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.
Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.
c 0 ACM 1529-3785/0/-ART0 $10.00
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* H is a complete vector space equipped with an inner product

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

such that

(1) $\langle \psi | \psi \rangle \geq 0$ for any $|\psi\rangle \in H$, with equality if and only if $|\psi\rangle = 0$;
(2) $\langle \psi | \varphi \rangle = \langle \varphi | \psi \rangle^{\dagger}$;
(3) $\langle \psi | \sum_i c_i |\varphi_i\rangle = \sum_i c_i \langle \psi | \varphi_i \rangle$,

where $\mathbb{C}$ is the set of complex numbers, and for each $c \in \mathbb{C}$, $c^{\dagger}$ stands for the complex conjugate of c. For any vector $|\psi\rangle \in H$, 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 $|\varphi\rangle$ are *orthogonal* if $\langle \psi | \varphi \rangle = 0$. An *orthonormal basis* of a Hilbert space H is a basis $\{|i\rangle\}$ where each $|i\rangle$ is normalised and any pair of them are orthogonal.

Let $\mathcal{L}(H)$ be the set of linear operators on H. For any $A \in \mathcal{L}(H)$, A is *Hermitian* if $A^{\dagger} = A$ where $A^{\dagger}$ is the adjoint operator of A such that $\langle \psi | A^{\dagger} | \varphi \rangle = \langle \varphi | A | \psi \rangle$ for any $|\psi\rangle, |\varphi\rangle \in H$. The fundamental *spectral theorem* states that the set of all normalised

eigenvectors of a Hermitian operator in $L(H)$ constitutes an orthonormal basis for 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 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 $A \in L(H)$ is *unitary* if $A^\dagger A = AA^\dagger = I_H$ where I_H is the identity operator on H. The *trace* of A is defined as $tr(A) = \sum_i \langle i|A|i\rangle$ for some given orthonormal basis $\{|i\rangle\}$ of 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 $tr(AB) = tr(BA)$ for any operators $A, B \in L(H)$.

Let H_1 and H_2 be two Hilbert spaces. Their *tensor product* $H_1 \otimes H_2$ 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 $|\psi_1\rangle \in H_1$ and $|\psi_2\rangle \in H_2$. Here the tensor product of two vectors is defined by a new vector such that

$$\left(\sum_i a_i|\psi_i\rangle\right) \otimes \left(\sum_j b_j|\varphi_j\rangle\right) = \sum_{i,j} a_i b_j |\psi_i\rangle \otimes |\varphi_j\rangle.$$

Then $H_1 \otimes H_2$ is also a Hilbert space where the inner product is defined as the following: for any $|\psi_1\rangle, |\varphi_1\rangle \in H_1$ and $|\psi_2\rangle, |\varphi_2\rangle \in H_2$,

$$\langle \psi_1 \otimes \psi_2 | \varphi_1 \otimes \varphi_2 \rangle = \langle \psi_1 | \varphi_1 \rangle_{H_1} \langle \psi_2 | \varphi_2 \rangle_{H_2}$$

where $\langle \cdot | \cdot \rangle_{H_i}$ is the inner product of H_i. For any $A_1 \in L(H_1)$ and $A_2 \in L(H_2)$, $A_1 \otimes A_2$ is defined as a linear operator in $L(H_1 \otimes H_2)$ such that for each $|\psi_1\rangle \in H_1$ and $|\psi_2\rangle \in H_2$,

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

The *partial trace* of $A \in L(H_1 \otimes H_2)$ with respect to H_1 is defined as $tr_{H_1}(A) = \sum_i \langle i|A|i\rangle$ where $\{|i\rangle\}$ is an orthonormal basis of H_1. Similarly, we can define the partial trace of A with respect to H_2. Partial trace functions are also independent of the orthonormal basis selected.

Traditionally, a linear operator E on $L(H)$ is called a *super-operator* on H. A super-operator is said to be *completely positive* if it maps positive operators in $L(H)$ to positive operators in $L(H)$, and for any auxiliary Hilbert space H', the trivially extended operator $I_{H'} \otimes E$ also maps positive operators in $L(H' \otimes H)$ to positive operators in $L(H' \otimes H)$. Here $I_{H'}$ is the identity operator on $L(H')$. The elegant and powerful *Kraus representation theorem* [Kraus 1983] of completely positive super-operators states that a super-operator E is completely positive if and only if there is some set of operators $\{E_i : i \in I\}$ with appropriate dimension such that

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

for any $A \in L(H)$. The operators E_i are called Kraus operators of E. We abuse the notation slightly by denoting $E = \{E_i : i \in I\}$. A super-operator E is said to be *trace-nonincreasing* if $tr(E(A)) \leq tr(A)$ for any positive $A \in L(H)$, 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 $\mathcal{CN} = \{\mathcal{C}_N\}$ 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 $\mathcal{H} = \{\mathcal{H}\}$, and Pauli super-operators $\mathcal{E}_0 = \{\mathcal{I}_2\}$; $\mathcal{E}_1 = \{\mathcal{X}\}$; $\mathcal{E}_2 = \{\mathcal{Z}\}$, and $\mathcal{E}_3 = \{\mathcal{Y}\}$ where

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

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

We also use the notations $X; Z$, and Y to denote $\mathcal{E}_1$; $\mathcal{E}_2$, and $\mathcal{E}_3$, 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 $p_i > 0$, $\sum_i p_i = 1$, 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

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

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 $M = \{M_0[|0\rangle], M_1[|1\rangle]\}$ is applied on the first qubit of $|\beta_{00}\rangle$ (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 M_0 or M_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 $_1$ and $_2$, respectively, then $_2 = U\ _1U^y$ 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 $U(\ ) = U\ \ U^y$ is a trace-preserving super-operator.

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

$$p(m) = \mathrm{tr}(M_m^y M_m\ );$$

and the state of the post-measurement system is $M_m\ \ M_m^y=p(m)$*:*

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

$$M = \sum_{m2spec(M)} mE_m \tag{1}$$

its spectral decomposition. Obviously, the projectors $fE_m : m\ 2\ spec(M)g$ form a quantum measurement. If the state of a quantum system is , then the probability that result m occurs when measuring M on the system is $p(m) = \mathrm{tr}(E_m\ )$*;* and the post-measurement state of the system is $E_m\ \ E_m=p(m)$*:* Note that for each outcome m, the map

$$E_m(\ ) = E_m\ \ E_m$$

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 $m\ 2\ spec(M)$, 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 , $:$, $\wedge$, $\_$, and $!$. In particular, we let $e\ ./\ e'$ be a boolean expression for any $e; e'\ 2\ Exp$ and $./2\ f>; <;\ \ ;\ ; =g$. 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 $c; d; \ldots$. 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 $\tilde{q}$ when $q_1,\ldots,q_n$ are distinct quantum variables and the dimension n is understood. Sometimes we also use $\tilde{q}$ 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 $\tilde{x}$ is a tuple of classical variables with $|\tilde{x}| = ar_c(A)$, and $\tilde{q}$ a tuple of distinct quantum variables with $|\tilde{q}| = ar_q(A)$, then $A(\tilde{x};\tilde{q})$ 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

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

where $c \in cChan$, $x \in cVar$, $c \in qChan$, $q \in qVar$, $\tilde{q} \subseteq qVar$, $e \in Exp$, $\tilde{e} \subseteq Exp$, τ is the silent action, $A(\tilde{x};\tilde{q})$ is a process constant, f is a relabelling function, $L \subseteq Chan$, $b \in BExp$, and 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 $\tilde{q}$. 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 $c!q.t$ 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:

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

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 $M[\tilde{q};x]$ has binding power on x. A quantum process term t is closed if $fv(t) = \emptyset$. We let $\mathcal{T}$, ranged over by $t, u, \ldots$, be the set of all qCCS terms, and $\mathcal{P}$, ranged over by $P, Q, \ldots$, the set of closed terms. To complete the definition of qCCS syntax, we assume that for each process constant $A(\tilde{x};\tilde{q})$, there is a defining equation

$$A(\tilde{x};\tilde{q}) \stackrel{def}{=} t$$

where $fv(t) \subseteq \tilde{x}$ and $qv(P) \subseteq \tilde{q}$. 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 $c?q$ and $c!q$ are their quantum counterparts. $E[\tilde{q}]$ denotes the action of performing the super-operator E on the qubits $\tilde{q}$ while $M[\tilde{q};x]$ measures the qubits $\tilde{q}$ 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 tt .

An evaluation is a function from $cVar$ to Real; it can be extended in an obvious way to functions from Exp to Realand from $BExp$ to $f$tt ; ff g, and finally, from T to P. For simplicity, we still use to denote these extensions. Let fv/xg be the evaluation which differs from 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 H_q to be the state space of the q-system. For any $S \subseteq qVar$, we denote

$$H_S = \bigotimes_{q \in S} H_q.$$

In particular, $H = H_{qVar}$ is the state space of the whole environment consisting of all the quantum variables. Note that 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 $\rho \in \mathcal{D}(H)$ is a density operator on H (As H is infinite dimensional, should be understood as a density operator on some finite dimensional subspace of H which contains $H_{qv(P)}$). The set of configurations is denoted Con, and ranged over by $C, D, \ldots$. Let

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

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

Let $Dist(Con)$, ranged over by $\Delta, \Theta, \ldots$, 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) $\langle Con, Act_c, \to \rangle$, where $\to \subseteq Con \times Act_c \times Dist(Con)$ 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 $C \to D$ if $C \to$ where is the simple distribution such that $(D) = 1$. We also use the obvious extension of the function κ on configurations to distributions. To be precise, if $= \sum_{i \in I} p_i \langle P_i, \rho_i \rangle$ then κQ denotes the distribution $\sum_{i \in I} p_i \langle P_i, \kappa Q \rho_i \rangle$. Similar extension applies to $[f]$ and νL.

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 $\Delta \mathcal{R}$ if

(1) $= \sum_{i \in I} p_i C_i$,
(2) for each $i \in I$, $C_i \mathcal{R} D_i$ for some D_i, and
(3) $= \sum_{i \in I} p_i D_i$.

Note that here the configurations $C_i, i \in I,$ 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 $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$,

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

(2) for any trace-preserving super-operator E acting on $H_{\overline{qv(P)}}$ (Again, E should be understood as a super-operator on some finite dimensional subspace of $H_{\overline{qv(P)}}$), whenever $\langle P; E(\ )i \not\rightarrow$, there exists such that $\langle Q; E(\ )i \not\rightarrow$ and R .

Definition 3.2.

(1) Two quantum configurations $\langle P;\ i$ and $\langle Q;\ i$ are open bisimilar, denoted by $\langle P;\ i \ \dot{} \ \langle Q;\ i$, if there exists an open bisimulation R such that $\langle P;\ iR\langle Q;\ i$;
(2) Two quantum process terms t and u are open bisimilar, denoted by $t \ \dot{} \ u$, if for any quantum state $\in D(H)$ and any evaluation , $\langle t\ ;\ i \ \dot{} \ \langle u\ ;\ i$:

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 $P \stackrel{def}{=} Set^0[q].I[q].\mathbf{nil}$ and

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

where $Set^0 = \{|0\rangle\langle 0|, |0\rangle\langle 1|\}$, $M_{0;1}$ is the 1-qubit measurement according to the computational basis $\{|0\rangle, |1\rangle\}$, I is the identity super-operator, and X is the Pauli-X super-operator. For any $\in D(H)$, the pLTSs rooted 6 Tf 86.055 0 Td [(nu9.962(81uper)37(-operator)10v.0 6.97q8

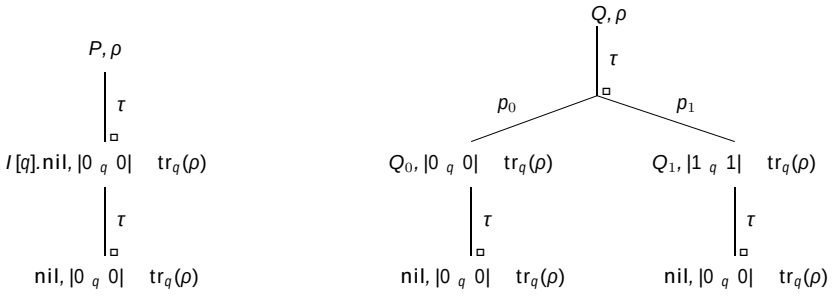


Fig. 2. pLTSs for the two ways of setting a quantum system to $|0\rangle$

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

$$R = \{(\langle P;\ \ i;\langle Q;\ \ i\rangle;(\langle I[q]{:}\mathbf{nil};\ \ _0\rangle i;\langle Q_0;\ \ _0\rangle i);\\ (\langle I[q]{:}\mathbf{nil};\ \ _0\rangle i;\langle Q_1;\ \ _1\rangle i);(\langle \mathbf{nil};\ \ _0\rangle i;\langle \mathbf{nil};\ \ _0\rangle i) : \quad 2\ D(H)\}$$

and $_i = |i\rangle\langle i|_q \quad \mathrm{tr}_q$, 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 $\mathcal{S}(H)$ the set of super-operators on H, ranged over by $\mathcal{A};\mathcal{B};\quad$. Obviously, both $(\mathcal{S}(H);0_H;+)$ and $(\mathcal{S}(H);I_H;\ )$ are monoids, where I_H and 0_H are the identity and null super-operators on H, respectively, and $\ $ is the composition of super-operators defined by $(\mathcal{A}\ \mathcal{B})(\ ) = \mathcal{A}(\mathcal{B}(\ ))$ for any $\ 2\ D(H)$. We always omit the symbol $\ $ and write $\mathcal{A}\mathcal{B}$ directly for $\mathcal{A}\ \mathcal{B}$. Furthermore, the operation $\ $ 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 $(\mathcal{S}(H);+;\ )$ forms a semiring.

For any $\mathcal{A};\mathcal{B}\ 2\ \mathcal{S}(H)$ and $V \quad qVar$, we write $\mathcal{A}\ .\ _V\ \mathcal{B}$ if for any $\ 2\ D(H)$, $\mathrm{tr}_{\overline{V}}(\mathcal{A}(\ ))\ v\ \mathrm{tr}_{\overline{V}}(\mathcal{B}(\ ))$, where $\overline{V}$ is the complement set of V in $qVar$, and v is the Löwner preorder defined on operators such as $A\ v\ B$ if and only if $B \quad A$ is positive semi-definite. Let $\approx_V$ be $.\ _V\ \backslash\ \&_V$. We usually abbreviate $.\ _{;}$ and $\approx_{;}$ to $.\ $ and $\approx$, respectively. It is easy to check that if $\mathcal{A}$ and $\mathcal{B}$ have Kraus operators $\{A_i : i\ 2\ I\}$ and $\{B_j : j\ 2\ J\}$ respectively, then $\mathcal{A}\ .\ \mathcal{B}$ if and only if $\sum_{i2I} A_i^\dagger A_i\ v\ \sum_{j2J} B_j^\dagger B_j$. The following proposition is direct from definitions:

PROPOSITION 4.1. *Let $\mathcal{A}$ and $\mathcal{B}\ 2\ \mathcal{S}(H)$. Then*

(1) $\mathcal{A} \approx I_H$ if and only if $\mathcal{A}$ is trace-preserving, i.e., $\mathrm{tr}(\mathcal{A}(\ )) = \mathrm{tr}(\ )$ *for any* $\ 2\ D(H)$.
(2) $\mathcal{A} \approx 0_H$ if and only if $\mathcal{A} = 0_H$.

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

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

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

LEMMA 4.3. *Let $A; A' \in \mathcal{S}(H)$ and $B \in \mathcal{S}(H_V)$ where $\overline{V} \not\subseteq V \subseteq qVar$. If $A \approx_V A'$, then both $AB \approx_V A'B$ and $BA \approx_V BA'$.*

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

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

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 $\mathcal{S}(H)$ such that $\sum_{s \in S} \Delta(s) \approx I_H$. We denote by $\lceil \Delta \rceil$ the support set of Δ, *i.e.*, the set of s such that $\Delta(s) \not\approx 0_H$. Let $Dist_H(S)$ be the set of finite-support super-operator valued distributions over S; that is,

$$Dist_H(S) = \{\Delta : S \to \mathcal{S}(H) \mid \lceil \Delta \rceil \text{ is finite, and } \sum_{s \in \lceil \Delta \rceil} \Delta(s) \approx I_H\}.$$

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

Definition 4.4. Given $\{\Delta_i : i \in I\} \subseteq Dist_H(S)$ and $\{A_i : i \in I\} \subseteq \mathcal{S}(H)$, $\sum_{i \in I} A_i \approx I_H$, we define the combination, denoted by $\sum_{i \in I} A_i \circledast \Delta_i$, to be a new distribution such that

(1) $\lceil \Theta \rceil = \bigcup \{\lceil \Delta_i \rceil : i \in I; A_i \not\approx 0_H\}$,
(2) for any $s \in \lceil \Theta \rceil$, $\Theta(s) = \sum_{i \in I} \Delta_i(s) A_i$.

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

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 pI_H where $0 \leq p \leq 1$. Since in this case all super-operators commute, we always omit the bullet $\bullet$ in the expressions.

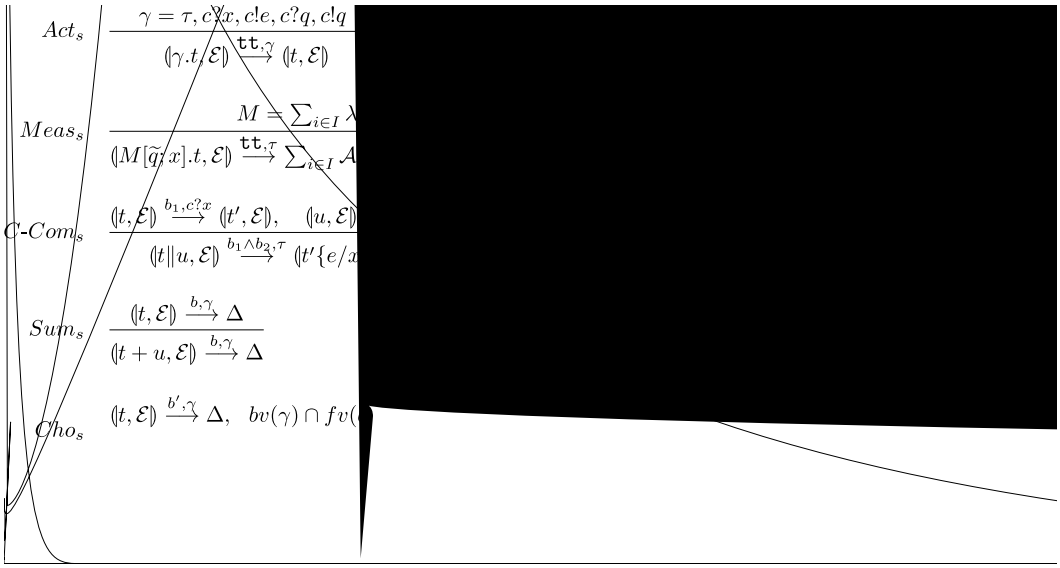


Fig. 3. Symbolic operational semantics of qCCS

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 $(S; Act; \quad !)$, where

(1) S is a countable set of states,
(2) Act is a countable set of transition actions,
(3) $\quad !$ is a subset of $S \quad Act \quad Dist_H(S)$.

For simplicity, we write $s \quad !$ instead of $(s; \ ; \ ) \ 2 \ !$. 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

$$Act_s = f \ g \ [\ fc?x; c!e \ j \ c \ 2 \ cChan; x \ 2 \ cVar; e \ 2 \ Expg$$
$$[\ fc?r; c!r \ j \ c \ 2 \ qChan; r \ 2 \ qVarg$$

and $BAct_s = BExp \quad Act_s$. For each $\quad 2 \ Act_s$, the notions $qbv(\ )$, $cn(\ )$, and $fv(\ )$ are similarly defined as for Act_c. We also define $bv(\ )$, the set of bound classical variables in $\quad$ in an obvious way.

A pair of the form $(\!|t; E|\!)$, where $t \ 2 \ T$ and $E \ 2 \ S_t(H)$, is called a snapshot. The set of snapshots is denoted by SN and sometimes ranged over by $t; u; \quad$. Then the symbolic semantics of qCCS is given by the qLTS $(SN; BAct_s; \quad !)$ on snapshots, where

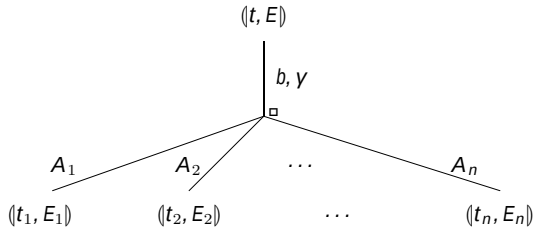
$! \quad SN \quad BAct_s \quad Dist_H(SN)$ is the smallest relation satisfying the rules defined in Fig. 3. In Rule $Meas_s$, for each $i \ 2 \ I$, $A_{e}{}^{i} \ 2 \ S(H)$ and $Set_{e}{}^{i} \ 2 \ S_t(H)$ are defined respectively as

$$A_{e}{}^{i} : \quad \overline{?} \ j \ _{j} i_{e} h \ _{i} j \ j \ _{i} i_{e} h \ _{i} j \tag{2}$$

$$Set_{e}{}^{i} : \quad \overline{?} \ \bigtimes_{j \ 2 \ I} j \ _{i} i_{e} h \ _{j} j \ j \ _{j} i_{e} h \ _{i} j: \tag{3}$$

The symmetric forms for rules Par_s, $C\text{-}Com_s$, $Q\text{-}Com_s$, and Sum_s are omitted. Here again, the functions k, $[f]$, and nL have been extended to super-operator valued distributions by denoting, say, ku the distribution $\sum_{i \ 2 \ I} A_i \ (\!|t_i ku; E_i|\!)$, if $= \sum_{i \ 2 \ I} A_i \ (\!|t_i; E_i|\!)$.

The transition graph of a snapshot is depicted as usual where each transition $(\!|t; E|\!) \ ^{b;} ! \ \sum_{i=1}^{n} A_i \ (\!|t_i; E_i|\!)$ is depicted as



For simplicity, lines marked with I_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 $j0i$, presented in Example 3.3. According to the symbolic operational semantics presented in Fig. 3, the qLTSs rooted by $(\!|P; I_H|\!)$ and $(\!|Q; I_H|\!)$ respectively can be depicted as in Fig. 4, where A_i has the single Kraus operator $ji i_q hij$ 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 ; 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 $M = \sum_{i=0}^{3} ij\overline{i}ih\overline{i}j$ be a 2-qubit measurement where $\overline{i}$ is the binary expansion of i. Let CN be the controlled-not operation and H the Hadamard operation. Then the quantum processes that participate in the super-dense coding protocol can be defined as follows:

$$Alice \stackrel{def}{=} c_A?q_1: \bigtimes_{0 \ i \ 3} \textbf{if } x = i \textbf{ then } \ ^{i}[q_1]:e!q_1:\textbf{nil} \ ;$$

$$Bob \stackrel{def}{=} c_B?q_2:e?q_1:CN[q_1; q_2]:H[q_1]:M[q_1; q_2; x]:d!x:\textbf{nil};$$

$$EPR \stackrel{def}{=} Set^{\Psi}[q_1; q_2]:c_B!q_2:c_A!q_1:\textbf{nil};$$

$$Sdc \stackrel{def}{=} c?x:(EPR \| Alice \| Bob) \backslash \{c_A; c_B; e\}:$$

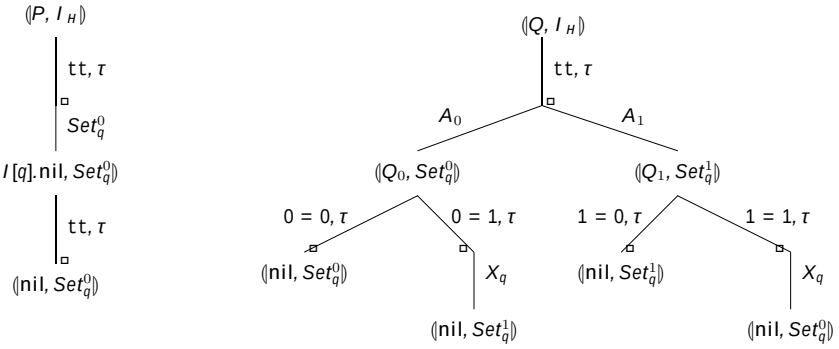


Fig. 4. qLTSs for two ways of setting a quantum system to $|0\rangle$

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

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

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 $|\Psi_i\rangle$ 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 $\langle\!| Sdc_{spec}; I_H |\!\rangle$ and $\langle\!| Sdc; I_H |\!\rangle$ respectively are depicted in Fig. 5 where $\mathbf{e} = \{q_1, q_2\}$, $A_{\mathbf{e}}$ is the super-operator with the single Kraus operator $|\Psi_i\rangle\langle\Psi_i|$, $L = \{c_A, c_B, e\}$,

$$Sdc^{x} = \sum_{i=0}^{3}(\mathbf{if}\ x = i\ \mathbf{then}\ \ ^{i}[q_1]:e!q_1:\mathbf{nil})\ \ \backslash\ L:$$

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* $\langle\!| t; E |\!\rangle \xrightarrow{b;\tau} \ldots$, *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) $\sum_{i\in I}\mathcal{B}_i \simeq \mathcal{I}_{\mathcal{H}}$,

(2) $\ldots = \sum_{i\in I}\mathcal{B}_i(\langle\!| t_i; \mathcal{F}_i E |\!\rangle)$;

(3) for any $G \in \mathcal{S}_t(\mathcal{H})$, $\langle\!| t; G |\!\rangle \xrightarrow{b;\tau} \sum_{i\in I}\mathcal{B}_i(\langle\!| t_i; \mathcal{F}_i G |\!\rangle)$.

Especially, if $|I| > 1$ *then* $\mathcal{B}_i$ *and* $\mathcal{F}_i$ *take the forms as* $\mathcal{A}_{\mathbf{e}^i}$ *and* $\mathcal{S}et_{\mathbf{e}^i}$ *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 $\ldots$ be an evaluation, $\ldots \in \mathcal{A}ct_c$, and $\ldots \in \mathcal{A}ct_s$. We write $\ldots = \ldots$ if either $\ldots = c!v$, $\ldots = c!e$, and $(e) = v$, or $\ldots = \ldots$ if neither of them is a classical output.

Fig. 5. qLTSs for LSdc_{spec} ; I_H M and LSdc; I_H M

LEMMA 5.5. Suppose $\langle t, \alpha \rangle \to$. Then there exist $b, I, \rho', \{A_i : i \in I\} \subseteq S(H)$, $\{E_i : i \in I\} \subseteq S_t(H)$, and $\{t_i : i \in I\} \subseteq T$, such that $\sum_{i \in I} A_i^\dagger A_i \sqsubseteq I_H$, and

(1) $(b) \rho = \rho$ tt ,
(2) $= \sum_{i \in I} \mathrm{tr}(A_i(\rho))\langle t_i, \rho'/\mathrm{tr}(A_i(\rho))\rangle$,
(3) for any $E \in S_t(H)$, $\langle t, E\rho\rangle \xrightarrow{b,\alpha} \sum_{i \in I} A_i \langle t_i, E_i\rho\rangle$, where
   (a) if $\alpha = c?v$ then $\alpha = c?x$ for some $x \notin fv(t)$, and $\rho' = \rho\{v/x\}$,
   (b) otherwise, $\alpha = \alpha$ and $\rho' = \rho$.

PROOF. We prove by induction on the depth of the inference by which the action $\langle t, \alpha \rangle \to$ is inferred. We argue by cases on the form of t.

(1) $t = c?x:t_0$. Then $t \alpha = c?x:u$ where u is the process term obtained from t_0 by instantiating all the free variables in $fv(t_0) \setminus \{x\}$ according to α. By Rule C-Inp$_c$ we deduce that $\alpha = c?v$ for some $v \in$ Real and $\rho' = \langle P, \rho'' \rangle$ where $P = u\{v/x\} = t_0\{v/x\}$. By Rule Act$_s$, for any $E \in S_t(H)$, we have $\langle t, E\rho\rangle \xrightarrow{\mathrm{tt}, c?x} \langle t_0, E\rho\rangle$. So we need only to take $b = \mathrm{tt}$, $|I| = 1$, $t_i = t_0$, $A_i = E_i = I_H$.
(2) $t = c!e:t_0$. Then $t \alpha = c!(e):(t_0 \alpha)$, and by Rule C-Out$_c$ we deduce that $\alpha = c!(e)$ and $\rho' = \langle t_0, \rho''\rangle$. By Rule Act$_s$, for any $E \in S_t(H)$, we have $\langle t, E\rho\rangle \xrightarrow{\mathrm{tt}, c!e} \langle t_0, E\rho\rangle$. So we need only to take $b = \mathrm{tt}$, $|I| = 1$, $t_i = t_0$, $A_i = E_i = I_H$ as well.
(3) $t = c?q:t_0$. Then $t \alpha = c?q:(t_0 \alpha)$, and by Rule Q-Inp$_c$ we deduce that $\alpha = c?r$ for some $r \notin qv(t)$ and $\rho' = \langle (t_0 \alpha)\{r/q\}, \rho''\rangle$. By Rule Act$_s$ and α-conversion, for any $E \in S_t(H)$,