho \in \mathcal{D}(\mathcal{H})$ and any evaluation ψ such that $\psi(b) = \mathtt{tt}$, we first derive $\langle t\psi, \rho\rangle \dot{\sim} \langle u\psi, \rho\rangle$ from the assumption that $t\psi \dot{\sim} u\psi$. Then by Lemma 5.24, we have $(\!|t, \mathcal{I}_\mathcal{H}|\!) \sim^b (\!|u, \mathcal{I}_\mathcal{H}|\!)$, and thus $t \sim^b u$ by definition. □

From the above lemmas, we finally reach our main result in this section, showing that the symbolic bisimulation presented in this paper coincides exactly with the open bisimulation introduced in [Deng and Feng 2012].

THEOREM 5.26. *Let $b \in BExp$, $t, u \in \mathcal{T}$, and $P, Q \in \mathcal{P}$. Then*

(1) $t \sim^b u$ if and only if for any evaluation ψ, $\psi(b) = \mathtt{tt}$ implies $t\psi \dot{\sim} u\psi$.
(2) $t \sim u$ if and only if $t \dot{\sim} u$.
(3) $P \sim^b Q$ if and only if $P \dot{\sim} Q$, provided that b is satisfiable.

PROOF. (1) is direct from Corollaries 5.22 and 5.25, while (2) and (3) from (1). □

6. AN ALGORITHM FOR SYMBOLIC GROUND BISIMULATION

From Clause (2) of Definition 5.7, to check whether two snapshots are symbolically bisimilar, we are forced to compare their behaviours under any super-operators. This is generally infeasible since all super-operators constitute a continuum, and it seems hopeless to design an algorithm which works for the most general case. In this section, we develop an efficient algorithm for symbolic ground bisimulation instead.

Note that many existing quantum communication protocols such as super-dense coding, teleportation, quantum key-distribution protocols, etc, are, or can easily be modified to be, free of quantum input. For example, recall that the quantum teleportation protocol can be described as follows [Feng et al. 2011; 2012]

$$\begin{aligned} Alice &= \mathsf{c}?q.\mathcal{CN}[q,q_1].\mathcal{H}[q].M[q,q_1;x].e!x.\mathbf{nil},\\ Bob &= e?x.\sum_{0\le i\le 3}(\mathbf{if}\ x=i\ \mathbf{then}\ \sigma^i[q_2].\mathsf{d}!q_2.\mathbf{nil}),\\ Tel &= (Alice\|Bob)\backslash\{e\}, \end{aligned}$$

and its soundness is guaranteed by the fact that Tel is bisimilar, when q_1 and q_2 are initially correlated as a maximally entangled state, to the ideal specification $\mathsf{c}?q.\mathcal{SW}_{1,3}[q,q_1,q_2].\mathsf{d}!q_2.\mathbf{nil}$, where $\mathcal{SW}_{1,3}$ is the 3-qubit unitary operator which exchanges the states of the first and the third qubits, keeping the second qubit untouched. To make the teleportation protocol free of quantum input, we simply delete $\mathsf{c}?q$ from $Alice$ and $\mathsf{d}!q_2$ from Bob. Denote by Tel' the resulting protocol. Then obviously, to show the soundness of Tel it suffices to prove that Tel' is bisimilar to $\mathcal{SW}_{1,3}[q,q_1,q_2].\mathbf{nil}$, again, when a maximally entangled state is present. The key point here is, for the purpose of analysis we can safely replace a quantum input by a free quantum variable, both in the implementation and in the specification. Now from Theorem 5.12 two quantum input free snapshots are symbolic bisimilar if and only if they are symbolic ground bisimilar. This technique works for any recursion-free processes, even if quantum inputs occur during the execution rather than at the very beginning. Thus our algorithm is actually applicable to verify the correctness of many existing quantum communication protocols.

Algorithm 1 computes the *most general boolean* b such that $\mathfrak{t} \sim_g^b \mathfrak{u}$, for two given snapshots $\mathfrak{t}$ and $\mathfrak{u}$ in a finite-state and finitely branching transition graph. By the most general boolean $mgb(\mathfrak{t},\mathfrak{u})$ we mean that $\mathfrak{t} \sim_g^{mgb(\mathfrak{t},\mathfrak{u})} \mathfrak{u}$ and whenever $\mathfrak{t} \sim_g^b \mathfrak{u}$ then $b \to mgb(\mathfrak{t},\mathfrak{u})$. From Theorem 5.12, this algorithm is applicable to verify the correctness of many existing quantum communication protocols.

The algorithm closely follows that introduced in [Hennessy and Lin 1995]. The main procedure is **Bisim**$(\mathfrak{t},\mathfrak{u})$. It starts with the initial snapshot pairs $(\mathfrak{t},\mathfrak{u})$, trying to find the smallest symbolic bisimulation relation containing the pair by comparing transitions from each pair of snapshots it reaches. The core procedure **Match** has four parameters: $\mathfrak{t}$ and $\mathfrak{u}$ are the current terms under examination; b is a boolean expression representing

the constraints accumulated by previous calls; W is a set of snapshot pairs which have been visited. For each possible action enabled by $\mathfrak{t}$ and $\mathfrak{u}$, the procedure **MatchAction** is used to compare possible moves from $\mathfrak{t}$ and $\mathfrak{u}$. Each comparison returns a boolean and a table; the boolean turns out to be $mgb(\mathfrak{t},\mathfrak{u})$ and the table is used to represent the witnessing bisimulation. We consider a table as a function that maps a pair of snapshots to a boolean. The disjoint union of tables, viewed as sets, is denoted by $\sqcup$.

The main difference from the algorithm of [Hennessy and Lin 1995] lies in the comparison of τ transitions. We introduce the procedure **MatchDistribution** to approximate $\sim_g^b$ by a relation $\mathcal{R}$. For any two snapshots $\mathfrak{t}_i \in \lceil\Delta\rceil$ and $\mathfrak{u}_j \in \lceil\Theta\rceil$, they are related by $\mathcal{R}$ if $b \to T(\mathfrak{t}_i,\mathfrak{u}_j)$. More precisely, we use the equivalence closure of $\mathcal{R}$ instead in order for it to be used in the procedure **Check**. Moreover, if a snapshot pair $(\mathfrak{t},\mathfrak{u})$ has been visited before, *i.e.* $(\mathfrak{t},\mathfrak{u}) \in W$, then $T(\mathfrak{t},\mathfrak{u})$ is assumed to be $\mathtt{tt}$ in all future visits. Hence, $\mathcal{R}$ is coarser than $\sim_g^b$ in general. We use $\mathbf{Check}(\Delta,\Theta,\mathcal{R})$ to compute the constraint so that the super-operator valued distribution Δ is related to Θ by a relation lifted from $\mathcal{R}$. The correctness of the algorithm is stated in the following theorem.

THEOREM 6.1. *For two snapshots* $\mathfrak{t}$ *and* $\mathfrak{u}$*, the function* $\boldsymbol{Bisim}(\mathfrak{t},\mathfrak{u})$ *terminates. Moreover, if* $\boldsymbol{Bisim}(\mathfrak{t},\mathfrak{u}) = (\theta, T)$ *then* $T(\mathfrak{t},\mathfrak{u}) = \theta = mgb(\mathfrak{t},\mathfrak{u})$.

PROOF. Termination is easy to show. Each time a new snapshot pair is encountered, the procedure **Match** is called and the pair is added to the set W. Since we are considering a finite-state transition graph, the number of different pairs is finite. Eventually every possible pair is in W and each call to **Match** immediately terminates.

Correctness of the algorithm is largely similar to that in [Hennessy and Lin 1995], though we use the additional procedure **MatchDistribution** to compute the constraint that relates two super-operator valued distributions. □

Let us consider the time complexity of the algorithm. Suppose the number of nodes in the transition graph reachable from $\mathfrak{t}$ and $\mathfrak{u}$ is n. The number of snapshot pairs examined by the algorithm is bounded by n^2. When a snapshot pair $(\mathfrak{t},\mathfrak{u})$ is examined, each transition of $\mathfrak{t}$ is compared with all the transitions of $\mathfrak{u}$ labelled with the same action. Since the transition graph is finitely branching, we could assume that each snapshot has at most c outgoing transitions. Therefore, for each snapshot pair, the number of comparisons of transitions is bounded by c^2. As a comparison of two transitions calls the function **MatchDistribution** once, which in turn may call **Check**. We regard quantum operations such as checking if $\mathcal{E} \eqsim_V \mathcal{F}$ as elementary operations. Then **Check** can finish in time $O(n^3/\log n)$ by computing the maximum flow in a network [Cheriyan et al. 1990; Deng and Du 2011]. As a result, examining each snapshot pair takes time $O(c^2n^3/\log n)$. Finally, the worst case time complexity of executing $\mathbf{Bisim}(\mathfrak{t},\mathfrak{u})$ is $O(n^5/\log n)$.

The complexity analysis is made by assuming the ability of real computation. To implement the algorithm, we have to approximate super-operators using matrices of algebraic or even rational numbers. This will increase the complexity of the algorithm, and it is practically very important to investigate how to minimise this increase by, say, designing better data structure for super-operators and developing efficient techniques to manipulate and compare them. However, this issue is of independent interest, and it is not the main concern of this paper.

7. MODAL CHARACTERISATION

We now present a Hennessy-Milner type modal logic to characterise the behaviour of quantum snapshots and their distributions.

ALGORITHM 1: Bisim$(\mathfrak{t},\mathfrak{u})$

Bisim$(\mathfrak{t},\mathfrak{u}) =$ **Match**$(\mathfrak{t},\mathfrak{u},\mathtt{tt},\emptyset)$

Match$(\mathfrak{t},\mathfrak{u},b,W) =$ where $\mathfrak{t} = (\!|t,\mathcal{E}|\!)$ and $\mathfrak{u} = (\!|u,\mathcal{F}|\!)$
if $(\mathfrak{t},\mathfrak{u}) \in W$ **then**
  $(\theta, T) := (\mathtt{tt}, \emptyset)$
else
  for $\gamma \in Act(\mathfrak{t},\mathfrak{u})$ **do**
    $(\theta_\gamma, T_\gamma) :=$ **MatchAction**$(\gamma,\mathfrak{t},\mathfrak{u},b,W)$
  end
  $(\theta, T) := (\bigwedge_\gamma \theta_\gamma,\ \bigsqcup_\gamma (T_\gamma \sqcup \{(\mathfrak{t},\mathfrak{u}) \mapsto (b \wedge \bigwedge_\gamma \theta_\gamma)\}))$
end
return $(\theta \wedge (qv(t) = qv(u)) \wedge (\mathcal{E} \approx_{\overline{qv(t)}} \mathcal{F}), T)$

MatchAction$(\gamma,\mathfrak{t},\mathfrak{u},b,W) =$
switch γ **do**
  case $c!$
    for $\mathfrak{t} \xrightarrow{b_i, c!e_i} \mathfrak{t}_i$ *and* $\mathfrak{u} \xrightarrow{b'_j, c!e'_j} \mathfrak{u}_j$ **do**
      $(\theta_{ij}, T_{ij}) :=$ **Match**$(\mathfrak{t}_i, \mathfrak{u}_j, b \wedge b_i \wedge b'_j \wedge e_i = e'_j, \{(\mathfrak{t},\mathfrak{u})\} \cup W)$
    end
    return $(\bigwedge_i (b_i \to \bigvee_j (b'_j \wedge e_i = e'_j \wedge \theta_{ij})) \wedge \bigwedge_j (b'_j \to \bigvee_i (b_i \wedge e_i = e'_j \wedge \theta_{ij})),\ \bigsqcup_{ij} T_{ij})$
  endsw
  case τ
    for $\mathfrak{t} \xrightarrow{b_i, \tau} \Delta_i$ *and* $\mathfrak{u} \xrightarrow{b'_j, \tau} \Theta_j$ **do**
      $(\theta_{ij}, T_{ij}) :=$ **MatchDistribution**$(\Delta_i, \Theta_j, b \wedge b_i \wedge b'_j, \{(\mathfrak{t},\mathfrak{u})\} \cup W)$
    end
    return $(\bigwedge_i (b_i \to \bigvee_j (b'_j \wedge \theta_{ij})) \wedge \bigwedge_j (b'_j \to \bigvee_i (b_i \wedge \theta_{ij})),\ \bigsqcup_{ij} T_{ij})$
  endsw
  otherwise
    for $\mathfrak{t} \xrightarrow{b_i, \gamma} \mathfrak{t}_i$ *and* $\mathfrak{u} \xrightarrow{b'_j, \gamma} \mathfrak{u}_j$ **do**
      $(\theta_{ij}, T_{ij}) :=$ **Match**$(\mathfrak{t}_i, \mathfrak{u}_j, b \wedge b_i \wedge b'_j, \{(\mathfrak{t},\mathfrak{u})\} \cup W)$
    end
    return $(\bigwedge_i (b_i \to \bigvee_j (b'_j \wedge \theta_{ij})) \wedge \bigwedge_j (b'_j \to \bigvee_i (b_i \wedge \theta_{ij})),\ \bigsqcup_{ij} T_{ij})$
  endsw
endsw

MatchDistribution(Δ,Θ,b,W)**=**
for $\mathfrak{t}_i \in \lceil\Delta\rceil$ *and* $\mathfrak{u}_j \in \lceil\Theta\rceil$ **do**
  $(\theta_{ij}, T_{ij}) :=$ **Match**$(\mathfrak{t}_i, \mathfrak{u}_j, b, W)$
end
$\mathcal{R} := \{(\mathfrak{t},\mathfrak{u}) \mid b \to (\bigsqcup_{ij} T_{ij})(\mathfrak{t},\mathfrak{u})\}^*$
return (**Check**$(\Delta,\Theta,\mathcal{R}),\ \bigsqcup_{ij} T_{ij}$)

Check$(\Delta,\Theta,\mathcal{R}) =$
$\theta := \mathtt{tt}$
for $S \in \lceil\Delta\rceil \cup \lceil\Theta\rceil / \mathcal{R}$ **do**
  $\theta := \theta \wedge (\Delta(S) \approx \Theta(S))$
end
return θ

Definition 7.1. The class $\mathcal{L}$ of quantum modal formulae over Act_s, ranged over by ϕ, Φ, etc, is defined by the following grammar:

$$\phi ::= \mathcal{G}_{\widetilde{q}} \mid \neg\phi \mid \bigwedge_{i\in I}\phi_i \mid \mathcal{G}.\phi \mid \langle\gamma\rangle\Phi$$

$$\Phi ::= Q_{\gtrsim\mathcal{A}}(\phi) \mid \bigwedge_{i\in I}\Phi_i$$

where $\mathcal{G} \in \mathcal{S}_t(\mathcal{H})$, $\gamma \in Act_s$, and $\mathcal{A} \in \mathcal{S}(\mathcal{H})$. We call ϕ a *snapshot formula* and Φ a *distribution formula*.

The satisfaction relation $\models \subseteq EV \times (SN \cup \mathcal{D}ist_{\mathcal{H}}(SN)) \times \mathcal{L}$ is defined as the minimal relation satisfying

— $\psi, \mathfrak{t} \models \mathcal{G}_{\widetilde{q}}$ if $qv(t) \cap \widetilde{q} = \emptyset$, and $\mathcal{E} \eqsim_{\widetilde{q}} \mathcal{G}$, where $\mathfrak{t} = (\!|t, \mathcal{E}|\!)$;
— $\psi, \mathfrak{t} \models \neg\phi$ if $\psi, \mathfrak{t} \not\models \phi$;
— $\psi, \mathfrak{t} \models \bigwedge_{i\in I}\phi_i$ if $\psi, \mathfrak{t} \models \phi_i$ for each $i \in I$;
— $\psi, \mathfrak{t} \models \mathcal{G}.\phi$ if $\mathcal{G} \in \mathcal{S}_t(\mathcal{H}_{\overline{qv(t)}})$ and $\psi, \mathcal{G}(\mathfrak{t}) \models \phi$, where $\mathcal{G}(\mathfrak{t}) = (\!|t, \mathcal{G}\mathcal{E}|\!)$ whenever $\mathfrak{t} = (\!|t, \mathcal{E}|\!)$;
— $\psi, \mathfrak{t} \models \langle\gamma\rangle\Phi$ if $\mathfrak{t} \xrightarrow{b,\gamma'} \Delta$ for some b, γ', and Δ, such that $\psi(b) = \mathtt{tt}$, $\gamma =_\psi \gamma'$, and $\psi, \Delta \models \Phi$;
— $\psi, \Delta \models Q_{\gtrsim\mathcal{A}}(\phi)$ if

$$\sum_{\mathfrak{t}\in\lceil\Delta\rceil}\{\Delta(\mathfrak{t}) : \psi, \mathfrak{t} \models \phi\} \gtrsim \mathcal{A};$$

— $\psi, \Delta \models \bigwedge_{i\in I}\Phi_i$ if $\psi, \Delta \models \Phi_i$ for each $i \in I$.

Definition 7.2. Let ψ be an evaluation. We write $\mathfrak{t} =^{\psi}_{\mathcal{L}} \mathfrak{u}$ if for any $\phi \in \mathcal{L}$,

$$\psi, \mathfrak{t} \models \phi \text{ if and only if } \psi, \mathfrak{u} \models \phi.$$

Similarly, $\Delta =^{\psi}_{\mathcal{L}} \Xi$ if for any $\Phi \in \mathcal{L}$,

$$\psi, \Delta \models \Phi \text{ if and only if } \psi, \Xi \models \Phi.$$

LEMMA 7.3. *Let ψ be an evaluation, $\mathfrak{t}, \mathfrak{u} \in SN$, and $\Delta, \Xi \in \mathcal{D}ist_{\mathcal{H}}(SN)$.*

(1) If $\mathfrak{t} \neq^{\psi}_{\mathcal{L}} \mathfrak{u}$, then there exists $\phi \in \mathcal{L}$, such that $\psi, \mathfrak{t} \models \phi$ but $\psi, \mathfrak{u} \not\models \phi$;
(2) If $\Delta \neq^{\psi}_{\mathcal{L}} \Xi$, then there exists $\Phi \in \mathcal{L}$, such that $\psi, \Delta \models \Phi$ but $\psi, \Xi \not\models \Phi$.

PROOF. (1) is easy as we have negation operator $\neg$ for state formulae. To prove (2), let $\Delta \neq^{\psi}_{\mathcal{L}} \Xi$, and Φ a distribution formula such that $\psi, \Delta \not\models \Phi$ but $\psi, \Xi \models \Phi$. We construct another distribution formula Φ' satisfying $\psi, \Delta \models \Phi'$ but $\psi, \Xi \not\models \Phi'$ by induction on the structure of Φ.

(i) $\Phi = Q_{\gtrsim\mathcal{A}}(\phi)$. Let

$$S = \{\mathfrak{u} \in SN : \psi, \mathfrak{u} \models \phi\} \qquad \text{and} \qquad \overline{S} = SN - S.$$

Then by definition, $\Xi(S) \gtrsim \mathcal{A}$ but $\Delta(S) \not\gtrsim \mathcal{A}$. Let $\mathcal{B} = \Delta(\overline{S})$ and $\Phi' = Q_{\gtrsim\mathcal{B}}(\neg\phi)$. Then we have trivially $\psi, \Delta \models \Phi'$. Now it suffices to show $\psi, \Xi \not\models \Phi'$. Otherwise, we have $\Xi(\overline{S}) \gtrsim \mathcal{B}$, and then

$$\mathcal{I}_{\mathcal{H}} \eqsim \Xi(S) + \Xi(\overline{S}) \gtrsim \mathcal{A} + \mathcal{B}.$$

On the other hand, we have

$$\mathcal{I}_{\mathcal{H}} \eqsim \Delta(S) + \Delta(\overline{S}) = \Delta(S) + \mathcal{B}.$$

Comparing the two formulae above, we conclude that $\Delta(S) \gtrsim \mathcal{A}$, a contradiction.

(ii) $\Phi = \bigwedge_{i\in I} \Phi_i$. Then by definition, $\psi, \Xi \models \Phi_i$ for each $i \in I$ but $\psi, \Delta \not\models \Phi_{i_0}$ for some $i_0 \in I$. By induction we have Φ'_{i_0} such that $\psi, \Delta \models \Phi'_{i_0}$ but $\psi, \Xi \not\models \Phi'_{i_0}$.

□

With this lemma, we can show that the logic $\mathcal{L}$ exactly characterises the behaviours of quantum snapshots up to symbolic bisimilarity.

THEOREM 7.4. *Let* $\mathfrak{t}$ *and* $\mathfrak{u}$ *be two snapshots and* $b \in BExp$. *Then* $\mathfrak{t} \sim^b \mathfrak{u}$ *if and only if for any evaluation* ψ, $\psi(b) = \mathtt{tt}$ *implies* $\mathfrak{t} =^{\psi}_{\mathcal{L}} \mathfrak{u}$.

PROOF. We first prove the necessity part. For any $\phi, \Phi \in \mathcal{L}$, it suffices to prove the following two properties:

$$\forall\, \mathfrak{t}, \mathfrak{u}, \psi,\ \text{if } \mathfrak{t} \sim^b \mathfrak{u} \text{ and } \psi(b) = \mathtt{tt} \text{ then } \psi, \mathfrak{t} \models \phi \Leftrightarrow \psi, \mathfrak{u} \models \phi,$$
$$\forall\, \Delta, \Xi, \psi,\ \text{if } \Delta \sim^b \Xi \text{ and } \psi(b) = \mathtt{tt} \text{ then } \psi, \Delta \models \Phi \Leftrightarrow \psi, \Xi \models \Phi.$$

We proceed by mutual induction on the structures of ϕ and Φ. Take arbitrarily $\mathfrak{t} \sim^b \mathfrak{u}$, $\Delta \sim^b \Xi$, and $\psi(b) = \mathtt{tt}$. Let $\mathfrak{t} = (\!|t, \mathcal{E}|\!)$, $\mathfrak{u} = (\!|u, \mathcal{F}|\!)$, $\psi, \mathfrak{t} \models \phi$, and $\psi, \Delta \models \Phi$. There are seven cases to consider:

— $\phi = \mathcal{G}_{\widetilde{q}}$. Then $qv(t) \cap \widetilde{q} = \emptyset$ and $\mathcal{E} \eqsim_{\widetilde{q}} \mathcal{G}$. Since $\mathfrak{t} \sim^b \mathfrak{u}$ and b is satisfiable, we have $qv(t) = qv(u)$ and $\mathcal{E} \eqsim_{\overline{qv(t)}} \mathcal{F}$. Thus $qv(u) \cap \widetilde{q} = \emptyset$, and $\mathcal{F} \eqsim_{\widetilde{q}} \mathcal{G}$ from the fact that $\widetilde{q} \subseteq \overline{qv(t)}$. Then $\psi, \mathfrak{u} \models \mathcal{G}_{\widetilde{q}}$ follows.

— $\phi = \neg\phi'$. Then $\psi, \mathfrak{t} \not\models \phi'$. By induction we have $\psi, \mathfrak{u} \not\models \phi'$, and $\psi, \mathfrak{u} \models \phi$.

— $\phi = \bigwedge_{i\in I} \phi_i$. Then $\psi, \mathfrak{t} \models \phi_i$ for each $i \in I$. By induction we have $\psi, \mathfrak{u} \models \phi_i$, and $\psi, \mathfrak{u} \models \phi$.

— $\phi = \mathcal{G}.\phi'$. Then $\mathcal{G} \in \mathcal{S}_t(\mathcal{H}_{\overline{qv(t)}})$ and $\psi, \mathcal{G}(\mathfrak{t}) \models \phi'$. Since $\mathfrak{t} \sim^b \mathfrak{u}$, we have $\mathcal{G}(\mathfrak{t}) \sim^b \mathcal{G}(\mathfrak{u})$ by proposition 5.10, and $qv(t) = qv(u)$. By induction we have $\psi, \mathcal{G}(\mathfrak{u}) \models \phi'$, and $\psi, \mathfrak{u} \models \phi$.

— $\phi = \langle\gamma\rangle\Phi'$. Then $\mathfrak{t} \xrightarrow{b_1, \gamma'} \Delta'$ for some b_1, γ', and Δ' such that $\psi(b_1) = \mathtt{tt}$, $\gamma =_{\psi} \gamma'$, and $\psi, \Delta' \models \Phi'$. Since $\mathfrak{t} \sim^b \mathfrak{u}$, there exists a collection of booleans B such that $b \wedge b_1 \to \bigvee B$ and $\forall\ b' \in B$, $\exists b_2, \gamma'$ with $b' \to b_2$, $\gamma' =_{b'} \gamma'$, $\mathfrak{u} \xrightarrow{b_2, \gamma'} \Xi'$, and $\Delta' \sim^{b'} \Xi'$. Note that $\psi(b \wedge b_1) = \mathtt{tt}$. We can find a $b' \in B$ such that $\psi(b') = \mathtt{tt}$. Thus $\psi(b_2) = \mathtt{tt}$, and $\gamma =_{\psi} \gamma'$. Furthermore, by induction we have $\psi, \Xi' \models \Phi'$ from $\Delta' \sim^{b'} \Xi'$ and $\psi, \Delta' \models \Phi'$. So $\psi, \mathfrak{u} \models \langle\gamma\rangle\Phi'$.

— $\Phi = Q_{\gtrsim\mathcal{A}}(\phi')$. Let $S = \{\mathfrak{t} \in SN : \psi, \mathfrak{t} \models \phi'\}$. Then by definition, $\Delta(S) \gtrsim \mathcal{A}$. Furthermore, by induction we can see that S is the disjoint union of some equivalence classes $S_1, \cdots, S_k$ of $\sim^b$. Thus

$$\Xi(S) = \Xi(S_1) + \cdots + \Xi(S_k) \eqsim \Delta(S_1) + \cdots + \Delta(S_k) = \Delta(S) \gtrsim \mathcal{A}$$

where the $\eqsim$ equality is derived from the assumption that $\Delta \sim^b \Xi$.

— $\Phi = \bigwedge_{i\in I} \Phi_i$. Then $\psi, \Delta \models \Phi_i$ for each $i \in I$. By induction we have $\psi, \Xi \models \Phi_i$, and $\psi, \Xi \models \Phi$.

By symmetry, we also have $\psi, \mathfrak{u} \models \phi$ implies $\psi, \mathfrak{t} \models \phi$ and $\psi, \Xi \models \Phi$ implies $\psi, \Delta \models \Phi$. That completes the proof of the necessity part.

We now turn to the sufficiency part. By Lemma 5.24, we need only to prove that $\mathfrak{t} =^{\psi}_{\mathcal{L}} \mathfrak{u}$ implies $(\mathfrak{t}\psi)(\rho) \dot{\sim} (\mathfrak{u}\psi)(\rho)$ for all $\rho \in \mathcal{D}(\mathcal{H})$. Let

$$\mathcal{R} = \{((\mathfrak{t}\psi)(\rho), (\mathfrak{u}\psi)(\rho)) : \rho \in \mathcal{D}(\mathcal{H}), \psi \in EV,\ \text{and } \mathfrak{t} =^{\psi}_{\mathcal{L}} \mathfrak{u}\}$$

It suffices to show that $\mathcal{R}$ is an open bisimulation. Suppose $(\mathfrak{t}\psi)(\rho)\mathcal{R}(\mathfrak{u}\psi)(\rho)$. Then $\mathfrak{t} =^{\psi}_{\mathcal{L}} \mathfrak{u}$, and

$$qv(t\psi) = qv(t) = qv(u) = qv(u\psi).$$

We further claim that $\mathrm{tr}_{qv(t)}\mathcal{E}(\rho) = \mathrm{tr}_{qv(t)}\mathcal{F}(\rho)$. Otherwise there exists $\widetilde{q} \subseteq \overline{qv(t)}$ such that $\mathcal{E} \not\approx_{\widetilde{q}} \mathcal{F}$. Then $\psi, \mathfrak{t} \models \mathcal{E}_{\widetilde{q}}$ while $\psi, \mathfrak{u} \not\models \mathcal{E}_{\widetilde{q}}$, a contradiction.

Now let $(\mathfrak{t}\psi)(\rho) \stackrel{\alpha}{\longmapsto} \mu$. By Lemma 5.5 we have $\mathfrak{t} \stackrel{b_1,\gamma}{\longrightarrow} \Delta_\mu$ such that $\psi(b_1) = \mathtt{tt}$, $\mu = (\Delta_\mu\psi')(\rho)$, and

(1) if $\alpha = c?v$ then $\gamma = c?x$ for some $x \notin fv(t)$, and $\psi' = \psi\{v/x\}$,
(2) otherwise, $\gamma =_\psi \alpha$ and $\psi' = \psi$.

Let

$$\mathcal{K} = \{\nu \in Dist(Con) : (\mathfrak{u}\psi)(\rho) \stackrel{\alpha}{\longmapsto} \nu \text{ and not } \mu\mathcal{R}\nu\}.$$

For any $\nu \in \mathcal{K}$, by Lemma 5.5 we have $\mathfrak{u} \stackrel{b(\Xi_\nu),\gamma(\Xi_\nu)}{\longrightarrow} \Xi_\nu$ such that $\psi(b(\Xi_\nu)) = \mathtt{tt}$, $\nu = (\Xi_\nu\psi'')(\rho)$, and

(1) if $\alpha = c?v$ then $\gamma(\Xi_\nu) = c?x$ for some $x \notin fv(u)$, and $\psi'' = \psi\{v/x\}$,
(2) otherwise, $\gamma(\Xi_\nu) =_\psi \alpha$ and $\psi'' = \psi$.

Here again, to ease the notations we only consider the case where for each Ξ, there is at most one pair, denoted $(b(\Xi), \gamma(\Xi))$, such that $\mathfrak{u} \stackrel{b(\Xi),\gamma(\Xi)}{\longrightarrow} \Xi$. Furthermore, by α-conversion, we can always take $\gamma(\Xi_\nu) =_\psi \gamma$ and $\psi'' = \psi'$. For any $\nu \in \mathcal{K}$, we claim $\Delta_\mu \neq^{\psi}_{\mathcal{L}} \Xi_\nu$. Otherwise, since $\mu = (\Delta_\mu\psi')(\rho)$ and $\nu = (\Xi_\nu\psi')(\rho)$, we have $\mu\mathcal{R}\nu$, a contradiction. Thus, from Lemma 7.3 (2), there exists $\Phi_\nu \in \mathcal{L}$ such that $\psi, \Delta_\mu \models \Phi_\nu$ but $\psi, \Xi_\nu \not\models \Phi_\nu$. Let

$$\Phi_\mu = \bigwedge\{\Phi_\nu : \nu \in \mathcal{K}\} \text{ and } \phi = \langle\gamma\rangle\Phi_\mu.$$

Then $\psi, \Delta_\mu \models \Phi_\mu$, thus $\psi, \mathfrak{t} \models \phi$. Since $\mathfrak{t} =^{\psi}_{\mathcal{L}} \mathfrak{u}$, we have $\psi, \mathfrak{u} \models \phi$ too. That is, there exists Θ such that $\psi(b(\Theta)) = \mathtt{tt}$, $\gamma =_\psi \gamma(\Theta)$, and $\psi, \Theta \models \Phi_\mu$. Now by Lemma 5.6, we have $(\mathfrak{u}\psi)(\rho) \stackrel{\alpha'}{\longmapsto} \omega = (\Theta\psi''')(\rho)$ such that

(1) if $\gamma(\Theta) = c?x$ then $\alpha' = c?v$ for some $v \in \mathsf{Real}$, and $\psi''' = \psi\{v/x\}$,
(2) otherwise, $\alpha' =_\psi \gamma(\Theta)$ and $\psi''' = \psi$.

By transition rule $C\text{-}Inp_c$, we can alway choose $\alpha' = \alpha$, and $\psi''' = \psi'$. We claim that $\omega \notin \mathcal{K}$. Otherwise, if $\omega \in \mathcal{K}$ then $\psi, \Xi_\omega \not\models \Phi_\omega$, and $\psi, \Xi_\omega \not\models \Phi_\mu$ as well. This is a contradiction since by assumption, $\Xi_\omega = \Theta$. So $\omega \notin \mathcal{K}$, and $\mu\mathcal{R}\omega$ as required.

Finally, we prove that $\mathcal{R}$ is closed under super-operator application. To this end, we only need to show that $=^{\psi}_{\mathcal{L}}$ is ; that is, for any $\mathcal{G} \in \mathcal{S}_t(\mathcal{H}_{\overline{qv(t)}})$, $\mathfrak{t} =^{\psi}_{\mathcal{L}} \mathfrak{u}$ implies $\mathcal{G}(\mathfrak{t}) =^{\psi}_{\mathcal{L}} \mathcal{G}(\mathfrak{u})$. Suppose $\mathfrak{t} =^{\psi}_{\mathcal{L}} \mathfrak{u}$ and let ϕ be a formula such that $\psi, \mathcal{G}(\mathfrak{t}) \models \phi$. Then $\psi, \mathfrak{t} \models \mathcal{G}.\phi$. It follows from $\mathfrak{t} =^{\psi}_{\mathcal{L}} \mathfrak{u}$ that $qv(t) = qv(u)$ and $\psi, \mathfrak{u} \models \mathcal{G}.\phi$. Therefore, $\psi, \mathcal{G}(\mathfrak{u}) \models \phi$. By symmetry if ϕ is satisfied by $\psi, \mathcal{G}(\mathfrak{u})$ then it is also satisfied by $\psi, \mathcal{G}(\mathfrak{t})$. In other words, we have $\mathcal{G}(\mathfrak{t}) =^{\psi}_{\mathcal{L}} \mathcal{G}(\mathfrak{u})$. Then $\mathcal{R}$ is an open bisimulation by proposition 5 of [Deng and Feng 2012]. □

For any $t, u \in \mathcal{T}$ and $b \in BExp$, we write $t =^{b}_{\mathcal{L}} u$ if for any evaluation ψ, $\psi(b) = \mathtt{tt}$ implies $(\!|t, \mathcal{I}_{\mathcal{H}}|\!) =^{\psi}_{\mathcal{L}} (\!|u, \mathcal{I}_{\mathcal{H}}|\!)$. Then we have the following theorem:

THEOREM 7.5. *For any $t, u \in \mathcal{T}$, $t \sim^b u$ if and only if $t =^{b}_{\mathcal{L}} u$.*

8. CONCLUSION AND FURTHER WORK

The main contribution of this paper is a notion of symbolic bisimulation for qCCS, a quantum extension of classical value-passing CCS. By giving the operational semantics of qCCS directly by means of the super-operators a process can perform, we are able to assign to each (non-recursively defined) quantum process a *finite* super-operator weighted labelled transition system, in contrast with the *infinite* probabilistic labelled transition system in previous literature. We prove that the symbolic bisimulation in this paper coincides with the open bisimulation in [Deng and Feng 2012], thus providing a practical way to decide the latter. We also design an algorithm to check symbolic ground bisimulation, which is applicable to reasoning about many existing quantum communication protocols. A modal logic characterisation for the symbolic bisimulation is also developed.

A natural extension of the current paper is to study symbolic weak bisimulation where the invisible actions, caused by internal (classical and quantum) communication as well as quantum operations, are abstracted away. To achieve this, we may need to define symbolic weak transitions similar to those proposed in [Feng et al. 2011; 2012; Deng and Feng 2012]. Note that one of the distinct features of weak transitions for probabilistic processes is the so-called left decomposability; that is, if $\mu \Longrightarrow \nu$ and $\mu = \sum_{i\in I} p_i\mu_i$ is a probabilistic decomposition of μ, then ν can be decomposed into $\sum_{i\in I} p_i\nu_i$ accordingly such that $\mu_i \Longrightarrow \nu_i$ for each $i \in I$. This property is essential in proving the transitivity of bisimilarity. However, it is not satisfied by symbolic transitions defined in this paper since, in general, a super-operator does not have an inverse. Therefore, we will have to explore other ways of defining weak symbolic transitions, which is one of the research directions we are now pursuing.

We have presented in this paper, for the first time in the literature to the best of our knowledge, the notion of super-operator weighted labelled transition systems, which serves as the semantic model for qCCS and plays an important role in describing and reasoning about quantum processes. For the next step, we are going to explore the possibility of model checking quantum communication protocols based on this model. As is well known, one of the main challenges for quantum model checking is that the set of all quantum states, traditionally regarded as the underlying state space of the models to be checked, forms a continuum. The techniques of classical model checking, which normally work only for finite state space, cannot be applied directly. Gay et al. [Gay et al. 2006; 2008; Papanikolaou 2008] provided a solution for this problem by restricting the state space to a set of finitely describable states called stabiliser states, and restricting the quantum operations applied on them to the class of Clifford group. By doing this, they were able to obtain an efficient model checker for quantum protocols, employing purely classical algorithms. The limit of their approach is obvious: it can only check the (partial) behaviours of a protocol on stabiliser states, and does not work for general protocols.

Our approach of treating both classical data and quantum operations in a symbolic way provides an efficient and compact way to describe behaviours of a quantum protocol without resorting to the underlying quantum states. In this model, all existing quantum protocols have finite state spaces, and consequently, classical model checking techniques will hopefully be adapted to verifying quantum protocols. Some preliminary work has been reported in [Feng et al. 2013].

REFERENCES

BENNETT, C. H. AND BRASSARD, G. 1984. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computer, Systems and Signal Processing*. 175–179.

BENNETT, C. H., BRASSARD, G., CREPEAU, C., JOZSA, R., PERES, A., AND WOOTTERS, W. 1993. Teleporting an unknown quantum state via dual classical and EPR channels. *Physical Review Letters 70*, 1895–1899.

BENNETT, C. H. AND WIESNER, S. J. 1992. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters 69,* 20, 2881–2884.

BURCH, J. R., CLARKE, E. M., MCMILLAN, K. L., DILL, D. L., AND HWANG, L. J. 1992. Symbolic model checking: 10^{20} states and beyond. *Information and Computation 98,* 2, 142–170.

CHERIYAN, J., HAGERUP, T., AND MEHLHORN, K. 1990. Can a maximum flow be computed in $o(nm)$ time? In *Automata, Languages and Programming*, M. Paterson, Ed. Lecture Notes in Computer Science Series, vol. 443. Springer Berlin Heidelberg, 235–248.

DAVIDSON, T. A. S. 2011. Formal Verification Techniques using Quantum Process Calculus. Ph.D. thesis.

DENG, Y. AND DU, W. 2011. Logical, Metric, and Algorithmic Characterisations of Probabilistic Bisimulation. arXiv:1103.4577v1 [cs.LO]. Tech. rep.

DENG, Y. AND FENG, Y. 2012. Open Bisimulation for Quantum Processes. In *Proc. IFIP TCS'12*. LNCS. Springer, 119–133. Full version available at http://arxiv.org/abs/1202.3484.

FENG, Y., DUAN, R., JI, Z., AND YING, M. 2007. Probabilistic bisimulations for quantum processes. *Information and Computation 205,* 11, 1608–1639.

FENG, Y., DUAN, R., AND YING, M. 2011. Bisimulation for quantum processes. In *Proceedings of the 38th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. ACM, 523–534.

FENG, Y., DUAN, R., AND YING, M. 2012. Bisimulation for Quantum Processes. *ACM Transactions on Programming Languages and Systems 34,* 4, 1–43.

FENG, Y., YU, N., AND YING, M. 2013. Journal of Computer and System Sciences. *Journal of Computer and System Sciences 79,* 7, 1181–1198.

GAY, S., NAGARAJAN, R., AND PAPANIKOLAOU, N. 2006. Probabilistic model-checking of quantum protocols. In *Proceedings of the 2nd International Workshop on Developments in Computational Models*.

GAY, S., NAGARAJAN, R., AND PAPANIKOLAOU, N. 2008. QMC: A model checker for quantum systems. In *CAV '08*. Springer, 543–547.

GAY, S. J. AND NAGARAJAN, R. 2005. Communicating quantum processes. In *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, J. Palsberg and M. Abadi, Eds. 145–157.

HENNESSY, M. AND INGÓLFSDÓTTIR, A. 1993. A theory of communicating processes value-passing. *Information and Computation 107,* 2, 202–236.

HENNESSY, M. AND LIN, H. 1995. Symbolic bisimulations. *Theoretical Computer Science 138,* 2, 353–389.

JORRAND, P. AND LALIRE, M. 2004. Toward a Quantum Process Algebra. In *Proceedings of the 2nd International Workshop on Quantum Programming Languages, 2004*, P. Selinger, Ed. 111.

KRAUS, K. 1983. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Springer.

KUBOTA, T., KAKUTANI, Y., KATO, G., KAWANO, Y., AND SAKURADA, H. 2012. Application of a process calculus to security proofs of quantum protocols. In *Proceedings of FCS'12 - The International Conference on Foundations of Computer Science*.

LALIRE, M. 2006. Relations among Quantum Processes: Bisimilarity and Congruence. *Mathematical Structures in Computer Science 16(3)*, 407–428.

MILNER, R. 1989. *Communication and Concurrency*. Prentice Hall, Englewood Cliffs, NJ.

NIELSEN, M. AND CHUANG, I. 2000. *Quantum computation and quantum information*. Cambridge university press.

PAPANIKOLAOU, N. K. 2008. Model Checking Quantum Protocols. Ph.D. thesis.

SANGIORGI, D. 1996. A Theory of Bisimulation for the pi-Calculus. *Acta Informatica 33,* 1, 69–97.

VON NEUMANN, J. 1955. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Princeton University Press.

YING, M., FENG, Y., DUAN, R., AND JI, Z. 2009. An algebra of quantum processes. *ACM Transactions on Computational Logic (TOCL) 10,* 3, 1–36.