Probabilistic bisimulations for quantum processes

Yuan Feng [a] Runyao Duan [a] Zhengfeng Ji [b] Mingsheng Ying [a]

[a] *State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology, Tsinghua University, Beijing, 100084, China*

[b] *State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, 100084, China*

Abstract

Modeling and reasoning about concurrent quantum systems is very important for both distributed quantum computing and quantum protocol verification. As a consequence, a general framework formally describing communication and concurrency in complex quantum systems is necessary. For this purpose, we propose a model named qCCS. It is a natural quantum extension of classical value-passing CCS which can deal with input and output of quantum states, and unitary transformations and measurements on quantum systems. The operational semantics of qCCS is given in terms of probabilistic labeled transition system. This semantics has many different features compared with the proposals in the available literature in order to describe the input and output of quantum systems which are possibly correlated with other components. Based on this operational semantics, the notions of strong probabilistic bisimulation and weak probabilistic bisimulation between quantum processes are introduced. Furthermore, some properties of these two probabilistic bisimulations, such as congruence under various combinators, are examined.

Key words: quantum process, probabilistic bisimulation, congruence

1. Introduction

Much attention has been devoted to quantum computation and quantum information theory (QCQI) in the last two decades since Feynman [8] proposed the idea that a quantum mechanical system can be used to perform computation. Benefiting from the possibility of superposition of different basis states and the linearity of quantum operations, quantum computing may provide considerable speedup over its classical analogue

Email addresses: feng-y@tsinghua.edu.cn (Yuan Feng), dry@tsinghua.edu.cn (Runyao Duan), jizhengfeng98@mails.tsinghua.edu.cn (Zhengfeng Ji), yingmsh@tsinghua.edu.cn (Mingsheng Ying).

[33,12,13]. To provide techniques of considering computational problems in a conceptual way, rather than focusing on the details of low-level implementations, some authors began to study the design and semantics of quantum programming languages. Knill made the first step by proposing a set of basic principles for writing quantum pseudo-codes [17], while the first real quantum programming language, QCL, is due to Ömer [25,26]. A quantum programming language in the style of Dijkstra's guarded-command language, qGCL, was designed by Sanders and Zuliani in [28,39,40]. They also presented a probabilistic predicate transformer semantics and a refinement calculus for their language. A quantum extension of C++ was proposed by Bettelli et al [5], and it was implemented in the form of a C++ library. The first functional quantum programming language, QPL, was proposed by Selinger [32] based on the idea of classical control and quantum data. For detailed surveys on quantum programming languages and related researches, we refer to [31] or [9].

The languages presented so far are, however, mostly designed for sequential quantum computing, where no communication between physically separated parties is considered. Design and investigation of languages which can describe quantum concurrent systems and their communication behaviors have just begun. On the other hand, although constructing real quantum computers in which quantum programming can be applied is very difficult, quantum cryptography [7,2,1], which can provide absolute security in principle even when it has been attacked by a potential quantum eavesdropper, has been developed so rapidly that quantum cryptographic systems became commercially available recently [27]. So, to some extent the need for a language describing concurrent systems is more urgent than that for sequential computations in the realm of quantum computation. Furthermore, a framework of modeling and reasoning about quantum concurrent systems will provide techniques to prove the properties, such as correctness and security, of quantum cryptographic protocols, just as we have noticed in classical world.

The first step of constructing such a general framework of modeling quantum concurrent systems was made independently by Jorrand and Lalire [16], and Gay and Nagarajan [10]. In [16], a process algebra for quantum processes was proposed which can describe both classical and quantum information passing. Later on, Lalire presented for their language a probabilistic branching bisimulation which identifies quantum processes associated with process graphs having the same branching structure [19,20]. In [10], a language called CQP (Communicating Quantum Processes), which combined the communication primitives of pi-calculus from [22] with primitives for unitary transformations and measurements, was defined. One distinctive feature of CQP is a type system which can guarantee the physical realizability of quantum processes. However, no equivalence notions between processes were presented there.

The main purpose of this paper is to propose a different model for quantum concurrent systems. This model, which we call qCCS, is a quantum extension of classical value-passing CCS [14,15]. To avoid no-go operations such as quantum cloning in syntactical level, we explicitly introduce the notion of free quantum variables, which intuitively denote the quantum systems a process can reference. When constructing more complicated processes from simpler ones, this type of variables must be taken into consideration. For example, if q is one of the free quantum variables of P then the process $\mathsf{c}!q.P$ is invalid because we cannot reference a quantum system when it has been output. This is in sharp contrast with classical variables, as classical values can be copied arbitrarily so that we can use them even after they have been output. As a consequence, the syntax of

qCCS is more complicated than those in [10] and [16]. But a type system as introduced in [10] is not necessary in qCCS. Note also that in [16], there was no such mechanism to avoid invalid quantum processes.

In classical process algebra, both call-by-value and call-by-name strategies can be adopted in the design of semantics. This flexibility is partially due to the fact that classical information can be cloned arbitrarily, and so we can talk about classical information without explicitly referring to the physical carrier of the information. Quantum information, however, cannot be perfectly cloned unless it is known. So the only universal way to realize quantum information transmission is to transfer the physical system which carries the information. As a consequence, only call-by-name semantics can be given in quantum process algebra.

To present the operational semantics of qCCS, we introduce the notion of configuration which is a pair consisting of a quantum process and an accompanied context instantiating all free quantum variables of the process. Intuitively, the context describes the quantum environment in which the process is performed. The operational semantics of qCCS is then given as a probabilistic labeled transition system consisting of configurations. There are some differences between our approach and the previous ones presented in literature. The first one is that in our semantics, transitions are from configurations to probability distributions over configurations, *i.e.*

$$\rightarrow \subseteq Con \times Act \times D(Con)$$

where Con is the set of configurations and $D(Con)$ is the set of finite-support distributions on Con. Notice that in [16] and [10], probabilistic choice induced by quantum measurement was resolved in each step. This was achieved by introducing a new kind of transition $\rightarrow_p$ to represent an evolution which is caused by an internal action and occurs with probability p. In this paper, however, we do not resolve any probabilistic choice in intermediate steps but instead keep the probability information all the time. The motivation for us to make such a design decision is as follows. First, transitions defined in this way make our operational semantics much simpler and more CCS-like; second, it gives us a convenient way to define combined transitions (resp. combined weak transitions) which are obtained by probabilistically taking different transitions with the same source configuration and the same actions (resp. observable actions). That is, the nondeterminism resulting from the non-probabilistic choice '+' can be resolved in a probabilistic manner. This is exactly the basis of strong bisimulation and weak bisimulation defined in this paper. Finally, by defining transitions in this way, many notions and techniques introduced in [29] and [30] for classical probabilistic processes can be extended to investigate the properties of probabilistic bisimulations between quantum processes.

The second difference between our approach of semantics and the previous ones is the ways of dealing with quantum input, quantum output, and quantum communication. The quantum input rule presented in [16] can only describe the case when the input system is initially not correlated with the systems the process holds. We introduce a new inference rule in this paper to deal with the general case where these systems are correlated. The rule for quantum output is also refined to keep track of possible correlation between an output system and the retained systems. As a consequence, the quantum communication rule in our qCCS has a very simple and CCS-like form. Note that in [10], no rules for quantum input and output were introduced because the authors took the viewpoint that any input action is necessarily accompanied with an output action (no matter from

another process or the environment). However, we still think it necessary to present rules describing input and output, since they give us a compositional way to describe quantum communication between different components.

The main contribution of this paper is a new notion of (strong and weak) probabilistic bisimulation between quantum processes. As mentioned above, Lalire [19] has proposed a notion of probabilistic branching bisimulation. Our bisimulations, however, are based on different probabilistic labeled transition system and motivated by different considerations: First, for two bisimilar configurations, any action performed by one configuration can be simulated by a combined action of the other. That is, different transitions with the same source configuration and the same action can be chosen simultaneously with different probabilities to simulate a single transition. Second, the final states of the quantum contexts when all matching actions have been executed must be the same when we want to check if two configurations are bisimilar. We add this requirement because unitary transformations and measurements are both considered as internal actions, and the effects of these kinds of actions can be fully reflected only by the state change of quantum contexts. Finally, note that in qCCS, a transition from a configuration generally leads to a finite-support distribution over configurations, and from each resulted configuration, different configurations can again be derived with different probabilities. As a consequence, the execution of a sequence of actions from a quantum configuration typically forms a tree rather than a linear path as in classical non-probabilistic case; any internal actions along any branch of the tree should be ignored when weak probabilistic bisimulation is concerned.

1.1. *Overview of this paper*

This paper is organized as follows: in Section 2, we review some basic notions from linear algebra and quantum mechanics which will be used in this paper. The syntax and operational semantics of qCCS are presented in Section 3. First, we define inductively quantum processes and at the same time free quantum variables associated with each process. Then the notion of configuration is introduced in which free quantum variables are instantiated by the accompanied quantum context. The operational semantics of qCCS is given in terms of probabilistic labeled transition system consisting of configurations. To show the expressive power of qCCS, we describe the well-known quantum teleportation protocol with qCCS and show that it indeed teleports any qubit from one party to another. Finally, ordinary one-step transitions are extended to combined multi-step transitions by probabilistically taking different transitions at each intermediate step.

Section 4 and Section 5 are the main parts of the present paper. We define the notions of strong and weak probabilistic bisimulations between configurations and then lift them to bisimulations between quantum processes. Some properties of these two bisimulations are also derived. Particularly, we show that probabilistic bisimilarity is the largest probabilistic bisimulation on Con; a weak version of the congruence property is proved in which bisimilarity of P and Q implies bisimilarity of $P\|R$ and $Q\|R$ for any quantum process R, if either P and Q are free of quantum input or R is free of unitary transformation and quantum measurement. An example is also presented to show why the standard proof technique for establishing the preservation of bisimilarity under parallel combinator in classical CCS cannot be used to prove the result in general quantum case

when the (non-commutative) quantum operations performed by parallel processes can be interweaved, although it works well in the two special cases mentioned above.

Section 6 is the concluding section in which we outline the main results and point out some problems for further study.

2. Preliminaries

For convenience of the reader, we briefly recall some basic notions from linear algebra and quantum theory which are needed in the sequel. We refer to [24] for more details.

2.1. *Basic linear algebra*

A Hilbert space $\mathcal{H}$ is a vector space equipped with an inner product which in turn is a mapping $\langle\cdot|\cdot\rangle : \mathcal{H} \times \mathcal{H} \to \mathbf{C}$ satisfying the following properties:

(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) $\langle\phi|\sum_i \lambda_i|\psi_i\rangle = \sum_i \lambda_i\langle\phi|\psi_i\rangle$,

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

Let $\mathcal{L}(\mathcal{H})$ be the set of linear operators on $\mathcal{H}$. For any $A \in \mathcal{L}(\mathcal{H})$, we have the following definitions:

(1) A non-zero vector $|\psi\rangle \in \mathcal{H}$ is an eigenvector of A with the corresponding eigenvalue $\lambda \in \mathbf{C}$ if $A|\psi\rangle = \lambda|\psi\rangle$. We write $spec(A)$ for the set of eigenvalues of A, and call it the spectrum of A.
(2) 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 spectrum theorem states that the set of all normalized eigenvectors of a Hermitian operator in $\mathcal{L}(\mathcal{H})$ contains an orthonormal basis for $\mathcal{H}$. That is, there exists a so-called spectral decomposition for each Hermitian A such that

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

where the set $\{|i\rangle\}$ constitute an orthonormal basis of $\mathcal{H}$, and $P_i = \sum_{j:A|j\rangle=\lambda_i|j\rangle} |j\rangle\langle j|$ is the projector to the corresponding eigenspace of λ_i.
(3) A is positive if $\langle\psi|A|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$; it is positive-definite if for any nonzero vector $|\psi\rangle$, $\langle\psi|A|\psi\rangle > 0$. Note that a positive operator is also Hermitian.
(4) A is unitary if $A^\dagger A = AA^\dagger = I_{\mathcal{H}}$ where $I_{\mathcal{H}}$ is the identity operator in $\mathcal{L}(\mathcal{H})$. In the examples of this paper, we will use some well-known unitary operators listed as follows: the $CNOT$ operator performed on two qubits such that

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

and the 1-qubit Hadamard operator H and Pauli operators $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ defined respectively as

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(5) 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 trace function is actually independent of the orthonormal basis selected. It is also easy to check that trace function is linear and $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for any operators $A, B \in \mathcal{L}(\mathcal{H})$.

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces of dimensions n_1 and n_2, respectively. Then their tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ is defined as an $n_1 n_2$-dimensional vector space consisting of linear combinations of the vectors $|\psi_1\psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$. Here the tensor product of two vectors is defined by a new vector such that

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

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

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

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

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

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

A linear operator $\mathcal{E}$ on $\mathcal{L}(\mathcal{H})$ is completely positive if it maps positive operators in $\mathcal{L}(\mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H})$, and for any auxiliary Hilbert space $\mathcal{H}'$, the trivially extended operator $\mathcal{I}_{\mathcal{H}'} \otimes \mathcal{E}$ also maps positive operators in $\mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$. Here $\mathcal{I}_{\mathcal{H}'}$ is the identity operator on $\mathcal{L}(\mathcal{H}')$. The elegant and powerful Kraus representation theorem [18] of completely positive operators states that a linear operator

$\mathcal{E}$ is completely positive if and only if there are some set of operators $\{E_i, i = 1, \ldots, d\}$ with appropriate dimension such that

$$\mathcal{E}(A) = \sum_{i=1}^{d} E_i A E_i^\dagger$$

for any $A \in \mathcal{L}(\mathcal{H})$. The operators E_i are called Kraus operators of $\mathcal{E}$. A linear operator is said to be a super-operator if it is completely positive and trace-preserving. Here an operator $\mathcal{E}$ is trace-preserving if $\mathrm{tr}(\mathcal{E}(A)) = \mathrm{tr}(A)$ for any linear operator A. Then a super-operator is just a completely positive operator with its Kraus operators E_i satisfying $\sum_i E_i^\dagger E_i = I$.

2.2. *Basic quantum mechanics*

According to von Neumann's formalism of quantum mechanics [34], an isolated physical system is associated with a (finite-dimensional) Hilbert space which is called the state space of the system. A pure state of a quantum system is a normalized vector in its state space, and a mixed state is represented by a density operator. Here a density operator ρ on Hilbert space $\mathcal{H}$ is a positive linear operator such that $\mathrm{tr}(\rho) = 1$. Another equivalent representation of density operator is probabilistic ensemble of pure states. In particular, given an ensemble $\{(p_i, |\psi_i\rangle)\}$ where $p_i \geq 0$, $\sum_i p_i = 1$, and $|\psi_i\rangle$ are pure states, $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ is a density operator. Conversely, each density operator can be generated by an ensemble of pure states in this way. In this paper, we denote by $\mathcal{D}(\mathcal{H})$ the set of density operators on Hilbert space $\mathcal{H}$.

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 particular, if ρ_1 and ρ_2 are pure states $|\psi_1\rangle$ and $|\psi_2\rangle$, respectively, then we have $|\psi_2\rangle = U|\psi_1\rangle$.

Observation of a quantum system is a quantum measurement represented by a Hermitian operator M on the associated state space. Suppose M has the spectral decomposition $M = \sum_m mP_m$, where P_m is the projector onto the eigenspace of M associated with eigenvalue m. Then the probability of obtaining measurement result m when the system is initially in the state ρ is $p_m = \mathrm{tr}(P_m\rho)$, and if $p_m > 0$ then the post-measurement state of the system given the outcome m becomes

$$\frac{P_m \rho P_m}{p_m}.$$

For the case that ρ is a pure state $|\psi\rangle$, we have $p_m = \langle\psi|P_m|\psi\rangle$, and the post-measurement state is $P_m|\psi\rangle/\sqrt{p_m}$.

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

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

in 2-qubit system. This kind of states is called entangled states. To see the weirdness of entanglement, suppose a measurement $M = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$ is applied on the first qubit of the EPR state. 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 a way. This is an outstanding feature of quantum mechanics which has no counterpart in classical world, and is the key to many quantum information processing tasks such as teleportation [3] and superdense coding [4].

2.3. *Quantum no-cloning theorem*

Classical information can be arbitrarily cloned. However, the linearity of quantum operations prohibits the possibility of perfectly cloning an unknown quantum state [35]. The formal argument goes as follows. Suppose a quantum cloning device is possible, *i.e.* there is a physically realizable procedure such that the transformation

$$|\psi\rangle|\Sigma\rangle \longrightarrow |\psi\rangle|\psi\rangle \tag{1}$$

holds for any $|\psi\rangle \in \mathcal{H}$. Here $|\Sigma\rangle$ is a standard state which is independent of $|\psi\rangle$. In particular, for two orthogonal states $|0\rangle$ and $|1\rangle$, we have

$$|0\rangle|\Sigma\rangle \longrightarrow |0\rangle|0\rangle \qquad \text{and} \qquad |1\rangle|\Sigma\rangle \longrightarrow |1\rangle|1\rangle.$$

Now let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Because of the linearity of quantum operations imposed by basic principles of quantum mechanics, we have

$$|\psi\rangle|\Sigma\rangle = \alpha|0\rangle|\Sigma\rangle + \beta|1\rangle|\Sigma\rangle \longrightarrow \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle. \tag{2}$$

On the other hand, Eq.(1) can be rewritten as

$$|\psi\rangle|\Sigma\rangle \longrightarrow \alpha^2|0\rangle|0\rangle + \beta^2|1\rangle|1\rangle + \alpha\beta(|0\rangle|1\rangle + |1\rangle|0\rangle). \tag{3}$$

Comparing the right-hand sides of Eq.(2) and Eq.(3), we deduce that $\alpha = 0$ or $\beta = 0$. That is, the universal cloning procedure presented in Eq.(1) does not exist. This is the well-known quantum no-cloning theorem.

Quantum no-cloning theorem has been shown to be connected with some other no-go principles such as no-signaling principle which states that signals can not be sent faster than the speed of light [6,11]. No-cloning theorem was also used to argue for the security of quantum cryptography [2]. In the scenario of communication, because unknown quantum states can not be perfectly cloned, transferring of quantum datum must be done by sending the physical system which carries the information, unless the datum to be transmitted is already known to the sender. This is in sharp contrast with the case in classical world where to send an unknown datum, one need only produce a copy of it and then transmit the copy. The sender needs not know the classical datum since perfect cloning is always possible.

3. Basic Definitions of qCCS

In this section, we give the basic definitions of qCCS. Subsections 3.1 and 3.2 are devoted to the syntax and the operational semantics, respectively. In subsection 3.3, we extend ordinary one-step transitions to combined multi-step transitions.

3.1. *Syntax*

For the sake of simplicity, we consider only two types of data: the set of real numbers Real for classical data, and the set of qubits Qbt for quantum data. We denote by $cVar$ (ranged over by $x, y, \ldots$) and $qVar$ (ranged over by $q, r, \ldots$) the set of classical variables on Real and quantum variables on Qbt, respectively. The set of expressions with the value domain Real is denoted by Exp and ranged over by e. 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 $\mathsf{c}, \mathsf{d}, \ldots$. Let $Chan = cChan \cup qChan$. A relabeling function f is a one to one function from $Chan$ to $Chan$ such that $f(cChan) \subseteq cChan$ and $f(qChan) \subseteq qChan$.

From these notations, we now propose the syntax of qCCS as follows. For simplicity, we often abbreviate the indexed set $\{q_1, \ldots, q_n\}$ to $\bar{q}$ when $q_1, \ldots, q_n$ are distinct quantum variables and the dimension n is understood.

Definition 1 *(quantum process)* The set of quantum processes $qProc$ and the free quantum variable function $qv : qProc \to 2^{qVar}$ are defined inductively by the following formation rules:

(1) $\mathbf{nil} \in qProc$, and $qv(\mathbf{nil}) = \emptyset$;
(2) $c?x.P \in qProc$, and $qv(c?x.P) = qv(P)$;
(3) $c!e.P \in qProc$, and $qv(c!e.P) = qv(P)$;
(4) $\mathsf{c}?q.P \in qProc$, and $qv(\mathsf{c}?q.P) = qv(P) - \{q\}$;
(5) If $q \notin qv(P)$ then $\mathsf{c}!q.P \in qProc$, and $qv(\mathsf{c}!q.P) = qv(P) \cup \{q\}$;
(6) $U[\bar{q}].P \in qProc$, and $qv(U[\bar{q}].P) = qv(P) \cup \bar{q}$;
(7) $M[\bar{q}; x].P \in qProc$, and $qv(M[\bar{q}; x].P) = qv(P) \cup \bar{q}$;
(8) $P + Q \in qProc$, and $qv(P + Q) = qv(P) \cup qv(Q)$;
(9) If $qv(P) \cap qv(Q) = \emptyset$ then $P \| Q \in qProc$, and $qv(P \| Q) = qv(P) \cup qv(Q)$;
(10) $P[f] \in qProc$, and $qv(P[f]) = qv(P)$;
(11) $P \backslash L \in qProc$, and $qv(P \backslash L) = qv(P)$;
(12) $\mathbf{if}\ b\ \mathbf{then}\ P \in qProc$, and $qv(\mathbf{if}\ b\ \mathbf{then}\ P) = qv(P)$,

where $P, Q \in qProc$, $c \in cChan$, $x, y \in cVar$, $\mathsf{c} \in qChan$, $q, q_1, \ldots, q_n \in qVar$, $e \in Exp$, f is a relabeling function, $L \subseteq Chan$, b is a boolean-valued expression, U is a unitary operator, and M is a Hermitian operator.

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. $U[\bar{q}]$ denotes the action of performing a unitary transformation U on the qubits $\bar{q}$ while $M[\bar{q}; x]$ measures the qubits $\bar{q}$ according to M and stores the measurement outcome into the classical variable x. $+$ models nondeterministic choice: $P + Q$ behaves like either P or Q depending on the choice of the environment. $\|$ denotes the usual parallel composition. The operators $\backslash L$ and $[f]$ model restriction and relabeling, respectively: $P \backslash L$ behaves like P as long as any action through the channels

in L is forbidden, and $P[f]$ behaves like P where each channel name is replaced by its image under the relabeling function f. Finally, **if** b **then** P is the standard conditional choice where P can be executed only if b is true.

For any quantum process P, $qv(P)$ is exactly the set of quantum variables which P can reference. Note that in the process $\mathsf{c}!q.P$, the assumption $q \notin qv(P)$ guarantees that a quantum system will not be referenced after it has been output. This is a requirement of quantum no-cloning theorem. For the same reason, we assume $q_1, \ldots, q_n$ distinct in $U[\bar{q}].P$ and $M[\bar{q}; x].P$ (Recall that the notation $\bar{q}$ implies that $q_1, \ldots, q_n$ are distinct). Furthermore, since we intend to use parallel combinator $\|$ to model separate parties which can perform actions locally on their own systems and communicate with each other through channels, the assumption $qv(P) \cap qv(Q) = \emptyset$ guarantees that P and Q will never reference a quantum system simultaneously.

The notion of free classical variables in quantum processes can be defined in the usual way with a unique modification that quantum measurement $M[\bar{q}; x]$ has binding power on x. A quantum process P is closed if it contains no free classical variables, *i.e.*, $fv(P) = \emptyset$.

3.2. *Operational semantics of qCCS*

To present the operational semantics of qCCS, we first introduce the notion of configuration. Note that for any $P \in qProc$ with $fv(P) \subseteq \{x_1, \ldots, x_n\}$ and any indexed set $\bar{v} = \{v_1, \ldots, v_n\}$ of real values, the process $P[\bar{v}/\bar{x}]$ obtained by instantiating classical variables $\bar{x}$ with $\bar{v}$ is closed. The following definition introduces a corresponding instantiation for free quantum variables. Similar notions were also presented in [16] and [10] in a somewhat different way.

Definition 2 *(Configuration) For any closed quantum process P, if $qv(P) \subseteq \bar{q}$ then a pair of the form*

$$< P; \bar{q} = \rho > \tag{4}$$

is called a configuration, where ρ is a density operator in 2^n-dimensional Hilbert space and n is the length of $\bar{q}$. The set of configurations is denoted by Con and ranged over by $\mathcal{C}, \mathcal{D}, \ldots$. In the configuration $\mathcal{C} =< P; \bar{q} = \rho >$, '$\bar{q} = \rho$' is called the quantum context of $\mathcal{C}$ and denoted $Context(\mathcal{C})$.

Intuitively, quantum context describes the 'quantum environment' in which a process lives. All of the quantum systems which a process can reference must be included in the accompanied quantum context.

Let $D(Con)$ be the set of finite-support probability distributions over Con, *i.e.*

$$D(Con) = \{\mu : Con \to [0,1] \mid \mu(\mathcal{C}) > 0 \text{ for finitely many } \mathcal{C}, \text{ and } \sum_{\mu(\mathcal{C})>0} \mu(\mathcal{C}) = 1\}.$$

For any $\mu \in D(Con)$, we denote by $supp(\mu)$ the support set of μ, *i.e.* the set of configurations $\mathcal{C}$ such that $\mu(\mathcal{C}) > 0$. When μ is a simple distribution such that $supp(\mu) = \{\mathcal{C}\}$ for some $\mathcal{C}$, we abuse the notation slightly to denote μ by $\mathcal{C}$. Just as in [16] and [10], sometimes we find it convenient to denote a distribution $\mu \in D(Con)$ by an explicit form $\mu = \boxplus_{i \in I} p_i \bullet \mathcal{C}_i$ (or $\mu = \boxplus p_i \bullet \mathcal{C}_i$ when the index set I is understood) where $supp(\mu) = \{\mathcal{C}_i \mid i \in I\}$ and $\mu(\mathcal{C}_i) = p_i$ for each $i \in I$. Given $\mu_1, \ldots, \mu_n \in D(Con)$ and $p_1, \ldots, p_n \in (0,1]$, $\sum_i p_i = 1$, we define the combined distribution, denoted by $\sum_{i=1}^n p_i \mu_i$,

to be a new distribution $\mu \in D(Con)$ such that for any $\mathcal{D} \in supp(\mu)$, $\mu(\mathcal{D}) = \sum_i p_i \mu_i(\mathcal{D})$. It is obvious that $supp(\sum_i p_i \mu_i) = \bigcup_i supp(\mu_i)$.

As usual, the operational semantics of qCCS is given in terms of probabilistic labeled transition system. Let

$$Act = \{c?v, c!v \mid c \in cChan, v \in \mathsf{Real}\}$$
$$\cup \{\mathsf{c}?r, \mathsf{c}?r : \rho, \mathsf{c}!r \mid \mathsf{c} \in qChan, r \in qVar, \rho \in \mathcal{D}(\mathcal{H}_2)\} \ \cup \ \{\tau\}$$

where τ is the silent action, and $\mathcal{D}(\mathcal{H}_2)$ is the set of density operators on a 2-dimensional Hilbert space. Then the semantics of qCCS is given by the probabilistic labeled transition system $(Con, Act, \rightarrow)$, where $\rightarrow \subseteq Con \times Act \times D(Con)$ is the smallest relation satisfying the rules defined in Definitions 3.3 through 3.13. (For brevity, we write $\mathcal{C} \stackrel{\alpha}{\rightarrow} \mu$ instead of $(\mathcal{C}, \alpha, \mu) \in \rightarrow$).

Definition 3 (Classical rules)

$$\textbf{C-Inp}: \ \frac{}{< c?x.P; C > \stackrel{c?v}{\rightarrow} < P[v/x]; C >} \quad \text{for all } v \in \mathsf{Real}$$

$$\textbf{C-Outp}: \ \frac{}{< c!e.P; C > \stackrel{c!v}{\rightarrow} < P; C >} \quad \text{where } v \text{ is the value of } e$$

$$\textbf{C-Com}: \ \frac{< P_1; C > \stackrel{c?v}{\rightarrow} < P_1'; C >, \quad < P_2; C > \stackrel{c!v}{\rightarrow} < P_2'; C >}{< P_1 \| P_2; C > \stackrel{\tau}{\rightarrow} < P_1' \| P_2'; C >}$$

$$\frac{< P_1; C > \stackrel{c!v}{\rightarrow} < P_1'; C >, \quad < P_2; C > \stackrel{c?v}{\rightarrow} < P_2'; C >}{< P_1 \| P_2; C > \stackrel{\tau}{\rightarrow} < P_1' \| P_2'; C >}$$

These three rules describe the passing of classical messages; they are almost the same as in classical value-passing CCS. Contexts remain untouched in these rules since they include only the accompanied *quantum* systems, which will not be changed by *classical* input and output. Other classical rules are incorporated into Definitions 3.9 through 3.13 below.

Definition 4 (Quantum-input rules)

$$\textbf{Q-Inp1}: \ \frac{}{< \mathsf{c}?q.P; \bar{q} = \rho > \stackrel{\mathsf{c}?r:\sigma}{\rightarrow} < P[r/q]; r, \bar{q} = \sigma \otimes \rho >} \quad \text{where } r \notin \bar{q} \text{ and } \sigma \in \mathcal{D}(\mathcal{H}_2)$$

$$\textbf{Q-Inp2}: \ \frac{}{< \mathsf{c}?q.P; \bar{q} = \rho > \stackrel{\mathsf{c}?r}{\rightarrow} < P[r/q]; \bar{q} = \rho >} \quad \text{where } r \in \bar{q} - qv(\mathsf{c}?q.P)$$

In [16], only a rule similar to the first one was presented for quantum input. This rule makes sense when the input system (denoted by the quantum variable r) is initially not correlated (neither entangled nor classically correlated) with the quantum systems in $\bar{q}$. However, one of the essential features which distinguish quantum mechanics from classical mechanics is that different systems can lie in an entangled state which can not

be determined by the reduced states of individual systems. This argument leads naturally to the following inference rule:

$$< \mathsf{c}?q.P; \bar{q} = \rho > \stackrel{\mathsf{c}?r:\rho'}{\rightarrow} < P[r/q]; r, \bar{q} = \sigma > \quad \text{where } r \notin \bar{q},\ \mathrm{tr}_{\bar{q}}\sigma = \rho',\ \text{and } \mathrm{tr}_r\sigma = \rho.$$

Any quantum input can be characterized by this rule since no constraints are made on the new state σ except $\mathrm{tr}_r\sigma = \rho$ which means that the state of initial systems remains untouched. This rule is, however, also problematic. First, it is not image-finite in the sense that from the source configuration $< \mathsf{c}?q.P; \bar{q} = \rho >$ and the action $\mathsf{c}?r : \rho'$, there are infinitely many derived configurations which satisfy the rule. Second, in general the effect of this transition on the accompanied context is not a super-operator independent of ρ. This will make some proofs in Sections 4 and 5 infeasible.

In consideration of the above arguments, we present rules **Q-Inp1** and **Q-Inp2** which describe the input of a qubit from the outside and the inside of the context, respectively. Note that the context is kept untouched in rule **Q-Inp2**. The intuition behind is that when the system to be input has already been described in the context, the input action is merely a declaration that the process can reference this system, which of course does not change the state of the whole system.

Definition 5 Q-Outp (Quantum-output rule)

$$\frac{}{< \mathsf{c}!q.P; \bar{q} = \rho > \stackrel{\mathsf{c}!q}{\rightarrow} < P; \bar{q} = \rho >}$$

The quantum output rule presented in [16] was of the following form (rewritten with our notations):

$$< \mathsf{c}!q.P; \bar{q} = \rho > \stackrel{\mathsf{c}!q}{\rightarrow} < P; \bar{q} - \{q\} = \mathrm{tr}_q\rho >$$

with the intuition that we do not care about the state of a quantum system when it has been output. The information about how the output system is correlated with the systems remained in the context is, however, totally lost; problems will arise if we input again the system which was just output. The **Q-Outp** rule presented above can deal with this problem since the quantum context remains unchanged so that any information is kept.

Definition 6 Unit (Unitary transformation rule)

$$\frac{}{< U[\bar{r}].P; \bar{q} = \rho > \stackrel{\tau}{\rightarrow} < P; \bar{q} = U_{\bar{r}}\rho U_{\bar{r}}^{\dagger} >}$$

where $U_{\bar{r}}\rho U_{\bar{r}}^{\dagger}$ denotes the application of unitary transformation U on the system consisting of $\bar{r}$. To be specific, let $length(\bar{r}) = k$ and $length(\bar{q}) = n$. Then $U_{\bar{r}} = \Pi_{\bar{r}}^{\dagger}(U \otimes I^{\otimes(n-k)})\Pi_{\bar{r}}$ where $\Pi_{\bar{r}}$ is a permutation which places $r_1, \ldots, r_k$ at the head of $\bar{q}$, and I is the identity transformation. Similar notations were also introduced in [16].

In our framework of qCCS, performing a unitary transformation is modeled by a τ-action which is unobservable from outside. The same treatment is applied to measurement on quantum systems.

Definition 7 Meas (Measurement rule)

$$\frac{}{< M[\bar{r}; x].P; \bar{q} = \rho > \stackrel{\tau}{\rightarrow} \boxplus_{i\in I} p_i \bullet < P[\lambda_i/x]; \bar{q} = P_{i,\bar{r}}\rho P_{i,\bar{r}}/p_i >}$$

where M is a Hermitian operator with the spectral decomposition $M = \sum_{i\in I} \lambda_i P_i$, $P_{i,\bar{r}}$ denotes the projection P_i performed on the system consisting of $\bar{r}$, *i.e.*, $P_{i,\bar{r}} = \Pi_{\bar{r}}^{\dagger}(P_i \otimes I^{\otimes(n-k)})\Pi_{\bar{r}}$, and $p_i = \mathrm{tr}(P_{i,\bar{r}}\rho)$.

Definition 8 Q-Com (Quantum-communication rule)

$$\frac{< P_1; C > \stackrel{\mathsf{c}?r}{\rightarrow} < P_1'; C >, \quad < P_2; C > \stackrel{\mathsf{c}!r}{\rightarrow} < P_2'; C >}{< P_1 \| P_2; C > \stackrel{\tau}{\rightarrow} < P_1' \| P_2'; C >}$$

$$\frac{< P_1; C > \stackrel{\mathsf{c}!r}{\rightarrow} < P_1'; C >, \quad < P_2; C > \stackrel{\mathsf{c}?r}{\rightarrow} < P_2'; C >}{< P_1 \| P_2; C > \stackrel{\tau}{\rightarrow} < P_1' \| P_2'; C >}$$

It may be surprising at first glance that there is no communication rule in which the participating action of either parallel process is of the form $\mathsf{c}?r : \rho$. In other words, quantum input from outside the accompanied context cannot lead to quantum communication. The reason is as follows. To make $< P_1 \| P_2; C >$ a valid configuration, the context C must involve all the free quantum variables occur in P_1 and P_2. As a consequence, any qubit which will be input by P_1 or P_2 during the quantum communication between them is from the context C.

Definition 9 (Interleaving rules)

$$\textbf{Inp-Int}: \frac{< P_1; C > \stackrel{\mathsf{c}?r}{\rightarrow} < P_1'; C' >}{< P_1 \| P_2; C > \stackrel{\mathsf{c}?r}{\rightarrow} < P_1' \| P_2; C' >} \quad \text{where } r \notin qv(P_2)$$

$$\frac{< P_2; C > \stackrel{\mathsf{c}?r}{\rightarrow} < P_2'; C' >}{< P_1 \| P_2; C > \stackrel{\mathsf{c}?r}{\rightarrow} < P_1 \| P_2'; C' >} \quad \text{where } r \notin qv(P_1)$$

$$\textbf{Oth-Int}: \frac{< P_1; C > \stackrel{\alpha}{\rightarrow} \boxplus p_i \bullet < P_1^i; C_i >}{< P_1 \| P_2; C > \stackrel{\alpha}{\rightarrow} \boxplus p_i \bullet < P_1^i \| P_2; C_i >} \quad \text{where } \alpha \text{ is not of the form } \mathsf{c}?r$$

$$\frac{< P_2; C > \stackrel{\alpha}{\rightarrow} \boxplus p_i \bullet < P_2^i; C_i >}{< P_1 \| P_2; C > \stackrel{\alpha}{\rightarrow} \boxplus p_i \bullet < P_1 \| P_2^i; C_i >} \quad \text{where } \alpha \text{ is not of the form } \mathsf{c}?r$$

The side conditions $r \notin qv(P_2)$ and $r \notin qv(P_1)$ in **Inp-Int** rules are presented to exclude the possibility that one process inputs a qubit which is referencing by another parallel process. Other interleaving rules, including those dealing with quantum output and classical actions, are incorporated into **Oth-Int** rules.

The following rules are similar to their classical counterparts.

Definition 10 Sum (Summation rule)

$$\frac{< P; C > \stackrel{\alpha}{\rightarrow} \mu}{< P + Q; C > \stackrel{\alpha}{\rightarrow} \mu}, \qquad \frac{< Q; C > \stackrel{\alpha}{\rightarrow} \mu}{< P + Q; C > \stackrel{\alpha}{\rightarrow} \mu}$$

Definition 11 Rel (Relabeling rule)

$$\frac{< P; C > \xrightarrow{\alpha} \boxplus p_i \bullet < P_i; C_i >}{< P[f]; C > \xrightarrow{\alpha[f]} \boxplus p_i \bullet < P_i[f]; C_i >}$$

Here we extend the definition of relabeling function to actions and quantum processes in an obvious way.

Definition 12 Res (Restriction rule)

$$\frac{< P; C > \xrightarrow{\alpha} \boxplus p_i \bullet < P_i; C_i >}{< P \backslash L; C > \xrightarrow{\alpha} \boxplus p_i \bullet < P_i \backslash L; C_i >} \text{ where } cn(\alpha) \notin L$$

Here the function cn returns the channel name used by an action.

Definition 13 Cho (Choice rule)

$$\frac{< P; C > \xrightarrow{\alpha} \mu}{< \textbf{if } b \textbf{ then } P; C > \xrightarrow{\alpha} \mu} \text{ where } b \text{ is true}$$

When b is false then the configuration $< \textbf{if } b \textbf{ then } P; C >$ cannot perform any action.

The following lemma can be easily observed from the inference rules defined above.

Lemma 14 *Suppose* $< P; \bar{q} = \rho > \xrightarrow{\alpha} \mu$ *where* $\rho \in \mathcal{D}(\mathcal{H})$. *Then*

(1) if $\alpha = \mathsf{c}?r : \sigma$ *for some* $\mathsf{c} \in qChan$, $r \notin \bar{q}$, *and* $\sigma \in \mathcal{D}(\mathcal{H}_2)$, *then there exists* $P' \in qProc$ *such that for any* $\rho' \in \mathcal{D}(\mathcal{H})$, $< P; \bar{q} = \rho' > \xrightarrow{\alpha} < P'; r, \bar{q} = \sigma \otimes \rho' >$,

(2) if α *is not of the form* $\mathsf{c}?r : \sigma$, *then there exist an index set* I, *a set of quantum processes* $\{P_i : i \in I\}$, *and a set of super-operators* $\{\mathcal{E}_i : i \in I\}$ *which only act nontrivially on* $\mathcal{L}(\mathcal{H}_{qv(P)})$ *such that for any* $\rho' \in \mathcal{D}(\mathcal{H})$, $< P; \bar{q} = \rho' > \xrightarrow{\alpha} \boxplus_{i \in I} p_i \bullet < P_i; \bar{q} = \mathcal{E}_i(\rho') >$. *Here* $\mathcal{H}_{qv(P)}$ *denotes the associated Hilbert space of the quantum systems in* $qv(P)$.

Proof. Obvious. □

The transition graph of a configuration is defined as usual where each transition $\mathcal{C} \xrightarrow{\alpha} \boxplus_{i=1}^{n} p_i \bullet \mathcal{C}_i$ is depicted as and each transition of the form $\mathcal{C} \xrightarrow{\alpha} \mathcal{D}$ is simply depicted as

Example 15 We now present a simple example to show the expressive power of our qCCS. This example is concerned with quantum teleportation [3], a famous protocol in quantum information theory which can make use of an entangled state shared between the sender and the receiver to teleport an unknown quantum state by sending only classical information. This example was also considered in [16] and [10].

Let M be a 2-qubit measurement such that $M = \sum_{i=0}^{3} \lambda_i |\tilde{i}\rangle\langle\tilde{i}|$, where $\tilde{i}$ is the binary expansion of i. Let $CNOT$, H, and $\sigma_i,\ i = 0, \ldots, 3$ be as defined in Section 2. Then the participating quantum processes in teleportation protocol are defined as follows:

$$\begin{aligned} Alice &:= CNot[q, q_1].H[q].M[q, q_1; x].c!x.\textbf{nil}, \\ Bob &:= c?x.U_x[q_2].\textbf{nil}, \\ Telep &:= (Alice \| Bob) \backslash \{c\}, \end{aligned}$$

where

Fig. 1. Quantum teleportation.

$$U_x[q_2].\mathbf{nil} := \mathbf{if}\ x=\lambda_0\ \mathbf{then}\ \sigma_0[q_2].\mathbf{nil}\ +\ \mathbf{if}\ x=\lambda_1\ \mathbf{then}\ \sigma_1[q_2].\mathbf{nil}\ +$$
$$\mathbf{if}\ x=\lambda_2\ \mathbf{then}\ \sigma_3[q_2].\mathbf{nil}\ +\ \mathbf{if}\ x=\lambda_3\ \mathbf{then}\ \sigma_2[q_2].\mathbf{nil}.$$

The transition graph of the configuration

$$< Telep; \bar{q} = [(\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)] >$$

is shown in Fig.1 where $\bar{q}$ is the abbreviation of the indexed set $\{q, q_1, q_2\}$, and for any pure state $|\psi\rangle$, $[|\psi\rangle]$ is the abbreviation of $|\psi\rangle\langle\psi|$. Note that in the whole procedure, Alice holds the qubits q and q_1 while Bob holds q_2. So the process $Telep$ indeed teleports the quantum state $\alpha|0\rangle + \beta|1\rangle$ from Alice's side to Bob's side with the aid of an EPR state. □

3.3. *Combined transitions*

There are two kinds of nondeterminism in qCCS: non-probabilistic nondeterminism caused by summation combinator '+' and probabilistic nondeterminism caused by quantum measurements. To define probabilistic bisimulations between quantum processes, we need a way to resolve the first kind of nondeterminism numerically. This is achieved in [19,20] by treating non-probabilistic nondeterminism as equiprobability. In this paper however, motivated by [29] and [30], we adopt a more flexible way of allowing combining different nondeterministic choices in any probabilistic way. To achieve this goal, a notion of adversary is introduced. With the help of adversaries, we extend ordinary transitions to combined transitions (resp. combined weak transitions) which is the basis of strong probabilistic bisimulation (resp. weak probabilistic bisimulation) defined later. Some definitions in this subsection are motivated by or borrowed directly from [29] and [30] where classical probabilistic processes were considered.

Definition 16 *An execution fragment $f = \mathcal{C}_0\alpha_1\mathcal{C}_1\ldots\alpha_n\mathcal{C}_n$ is a finite sequence of alternating configurations and actions starting and ending with configurations, such that for each $i = 0, \ldots, n-1$, there exists a transition $\mathcal{C}_i \stackrel{\alpha_{i+1}}{\rightarrow} \mu_{i+1}$ with $\mu_{i+1}(\mathcal{C}_{i+1}) > 0$. We call n the length of f, and denote by $head(f)$ and $tail(f)$ the first and the last configurations of f , respectively.*

The set of all execution fragments is denoted by $frag$. For any $f \in frag$, we let $Pre(f)$ be the set of execution fragments which are prefixes of f.

Definition 17 *An adversary $\mathcal{A}$ is a function from execution fragments to finite-support distributions over transitions, i.e.*

$$\mathcal{A}\ :\ frag\ \rightarrow\ D(\rightarrow),$$

such that for any $f \in frag$, if $\mathcal{A}(f) = \boxplus_{i\in I} p_i \bullet (\mathcal{C}_i, \alpha_i, \mu_i)$ then $\mathcal{C}_i = tail(f)$ for any $i \in I$.

Intuitively, an adversary provides a mechanism to resolve nondeterminism probabilistically by deciding next transition based on the execution history.

Definition 18 *Suppose $f = \mathcal{C}_0\alpha_1\mathcal{C}_1\ldots\alpha_n\mathcal{C}_n$ is an execution fragment and $\mathcal{A}$ is an adversary. We say that f coincides with $\mathcal{A}$ if for any $i = 0, \ldots, n-1$, $\mathcal{A}(\mathcal{C}_0\alpha_1\mathcal{C}_1\ldots\alpha_i\mathcal{C}_i) = \boxplus_{j\in J} p_j \bullet (\mathcal{C}_i, \beta_j, \mu_j)$ such that the set $J_i = \{j \in J \mid \beta_j = \alpha_{i+1}$ and $\mu_j(\mathcal{C}_{i+1}) > 0\}$ is nonempty.*

We denote by $P^i_{\mathcal{A}}(f) = \sum_{j\in J_i} p_j\mu_j(\mathcal{C}_{i+1})$ *the probability of the* i*-th choice in* f *according to the adversary* $\mathcal{A}$.

For any adversary $\mathcal{A}$, let $F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}}$ be the set of execution fragments with head $\mathcal{C}$ and tail $\mathcal{D}$ which coincide with $\mathcal{A}$. If $f = \mathcal{C}_0\alpha_1\mathcal{C}_1\ldots\alpha_n\mathcal{C}_n \in F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}}$, then we denote by

$$P_{\mathcal{A}}(f) = \prod_{i=0}^{n-1} P^i_{\mathcal{A}}(f)$$

the probability of the execution fragment f according to $\mathcal{A}$. When f does not coincide with $\mathcal{A}$, we simply let $P_{\mathcal{A}}(f) = 0$.

With the above definitions, we are now ready to define the notions of combined transitions.

Definition 19 *For any* $\mathcal{C} \in Con$, $s = \alpha_1\ldots\alpha_n \in Act^*$, *and* $\mu \in D(Con)$, *we say that* $\mathcal{C}$ *can evolve into* μ *by a combined (resp. a combined weak)* s*-transition, denoted by* $\mathcal{C} \xrightarrow{s}_C \mu$ *(resp.* $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu$*), if there exists an adversary* $\mathcal{A}$ *such that for any* $\mathcal{D} \in supp(\mu)$,

(1) $\sum_{f\in F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}}} P_{\mathcal{A}}(f) = \mu(\mathcal{D})$,

(2) for any $f = \mathcal{C}_0\beta_1\mathcal{C}_1\ldots\beta_m\mathcal{C}_m \in F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}}$, *the string* $\beta_1\ldots\beta_m = s$ *(resp.* $\beta_1\ldots\beta_m$ *has the form* $\tau^*\alpha_1\tau^*\ldots\tau^*\alpha_n\tau^*$*).*

In the following, we prove two lemmas which are useful for the next sections. The first lemma shows that any convex combination of combined s-transitions is also a combined s-transition.

Lemma 20 *For any* $\mu_1,\ldots,\mu_n \in D(Con)$ *and* $p_1,\ldots,p_n \in (0,1)$ *such that* $\mathcal{C} \xrightarrow{s}_C \mu_i$ *(resp.* $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu_i$*) and* $\sum_i p_i = 1$, *we have* $\mathcal{C} \xrightarrow{s}_C \mu$ *(resp.* $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu$*) for* $\mu = \sum_i p_i\mu_i$.

Proof. We only prove the result for combined weak transitions in the case of $n = 2$. The general case can be proved similarly by induction.

Suppose an adversary corresponding to $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu_i$ is $\mathcal{A}_i$, $i = 1, 2$. We construct a new adversary $\mathcal{A}$, which will be proven to be a corresponding adversary of $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu$, as follows. For any $f \in frag$,

$$\mathcal{A}(f) = \begin{cases} \frac{pP_{\mathcal{A}_1}(f)}{P_{\mathcal{A}}(f)}\mathcal{A}_1(f) + (1 - \frac{pP_{\mathcal{A}_1}(f)}{P_{\mathcal{A}}(f)})\mathcal{A}_2(f) & \text{if } P_{\mathcal{A}}(f) \neq 0, \\ p\mathcal{A}_1(f) + (1-p)\mathcal{A}_2(f) & \text{otherwise.} \end{cases} \tag{5}$$

Note that $P_{\mathcal{A}}(\mathcal{C}) = 1$ for any adversary $\mathcal{A}$ and any $\mathcal{C} \in Con$, and $P_{\mathcal{A}}(f)$ is dependent only on the set $\{\mathcal{A}(f') \mid f' \in Pre(f),\ f' \neq f\}$. The definition Eq.(5) is meaningful and is an inductive one. Now we show that for any $f \in frag$ with $head(f) = \mathcal{C}$,

$$P_{\mathcal{A}}(f) = pP_{\mathcal{A}_1}(f) + (1-p)P_{\mathcal{A}_2}(f) \tag{6}$$

by induction on the structure of f.

When $f = \mathcal{C}$, we have

$$P_{\mathcal{A}}(\mathcal{C}) = 1 = p + (1-p) = pP_{\mathcal{A}_1}(\mathcal{C}) + (1-p)P_{\mathcal{A}_2}(\mathcal{C}).$$

Now suppose Eq.(6) holds for $f = \mathcal{C}\alpha_1\mathcal{C}_1\ldots\alpha_n\mathcal{C}_n$. Then for $f' = \mathcal{C}\alpha_1\mathcal{C}_1\ldots\alpha_{n+1}\mathcal{C}_{n+1}$, there are two cases to consider.

(i) $P_{\mathcal{A}}(f) = 0$. Then from Eq.(6) we also find that $P_{\mathcal{A}_1}(f) = P_{\mathcal{A}_2}(f) = 0$. So we have $P_{\mathcal{A}}(f') = P_{\mathcal{A}_1}(f') = P_{\mathcal{A}_2}(f') = 0$, and Eq.(6) holds trivially for f'.

(ii) $P_{\mathcal{A}}(f) \neq 0$. In this case, we derive that

$$\begin{aligned}
P_{\mathcal{A}}(f') &= P_{\mathcal{A}}(f)P^n_{\mathcal{A}}(f') && \text{Definition}\\
&= P_{\mathcal{A}}(f)\left[\frac{pP_{\mathcal{A}_1}(f)}{P_{\mathcal{A}}(f)}P^n_{\mathcal{A}_1}(f') + (1-\frac{pP_{\mathcal{A}_1}(f)}{P_{\mathcal{A}}(f)})P^n_{\mathcal{A}_2}(f')\right] && \text{Eq.(5)}\\
&= pP_{\mathcal{A}_1}(f)P^n_{\mathcal{A}_1}(f') + (P_{\mathcal{A}}(f) - pP_{\mathcal{A}_1}(f))P^n_{\mathcal{A}_2}(f')\\
&= pP_{\mathcal{A}_1}(f)P^n_{\mathcal{A}_1}(f') + (1-p)P_{\mathcal{A}_2}(f)P^n_{\mathcal{A}_2}(f') && \text{Eq.(6)}\\
&= pP_{\mathcal{A}_1}(f') + (1-p)P_{\mathcal{A}_2}(f'). && \text{Definition}
\end{aligned}$$

So for any $\mathcal{D} \in supp(\mu)$,

$$\begin{aligned}
\sum_{f\in F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}}} P_{\mathcal{A}}(f) &= \sum_{f\in F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}}} [pP_{\mathcal{A}_1}(f) + (1-p)P_{\mathcal{A}_2}(f)]\\
&= p\sum_{f\in F^{\mathcal{A}_1}_{\mathcal{C}\to\mathcal{D}}} P_{\mathcal{A}_1}(f) + (1-p)\sum_{f\in F^{\mathcal{A}_2}_{\mathcal{C}\to\mathcal{D}}} P_{\mathcal{A}_2}(f)\\
&= p\mu_1(\mathcal{D}) + (1-p)\mu_2(\mathcal{D})\\
&= \mu(\mathcal{D}).
\end{aligned}$$

Here for the second equality, we have used the fact

$$F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}} = F^{\mathcal{A}_1}_{\mathcal{C}\to\mathcal{D}} \cup F^{\mathcal{A}_2}_{\mathcal{C}\to\mathcal{D}} \tag{7}$$

which is direct from Eq.(6) and the observation that $f \in F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}}$ if and only if $P_{\mathcal{A}}(f) > 0$.

Furthermore, from Eq.(7) we deduce that for each $f = \mathcal{C}_0\beta_1\mathcal{C}_1\ldots\beta_m\mathcal{C}_m \in F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}}$, the string $\beta_1\ldots\beta_m$ has the form $\tau^*\alpha_1\tau^*\ldots\tau^*\alpha_n\tau^*$ since any execution fragment in $F^{\mathcal{A}_1}_{\mathcal{C}\to\mathcal{D}}$ and $F^{\mathcal{A}_2}_{\mathcal{C}\to\mathcal{D}}$ does. □

Lemma 21 *Suppose $\mathcal{C} \xrightarrow{s}_C \mu$ (resp. $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu$), $s = \alpha_1\ldots\alpha_n \in Act^*$, and $\mathcal{A}$ is a corresponding adversary. Let $\mathcal{A}(\mathcal{C}) = \uplus_{i\in I} p_i \bullet (\mathcal{C}, \beta_i, \mu_i)$. Then for any $i \in I$,*

(1) $\beta_i = \alpha_1$ (resp. $\beta_i = \tau$ or α_1),

(2) for any $\mathcal{C}' \in supp(\mu_i)$, there exist $\mu_{\mathcal{C}'}$ and s' such that $\mathcal{C}' \xrightarrow{s'}_C \mu_{\mathcal{C}'}$ (resp. $\mathcal{C}' \stackrel{s'}{\Rightarrow}_C \mu_{\mathcal{C}'}$) and $\beta_i s' = s$ (resp. $\widehat{\beta_i s'} = \widehat{s}$. Here for any $s \in Act^*$, $\widehat{s}$ denotes the string obtained from s by deleting all the occurrences of τ),

(3) $\mu = \sum_{i\in I}\sum_{\mathcal{C}'\in supp(\mu_i)} p_i\mu_i(\mathcal{C}')\mu_{\mathcal{C}'}$.

Proof. We only prove the result for combined weak transitions. (1) is obvious. To prove (2), for any $\mathcal{C}' \in supp(\mu_i)$, let

$$J_{\mathcal{C}'} = \{j \in I \mid \beta_j = \beta_i \text{ and } \mu_j(\mathcal{C}') > 0\},$$

$r_{\mathcal{C}'} = \sum_{j\in J_{\mathcal{C}'}} p_j\mu_j(\mathcal{C}')$, and $\mu_{\mathcal{C}'} \in D(Con)$ such that for any $\mathcal{D} \in Con$,

$$\mu_{\mathcal{C}'}(\mathcal{D}) = \frac{1}{r_{\mathcal{C}'}}\sum\{|\ P_{\mathcal{A}}(f) \mid f \in F^{\mathcal{A}}_{\mathcal{C}\to\mathcal{D}} \text{ and } \mathcal{C}\beta_i\mathcal{C}' \in Pre(f)\ |\}.$$

Here $\{|\ldots|\}$ stands for the multi-set brackets. Let $s' = s$ or $\alpha_2\ldots\alpha_n$ depending on whether $\beta_i = \tau$ or α_1. Then $\widehat{\beta_i s'} = \widehat{s}$ as required. We now prove $\mathcal{C}' \stackrel{s'}{\Rightarrow}_C \mu_{\mathcal{C}'}$ by constructing a corresponding adversary $\mathcal{A}_{\mathcal{C}'}$ as follows. For any $f \in frag$, let

$$\mathcal{A}_{\mathcal{C}'}(f) = \begin{cases} \mathcal{A}(\mathcal{C}\beta_i f) & \text{if } head(f) = \mathcal{C}', \\ \mathcal{A}(f) & \text{otherwise.} \end{cases}$$

Then when $head(f) = \mathcal{C}'$, we have $P_{\mathcal{A}}(\mathcal{C}\beta_i f) = r_{\mathcal{C}'} P_{\mathcal{A}_{\mathcal{C}'}}(f)$. Thus for any $\mathcal{D} \in supp(\mu_{\mathcal{C}'})$,

$$\begin{aligned} \sum_{f \in F^{\mathcal{A}_{\mathcal{C}'}}_{\mathcal{C}' \to \mathcal{D}}} P_{\mathcal{A}_{\mathcal{C}'}}(f) &= \frac{1}{r_{\mathcal{C}'}} \sum_{f \in F^{\mathcal{A}_{\mathcal{C}'}}_{\mathcal{C}' \to \mathcal{D}}} P_{\mathcal{A}}(\mathcal{C}\beta_i f) \\ &= \frac{1}{r_{\mathcal{C}'}} \sum \{\mid P_{\mathcal{A}}(f') \mid f' \in F^{\mathcal{A}}_{\mathcal{C} \to \mathcal{D}} \text{ and } \mathcal{C}\beta_i\mathcal{C}' \in Pre(f') \mid\} \\ &= \mu_{\mathcal{C}'}(\mathcal{D}). \end{aligned}$$

Finally, to prove (3), we need only to check that for any $\mathcal{D} \in Con$,

$$\begin{aligned} \mu(\mathcal{D}) &= \sum_{f \in F^{\mathcal{A}}_{\mathcal{C} \to \mathcal{D}}} P_{\mathcal{A}}(f) \\ &= \sum_{\mathcal{C}' \in \cup_i supp(\mu_i)} \sum_{i \in I_{\mathcal{C}'}} \sum \{\mid P_{\mathcal{A}}(f) \mid f \in F^{\mathcal{A}}_{\mathcal{C} \to \mathcal{D}} \text{ and } \mathcal{C}\beta_i\mathcal{C}' \in Pre(f) \mid\} \\ &= \sum_{\mathcal{C}' \in \cup_i supp(\mu_i)} \sum_{i \in I_{\mathcal{C}'}} r_{\mathcal{C}'} \mu_{\mathcal{C}'}(\mathcal{D}) \\ &= \sum_{\mathcal{C}' \in \cup_i supp(\mu_i)} \sum_{i \in I_{\mathcal{C}'}} \sum_{j \in J_{\mathcal{C}'}} p_j \mu_j(\mathcal{C}') \mu_{\mathcal{C}'}(\mathcal{D}) \\ &= \sum_{j \in I} \sum_{\mathcal{C}' \in supp(\mu_j)} p_j \mu_j(\mathcal{C}') \mu_{\mathcal{C}'}(\mathcal{D}) \end{aligned}$$

where $I_{\mathcal{C}'} = \{i \in I : \mu_i(\mathcal{C}') > 0\}$. □

To illustrate the definitions and lemmas in this subsection, we present a simple example as follows.

Example 22 Suppose $M_{0,1} = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$ is a one-qubit measurement according to the computational basis, H is the Hadarmard transformation, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Let

$$P = M_{0,1}[q; x].H[q].\mathsf{c}!q.\mathbf{nil} + \mathsf{c}!q.\mathbf{nil}$$

be a quantum process which can either perform sequentially the measurement M and the transformation H on q before outputing q, or output q directly. Now consider the configuration

$$\mathcal{C} =< P; q = |+\rangle\langle +| > .$$

The transition graph of $\mathcal{C}$ can be depicted as where

$$\begin{aligned} &\mathcal{C}_1 =< H[q].\mathsf{c}!q.\mathbf{nil}; q = |0\rangle\langle 0| >, \quad \mathcal{C}_2 =< H[q].\mathsf{c}!q.\mathbf{nil}; q = |1\rangle\langle 1| >, \\ &\mathcal{C}_3 =< \mathsf{c}!q.\mathbf{nil}; q = |+\rangle\langle +| >, \qquad \mathcal{C}_4 =< \mathsf{c}!q.\mathbf{nil}; q = |-\rangle\langle -| >, \\ &\mathcal{C}_5 =< \mathbf{nil}; q = |+\rangle\langle +| >, \qquad \mathcal{C}_6 =< \mathbf{nil}; q = |-\rangle\langle -| > . \end{aligned}$$

Then by taking an adversary $\mathcal{A}_1$ such that

$$\mathcal{A}_1(\mathcal{C}) = (\mathcal{C}, \tau, \frac{1}{2} \bullet \mathcal{C}_1 \boxplus \frac{1}{2} \bullet \mathcal{C}_2), \qquad \mathcal{A}_1(\mathcal{C}\tau\mathcal{C}_1) = (\mathcal{C}_1, \tau, \mathcal{C}_3),$$
$$\mathcal{A}_1(\mathcal{C}\tau\mathcal{C}_2) = (\mathcal{C}_2, \tau, \mathcal{C}_4), \qquad \mathcal{A}_1(\mathcal{C}\tau\mathcal{C}_1\tau\mathcal{C}_3) = (\mathcal{C}_3, \mathsf{c}!q, \mathcal{C}_5),$$

and

$$\mathcal{A}_1(\mathcal{C}\tau\mathcal{C}_2\tau\mathcal{C}_4) = (\mathcal{C}_4, \mathsf{c}!q, \mathcal{C}_6),$$

we have the combined (weak) transitions

$$\mathcal{C} \stackrel{\tau\tau\mathsf{c}!q}{\rightarrow}_C \frac{1}{2} \bullet \mathcal{C}_5 \boxplus \frac{1}{2} \bullet \mathcal{C}_6 \qquad \text{and} \qquad \mathcal{C} \stackrel{\mathsf{c}!q}{\Rightarrow}_C \frac{1}{2} \bullet \mathcal{C}_5 \boxplus \frac{1}{2} \bullet \mathcal{C}_6.$$

On the other hand, the adversary $\mathcal{A}_2$ satisfying $\mathcal{A}_2(\mathcal{C}) = (\mathcal{C}, \mathsf{c}!q, \mathcal{C}_5)$ leads to the combined weak transition $\mathcal{C} \stackrel{\mathsf{c}!q}{\Rightarrow}_C \mathcal{C}_5$. Thus for any $p \in [0, 1]$, we have

$$\mathcal{C} \stackrel{\mathsf{c}!q}{\Rightarrow}_C (1 - \frac{p}{2}) \bullet \mathcal{C}_5 \boxplus \frac{p}{2} \bullet \mathcal{C}_6$$

by combining the above two weak $\mathsf{c}!q$-transitions. The corresponding adversary $\mathcal{A}$ is constructed as

$$\mathcal{A}(\mathcal{C}) = p\mathcal{A}_1(\mathcal{C}) + (1-p)\mathcal{A}_2(\mathcal{C}) = p \bullet (\mathcal{C}, \tau, \frac{1}{2} \bullet \mathcal{C}_1 \boxplus \frac{1}{2} \bullet \mathcal{C}_2) \boxplus (1-p) \bullet (\mathcal{C}, \mathsf{c}!q, \mathcal{C}_5),$$
$$\mathcal{A}(\mathcal{C}\tau\mathcal{C}_1) = \mathcal{A}_1(\mathcal{C}\tau\mathcal{C}_1) = (\mathcal{C}_1, \tau, \mathcal{C}_3), \quad \cdots.$$

□

4. Strong probabilistic bisimulation between quantum processes

This section is devoted to the notion of strong probabilistic bisimulation between quantum processes and its properties such as congruence under various combinators.

Given an equivalence relation $\mathcal{R} \subseteq Con \times Con$, two distributions μ and ν on Con are said to be equivalent under $\mathcal{R}$, denoted by $\mu \equiv_{\mathcal{R}} \nu$, if for any equivalence class $M \in Con/\mathcal{R}$ it holds $\mu(M) = \nu(M)$. Two quantum contexts $\bar{q} = \rho$ and $\bar{r} = \sigma$ are equal if there exists a permutation Π such that $\Pi(\bar{q}) = \bar{r}$ and at the same time $\Pi\rho\Pi^\dagger = \sigma$. We denote $\mathcal{C} \stackrel{\alpha}{\not\rightarrow}$ if there exists no $\mu \in D(Con)$ such that $\mathcal{C} \stackrel{\alpha}{\rightarrow} \mu$; we simply write $\mathcal{C} \not\rightarrow$ if $\mathcal{C} \stackrel{\alpha}{\not\rightarrow}$ for all $\alpha \in Act$.

Definition 23 *An equivalence relation $\mathcal{R} \subseteq Con \times Con$ is a strong probabilistic bisimulation if for any $\mathcal{C}, \mathcal{D} \in Con$, $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$ implies that*

(1) whenever $\mathcal{C} \stackrel{\alpha}{\rightarrow} \mu$ for some α and μ, there exists ν such that $\mathcal{D} \stackrel{\alpha}{\rightarrow}_C \nu$ and $\mu \equiv_{\mathcal{R}} \nu$,

(2) if $\mathcal{C} \not\rightarrow$, then $Contex(\mathcal{C}) = Contex(\mathcal{D})$.

As mentioned in Section 1, one of the purposes of qCCS is to provide a theoretical framework to describe quantum concurrent systems such as quantum cryptographic protocols. As a consequence, not only the observable actions but also the quantum operations such as unitary transformations and measurements performed by processes must be taken into consideration when bisimulation relations are investigated. For example, we cannot in any sense regard a quantum process which can merely sequentially perform 5 τ actions and then terminates as bisimilar to the teleportation process $Telep$ defined in

Example 3.1. Furthermore, because of the possible entanglement between different quantum systems, the effect of quantum operations can be fully reflected only by state change of the whole quantum context. This is the reason why we need clause (2) in Definition 23. The clause (1) is originated from [21] and [29].

Definition 24 *(1) Two configurations $\mathcal{C}$ and $\mathcal{D}$ are strongly bisimilar, denoted by $\mathcal{C} \sim_c \mathcal{D}$, if there is a strong probabilistic bisimulation $\mathcal{R}$ such that $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$.*

(2) Two processes P and Q are strongly bisimilar, denoted by $P \sim_p Q$, if for any context C and any indexed set $\bar{v}$ of values, $< P[\bar{v}/\bar{x}]; C > \sim_c < Q[\bar{v}/\bar{x}]; C >$. Here $\bar{x}$ is the set of free classical variables contained in processes P and Q.

We usually omit the subscripts of $\sim_c$ and $\sim_p$ when no confusion arises.

The difference between our notion of probabilistic bisimulation and the probabilistic branching bisimulation defined in [19,20] can be best illustrated by the following example.

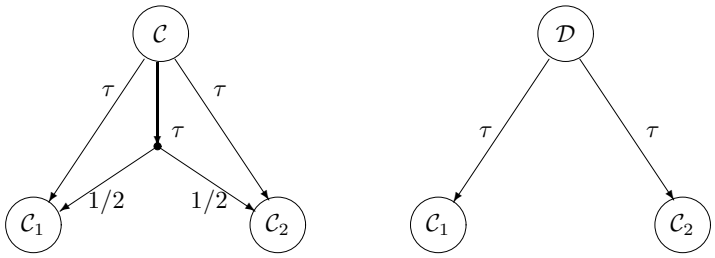
Example 25 Suppose $M_{0,1}$, H, and $|+\rangle$ are given as in Example 22, and $U = \sigma_1 H$. Suppose

$$\mathcal{C} =< H[q].\mathbf{nil} + U[q].\mathbf{nil} + M_{0,1}[q; x].\mathbf{nil}; q = |+\rangle\langle+| >$$

and

$$\mathcal{D} =< H[q].\mathbf{nil} + U[q].\mathbf{nil}; q = |+\rangle\langle+| >$$

with transition graphs depicted as



where

$$\mathcal{C}_1 =< \mathbf{nil}; q = |0\rangle\langle 0| > \quad \text{and} \quad \mathcal{C}_2 =< \mathbf{nil}; q = |1\rangle\langle 1| > .$$

Then $\mathcal{C}$ and $\mathcal{D}$ are bisimilar in our notion of strong probabilistic bisimulation, since $\mathcal{D}$ can simulate the action $M_{0,1}[q; x]$ of $\mathcal{C}$ by choosing its actions $H[q]$ and $U[q]$ with respective probabilities one half.

Note that in the sense of probabilistic branching bisimulation presented in [19,20], the configurations $\mathcal{C}$ and $\mathcal{D}$ are also bisimilar. But the reason is that state change of contexts caused by quantum operations is not considered there. As a consequence, the configurations $\mathcal{C}_1$ and $\mathcal{C}_2$, which are not bisimilar in our sense of bisimulation, are treated to be bisimilar in [19,20]. □

In the following, we derive some properties of strong probabilistic bisimulation. The proofs are similar to but much simpler than those of the corresponding results for weak probabilistic bisimulation in the next section except for Theorem 28 (2), so we omit them here.

Theorem 26 *$\sim$ is the largest strong probabilistic bisimulation on Con.*

Theorem 27 *For any $\mathcal{C}, \mathcal{D} \in Con$, $\mathcal{C} \sim \mathcal{D}$ if and only if for any $s \in Act^*$,*

(1) whenever $\mathcal{C} \stackrel{s}{\rightarrow}_C \mu$ for some μ, then there exists ν such that $\mathcal{D} \stackrel{s}{\rightarrow}_C \nu$ and $\mu \equiv_\sim \nu$,

(2) whenever $\mathcal{D} \stackrel{s}{\rightarrow}_C \nu$ for some ν, then there exists μ such that $\mathcal{C} \stackrel{s}{\rightarrow}_C \mu$ and $\mu \equiv_\sim \nu$,

(3) if $\mathcal{C} \not\rightarrow$ and $\mathcal{D} \not\rightarrow$, then $Contex(\mathcal{C}) = Contex(\mathcal{D})$.

Theorem 28 *If $P \sim Q$ then*

(1) $a.P \sim a.Q$, for any $a \in \{c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, U[\bar{q}], M[\bar{q}; x]\}$;

(2) $P + R \sim Q + R$ for any R;

(3) $P \| R \sim Q \| R$ provided that R is free of unitary transformation and measurement, or P and Q are free of quantum input;

(4) $P[f] \sim Q[f]$, for any relabeling function f;

*(5) **if** b **then** $P \sim$ **if** b **then** Q, for any boolean expression b.*

Proof. The cases other than (2) are simpler than the counterparts for weak probabilistic bisimulation. In the following, we prove (2) by showing a stronger result: for any contexts C and D, if $< P_i[\bar{v}/\bar{x}]; C > \sim < Q_i[\bar{v}/\bar{x}]; D >$ for $i = 1, 2$, then $< P_1[\bar{v}/\bar{x}] + P_2[\bar{v}/\bar{x}]; C > \sim < Q_1[\bar{v}/\bar{x}] + Q_2[\bar{v}/\bar{x}]; D >$. Here $\bar{x}$ is the set of free classical variables contained in processes P_i and Q_i.

Suppose $< P_1[\bar{v}/\bar{x}] + P_2[\bar{v}/\bar{x}]; C > \stackrel{\alpha}{\rightarrow} \mu$ for some α and μ. Then from **Sum** rule, we have $< P_1[\bar{v}/\bar{x}]; C > \stackrel{\alpha}{\rightarrow} \mu$ or $< P_2[\bar{v}/\bar{x}]; C > \stackrel{\alpha}{\rightarrow} \mu$. By the assumption $< P_i[\bar{v}/\bar{x}]; C > \sim < Q_i[\bar{v}/\bar{x}]; D >$ and Theorem 27, it holds that $< Q_1[\bar{v}/\bar{x}]; D > \stackrel{\alpha}{\rightarrow}_C \nu$ or $< Q_2[\bar{v}/\bar{x}]; D > \stackrel{\alpha}{\rightarrow}_C \nu$ for some ν such that $\mu \equiv_\sim \nu$. In either case, using **Sum** rule again, we have $< Q_1[\bar{v}/\bar{x}] + Q_2[\bar{v}/\bar{x}]; D > \stackrel{\alpha}{\rightarrow}_C \nu$.

Similarly, if $< Q_1[\bar{v}/\bar{x}] + Q_2[\bar{v}/\bar{x}]; D > \stackrel{\alpha}{\rightarrow} \nu$ for some α and ν, we can also find a μ such that $< P_1[\bar{v}/\bar{x}] + P_2[\bar{v}/\bar{x}]; C > \stackrel{\alpha}{\rightarrow}_C \mu$ and $\mu \equiv_\sim \nu$.

Finally, if $< P_1[\bar{v}/\bar{x}] + P_2[\bar{v}/\bar{x}]; C > \not\rightarrow$ and $< Q_1[\bar{v}/\bar{x}] + Q_2[\bar{v}/\bar{x}]; D > \not\rightarrow$, then we have $< P_1[\bar{v}/\bar{x}]; C > \not\rightarrow$ and $< Q_1[\bar{v}/\bar{x}; D] > \not\rightarrow$. Hence $C = D$ from the assumption that $< P_1[\bar{v}/\bar{x}]; C > \sim < Q_1[\bar{v}/\bar{x}]; D >$. Then the result follows from Theorem 27. □

Theorem 29 *For any $P, Q, R \in qProc$,*

*(1) $P +$ **nil** $\sim P$,*

(2) $P + P \sim P$,

(3) $P + Q \sim Q + P$,

(4) $P + (Q + R) \sim (P + Q) + R$,

(5) $P \| \mathbf{nil} \sim P$,

(6) $P \| Q \sim Q \| P$,

(7) $P \| (Q \| R) \sim (P \| Q) \| R$.

5. Weak probabilistic bisimulation between quantum processes

As in classical CCS, the notion of weak probabilistic bisimulation which abstracts from unobservable internal actions is more useful in implementation and verification. In this section, based on the notion of combined weak transition introduced in Section 3.3, we present weak probabilistic bisimulation for our qCCS.

Definition 30 *An equivalence relation $\mathcal{R} \subseteq Con \times Con$ is a weak probabilistic bisimulation if for any $\mathcal{C}, \mathcal{D} \in Con$, $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$ implies that*

(1) whenever $\mathcal{C} \stackrel{\alpha}{\rightarrow} \mu$ for some α and μ, there exists ν such that $\mathcal{D} \stackrel{\widehat{\alpha}}{\Rightarrow}_C \nu$ and $\mu \equiv_{\mathcal{R}} \nu$,

(2) if $\mathcal{C} \not\rightarrow$ and $\mathcal{D} \not\rightarrow$, then $Contex(\mathcal{C}) = Contex(\mathcal{D})$.

The following lemma shows that the ordinary transition in clause (1) of the above definition can be strengthened to combined weak transition.

Lemma 31 *Let $\mathcal{R} \subseteq Con \times Con$ be a weak probabilistic bisimulation and $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$. Then for any $s \in Act^*$, if $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu$, then $\mathcal{D} \stackrel{\widehat{s}}{\Rightarrow}_C \nu$ for some ν such that $\mu \equiv_{\mathcal{R}} \nu$.*

Proof. Let $\mathcal{A}$ be an adversary corresponding to $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu$. Since there are no recursive constructs in qCCS, we can prove this lemma by induction on the maximal length h of the execution fragments in $\cup_{\mathcal{D} \in supp(\mu)} F^{\mathcal{A}}_{\mathcal{C} \to \mathcal{D}}$.

If $h = 0$, then s is the empty string and $\mu = \mathcal{C}$. In this case, we need only to take $\nu = \mathcal{D}$.

Suppose the result holds for $h \leq n$. We now prove that it also holds for $h = n + 1$. Let $\mathcal{A}(\mathcal{C}) = \uplus_{i \in I} p_i \bullet (\mathcal{C}, \alpha_i, \mu_i)$. Then for each $i \in I$ we have $\mathcal{C} \stackrel{\alpha_i}{\to} \mu_i$, and so there exists ν_i such that $\mathcal{D} \stackrel{\widehat{\alpha_i}}{\Rightarrow}_C \nu_i$ and $\mu_i \equiv_{\mathcal{R}} \nu_i$. Furthermore, from Lemma 21, for any $\mathcal{C}' \in supp(\mu_i)$ there exist $\mu_{\mathcal{C}'}$ and s' such that $\mathcal{C}' \stackrel{s'}{\Rightarrow}_C \mu_{\mathcal{C}'}$, $\widehat{\alpha_i s'} = \widehat{s}$, and

$$\mu = \sum_{i \in I} \sum_{\mathcal{C}' \in supp(\mu_i)} p_i \mu_i(\mathcal{C}') \mu_{\mathcal{C}'}.$$

Now take arbitrarily $\mathcal{D}' \in supp(\nu_i)$. Let $[\mathcal{D}']_{\mathcal{R}}$ denote the equivalence class of $\mathcal{R}$ in which $\mathcal{D}'$ lies. Then $supp(\mu_i) \cap [\mathcal{D}']_{\mathcal{R}} \neq \emptyset$ from $\mu_i \equiv_{\mathcal{R}} \nu_i$. For any $\mathcal{C}' \in supp(\mu_i) \cap [\mathcal{D}']_{\mathcal{R}}$, we can choose an adversary $\mathcal{A}_{\mathcal{C}'}$ corresponding to $\mathcal{C}' \stackrel{s'}{\Rightarrow}_C \mu_{\mathcal{C}'}$ such that the maximal length of the execution fragments in $\cup_{\mathcal{D} \in supp(\mu_{\mathcal{C}'})} F^{\mathcal{A}_{\mathcal{C}'}}_{\mathcal{C}' \to \mathcal{D}}$ is less than $n + 1$. So by induction we have $\mathcal{D}' \stackrel{\widehat{s'}}{\Rightarrow}_C \nu^{\mathcal{C}'}_{\mathcal{D}'}$ for some $\nu^{\mathcal{C}'}_{\mathcal{D}'}$, and $\mu_{\mathcal{C}'} \equiv_{\mathcal{R}} \nu^{\mathcal{C}'}_{\mathcal{D}'}$. From Lemma 20 it holds $\mathcal{D}' \stackrel{\widehat{s'}}{\Rightarrow}_C \nu_{\mathcal{D}'}$ where

$$\nu_{\mathcal{D}'} = \sum_{\mathcal{C}' \in supp(\mu_i) \cap [\mathcal{D}']_{\mathcal{R}}} \frac{\mu_i(\mathcal{C}')}{\mu_i(supp(\mu_i) \cap [\mathcal{D}']_{\mathcal{R}})} \nu^{\mathcal{C}'}_{\mathcal{D}'}.$$

It is now direct to check that $\mathcal{D} \stackrel{\widehat{s}}{\Rightarrow}_C \nu$ for

$$\nu = \sum_{i \in I} \sum_{\mathcal{D}' \in supp(\nu_i)} p_i \nu_i(\mathcal{D}') \nu_{\mathcal{D}'}.$$

Finally, we show that $\mu \equiv_{\mathcal{R}} \nu$. For any $M \in Con/\mathcal{R}$,

$$\begin{aligned}
\nu(M) &= \sum_{i \in I} \sum_{\mathcal{D}' \in supp(\nu_i)} p_i \nu_i(\mathcal{D}') \nu_{\mathcal{D}'}(M) \\
&= \sum_{i \in I} \sum_{\mathcal{D}' \in supp(\nu_i)} p_i \nu_i(\mathcal{D}') \sum_{\mathcal{C}' \in supp(\mu_i) \cap [\mathcal{D}']_{\mathcal{R}}} \frac{\mu_i(\mathcal{C}')}{\mu_i(supp(\mu_i) \cap [\mathcal{D}']_{\mathcal{R}})} \nu^{\mathcal{C}'}_{\mathcal{D}'}(M) \\
&= \sum_{i \in I} \sum_{\mathcal{C}' \in supp(\mu_i)} p_i \mu_i(\mathcal{C}') \mu_{\mathcal{C}'}(M) \sum_{\mathcal{D}' \in supp(\nu_i) \cap [\mathcal{C}']_{\mathcal{R}}} \frac{\nu_i(\mathcal{D}')}{\mu_i(supp(\mu_i) \cap [\mathcal{C}']_{\mathcal{R}})} \\
&= \sum_{i \in I} \sum_{\mathcal{C}' \in supp(\mu_i)} p_i \mu_i(\mathcal{C}') \mu_{\mathcal{C}'}(M) \frac{\nu_i([\mathcal{C}']_{\mathcal{R}})}{\mu_i([\mathcal{C}']_{\mathcal{R}})} \\
&= \sum_{i \in I} \sum_{\mathcal{C}' \in supp(\mu_i)} p_i \mu_i(\mathcal{C}') \mu_{\mathcal{C}'}(M)
\end{aligned}$$

$= \mu(M)$.

Here the third equality is due to the fact that $\mu_{\mathcal{C}'} \equiv_{\mathcal{R}} \nu_{\mathcal{D}'}^{\mathcal{C}'}$ for any $\mathcal{D}' \in supp(\nu_i)$ and $\mathcal{C}' \in supp(\mu_i) \cap [\mathcal{D}']_{\mathcal{R}}$; the fifth equality holds because $\mu_i \equiv_{\mathcal{R}} \nu_i$ for any $i \in I$. □

Lemma 32 *Let $\mathcal{R} \subseteq Con \times Con$ be a weak probabilistic bisimulation and $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$.*

(1) If $\mathcal{C} \not\rightarrow$ then $\mathcal{D} \stackrel{\alpha}{\not\rightarrow}$ for any $\alpha \in Act - \{\tau\}$.

(2) For any $s \in Act^*$, if $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu$ such that $\mathcal{C}' \not\rightarrow$ for some $\mathcal{C}' \in supp(\mu)$, then there exists ν such that $\mathcal{D} \stackrel{\widehat{s}}{\Rightarrow}_C \nu$ and $\mathcal{D}' \not\rightarrow$ for some $\mathcal{D}' \in supp(\nu)$. Furthermore, $Contex(\mathcal{C}') = Context(\mathcal{D}')$.

Proof. (1) is easy. To prove (2), from $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu$ we first find some ν_1 such that $\mathcal{D} \stackrel{\widehat{s}}{\Rightarrow}_C \nu_1$ and $\mu \equiv_{\mathcal{R}} \nu_1$. If there exists a $\mathcal{D}_1 \in supp(\nu_1) \cap [\mathcal{C}']_{\mathcal{R}}$ such that $\mathcal{D}_1 \not\rightarrow$ then we are done. Otherwise, for any $\mathcal{D}_1 \in supp(\nu_1) \cap [\mathcal{C}']_{\mathcal{R}}$, from $\mathcal{C}' \not\rightarrow$ and (1) we have $\mathcal{D}_1 \stackrel{\tau}{\rightarrow} \nu_2$ for some ν_2 such that $\mathcal{C}'\mathcal{R}\mathcal{D}_2$ for any $\mathcal{D}_2 \in supp(\nu_2)$. Then we check if there exists a $\mathcal{D}_2 \in supp(\nu_2)$ such that $\mathcal{D}_2 \not\rightarrow$. Note that the quantum processes we consider in this paper are all finitely derivable. It follows that we will finally find a distribution ν such that $\mathcal{D} \stackrel{\widehat{s}}{\Rightarrow}_C \nu$ and there exists some $\mathcal{D}' \in supp(\nu)$ satisfying $\mathcal{C}'\mathcal{R}\mathcal{D}'$ and $\mathcal{D}' \not\rightarrow$. Furthermore, from Definition 30 (2) we have $Context(\mathcal{C}') = Context(\mathcal{D}')$. □

Since the union of equivalence relations is not necessarily an equivalence relation, the union of weak probabilistic bisimulations is not necessarily a weak probabilistic bisimulation either. Nevertheless, we can prove that the reflexive and transitive closure of the union of weak probabilistic bisimulations is also a weak probabilistic bisimulation.

Theorem 33 *If $\mathcal{R}_i, i \in I$, is a collection of weak probabilistic bisimulations on Con, then their reflexive and transitive closure $(\cup_i \mathcal{R}_i)^*$ is also a weak probabilistic bisimulation.*

Proof. By definition, $\mathcal{R}_i$ is symmetric for any $i \in I$. So $(\cup_i \mathcal{R}_i)^*$ is also symmetric and hence an equivalence relation. Now suppose $(\mathcal{C}, \mathcal{D}) \in (\cup_i \mathcal{R}_i)^*$. Then there exist an integer n and a series of configurations $\mathcal{C}_0, \ldots, \mathcal{C}_n$ such that $\mathcal{C}_0 = \mathcal{C}$, $\mathcal{C}_n = \mathcal{D}$, and $(\mathcal{C}_i, \mathcal{C}_{i+1}) \in \mathcal{R}_{k_i}$ for some $k_i \in I$, $i = 0, \ldots, n-1$. There are two cases we should consider:

(i) $\mathcal{C} \stackrel{\alpha}{\rightarrow} \mu_0$ for some α and μ_0. Then from $\mathcal{C}\mathcal{R}_{k_0}\mathcal{C}_1$, there exists μ_1 such that $\mathcal{C}_1 \stackrel{\widehat{\alpha}}{\Rightarrow}_C \mu_1$ and $\mu_0(M_0) = \mu_1(M_0)$ for any $M_0 \in Con/\mathcal{R}_{k_0}$. Furthermore, from $\mathcal{C}_1\mathcal{R}_{k_1}\mathcal{C}_2$ and Lemma 31, we have $\mathcal{C}_2 \stackrel{\widehat{\alpha}}{\Rightarrow}_C \mu_2$ for some μ_2, and $\mu_1(M_1) = \mu_2(M_1)$ for any $M_1 \in Con/\mathcal{R}_{k_1}$. In this way, we can derive that $\mathcal{C}_{i+1} \stackrel{\widehat{\alpha}}{\Rightarrow}_C \mu_{i+1}$ for some μ_{i+1} such that $\mu_i(M_i) = \mu_{i+1}(M_i)$ for any $M_i \in Con/\mathcal{R}_{k_i}$, $i = 0, \ldots, n-1$. Now suppose $M \in Con/(\cup_i \mathcal{R}_i)^*$. Notice that for any $i = 0, \ldots, n-1$, M is the disjoint union of some equivalence classes of $Con/\mathcal{R}_{k_i}$ since $\mathcal{R}_{k_i} \subseteq (\cup_i \mathcal{R}_i)^*$. It follows that $\mu_i(M) = \mu_{i+1}(M)$ for any $i = 0, \ldots, n-1$. Thus we have $\mu_0(M) = \mu_n(M)$.

(ii) $\mathcal{C} \not\rightarrow$ and $\mathcal{D} \not\rightarrow$. Then from $\mathcal{C}\mathcal{R}_{k_0}\mathcal{C}_1$ and Lemma 32 we have $\mathcal{C}_1 \stackrel{\widehat{\tau}}{\Rightarrow}_C \mu_1$, and there exists some $\mathcal{D}_1 \in supp(\mu_1)$ such that $\mathcal{D}_1 \not\rightarrow$ and $Contex(\mathcal{C}) = Context(\mathcal{D}_1)$. Similarly, for any $i = 2, \ldots, n$ we can derive that $\mathcal{C}_i \stackrel{\widehat{\tau}}{\Rightarrow}_C \mu_i$, and there exists some $\mathcal{D}_i \in supp(\mu_i)$ such that $\mathcal{D}_i \not\rightarrow$ and $Contex(\mathcal{D}_{i-1}) = Context(\mathcal{D}_i)$. Finally, from the fact $\mathcal{D} \not\rightarrow$, it is the only case that $\mathcal{D}_n = \mathcal{D}$ and so $Context(\mathcal{D}) = Context(\mathcal{D}_{n-1}) = \ldots = Context(\mathcal{C})$.

From (i) and (ii), we know that $(\cup_i \mathcal{R}_i)^*$ is also a weak probabilistic bisimulation. □

Definition 34 *(1) Two configurations $\mathcal{C}$ and $\mathcal{D}$ are weakly bisimilar, denoted by $\mathcal{C} \approx_c \mathcal{D}$, if there is a weak probabilistic bisimulation $\mathcal{R}$ such that $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$.*

(2) Two quantum processes P and Q are weakly bisimilar, denoted by $P \approx_p Q$, if for any context C and any indexed set $\bar{v}$ of values, $< P[\bar{v}/\bar{x}]; C > \approx_c < Q[\bar{v}/\bar{x}]; C >$. Here $\bar{x}$ is the set of free classical variables contained in processes P and Q.

We usually omit the subscripts of $\approx_c$ and $\approx_p$ when no confusion arises.

We now show that the weak bisimilarity relation $\approx$ is a weak probabilistic bisimulation; it is in fact the largest weak probabilistic bisimulation on Con.

Corollary 35 *$\approx$ is a weak probabilistic bisimulation on Con.*

Proof. By definition, we have

$$\approx = \bigcup \{\mathcal{R} \mid \mathcal{R} \text{ is a weak probabilistic bisimulation on } Con\}.$$

From Theorem 33, the reflexive and transitive closure $\approx^*$ is also a weak probabilistic bisimulation. Hence $\approx^* \subseteq \approx$. On the other hand, we have obviously $\approx \subseteq \approx^*$. So we derive that $\approx = \approx^*$, and then $\approx$ is also a weak probabilistic bisimulation. □

The next theorem gives us a necessary and sufficient condition to decide whether a pair of configurations are weakly bisimilar.

Theorem 36 *For any $\mathcal{C}, \mathcal{D} \in Con$, $\mathcal{C} \approx \mathcal{D}$ if and only if for any $s \in Act^*$,*

(1) whenever $\mathcal{C} \stackrel{s}{\Rightarrow}_C \mu$ then there exists ν such that $\mathcal{D} \stackrel{\widehat{s}}{\Rightarrow}_C \nu$ and $\mu \equiv_{\approx} \nu$,

(2) whenever $\mathcal{D} \stackrel{s}{\Rightarrow}_C \nu$ then there exists μ such that $\mathcal{C} \stackrel{\widehat{s}}{\Rightarrow}_C \mu$ and $\mu \equiv_{\approx} \nu$,

(3) if $\mathcal{C} \not\rightarrow$ and $\mathcal{D} \not\rightarrow$, then $Contex(\mathcal{C}) = Contex(\mathcal{D})$.

Proof. First, we define a new relation $\approx'$ on Con such that $\mathcal{C} \approx' \mathcal{D}$ if and only if for any $s \in Act^*$, the conditions (1), (2), and (3) hold. It is obvious that $\approx'$ is an equivalence relation. Furthermore, from Corollary 35 and Lemma 31, we have $\approx \subseteq \approx'$. Then $\approx'$ is also a weak probabilistic bisimulation on Con since $\mu \equiv_{\approx} \nu$ implies $\mu \equiv_{\approx'} \nu$. Hence we have $\approx' \subseteq \approx$ and then $\approx = \approx'$. □

5.1. *Congruence of weak probabilistic bisimilarity*

This subsection is devoted to the congruence property of weak probabilistic bisimilarity.

Lemma 37 *If $P \approx Q$, then $P[r/q] \approx Q[r/q]$ for any $r \notin qv(P) \cup qv(Q)$.*

Proof. It is direct to check that for any quantum contexts C and D, $< P[r/q]; C > \approx < Q[r/q]; D >$ if and only if $< P; C[q'/q][q/r] > \approx < Q; D[q'/q][q/r] >$ where $q' \notin qv(C) \cup qv(D)$. Then the lemma follows. □

Theorem 38 *If $P \approx Q$ then $a.P \approx a.Q$ for any $a \in \{c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, U[\bar{r}], M[\bar{r}; x]\}$.*

Proof. Assume that $\bar{x}$ is the set of free classical variables contained in processes P and Q. For any context C and any indexed value set $\bar{v}$, we need to prove $< a.P[\bar{v}/\bar{x}]; C > \approx < a.Q[\bar{v}/\bar{x}]; C >$. Suppose $< a.P[\bar{v}/\bar{x}]; C > \stackrel{\alpha}{\rightarrow} \mu$ and C is of the form $\bar{q} = \rho$. We only consider the cases where a has the form $\mathsf{c}?q$ or $M[\bar{r}; x]$; other cases are simpler.

(i) $a = \mathsf{c}?q$. There are two subcases to consider.

Case 1: $\alpha = \mathsf{c}?r$ for some $r \in \bar{q} - qv(\mathsf{c}?q.P)$. Then $\mu = < P[\bar{v}/\bar{x}][r/q]; C >$. From **Q-Inp2** rule, we have $< a.Q[\bar{v}/\bar{x}]; C > \stackrel{\alpha}{\rightarrow} < Q[\bar{v}/\bar{x}][r/q]; C >$, and furthermore, $< P[\bar{v}/\bar{x}][r/q]; C > \approx < Q[\bar{v}/\bar{x}][r/q]; C >$ from the assumption that $P \approx Q$ and Lemma 37.

Case 2: $\alpha = \mathsf{c}?r : \sigma$ for some $r \notin \bar{q}$ and $\sigma \in \mathcal{D}(\mathcal{H}_2)$. Then $\mu =< P[\bar{v}/\bar{x}][r/q]; r, \bar{q} = \sigma \otimes \rho >$. From **Q-Inp1** rule, we have $< a.Q[\bar{v}/\bar{x}]; C > \xrightarrow{\alpha} < Q[\bar{v}/\bar{x}][r/q]; r, \bar{q} = \sigma \otimes \rho >$. Furthermore, we can check that $< P[\bar{v}/\bar{x}][r/q]; r, \bar{q} = \sigma \otimes \rho > \approx < Q[\bar{v}/\bar{x}][r/q]; r, \bar{q} = \sigma \otimes \rho >$ from the assumption that $P \approx Q$ and Lemma 37.

(ii) $a = M[\bar{r}; x]$, M has the spectral decomposition $M = \sum_i \lambda_i P_i$. Then $\alpha = \tau$ and $\mu = \boxplus p_i \bullet < P[\bar{v}/\bar{x}, \lambda_i/x]; \bar{q} = P_{i,\bar{r}} \rho P_{i,\bar{r}}/p_i >$, where $p_i = \mathrm{tr} P_{i,\bar{r}} \rho$. From **Meas** rule, we derive

$$< a.Q[\bar{v}/\bar{x}]; C > \xrightarrow{\alpha} \nu = \boxplus p_i \bullet < Q[\bar{v}/\bar{x}, \lambda_i/x]; \bar{q} = P_{i,\bar{r}} \rho P_{i,\bar{r}}/p_i > .$$

Furthermore, for any $N \in Con/\approx$,

$$\mu(N) = \sum_i \{\mid p_i \mid < P[\bar{v}/\bar{x}, \lambda_i/x]; \bar{q} = P_{i,\bar{r}} \rho P_{i,\bar{r}}/p_i > \in N \mid\}$$

and

$$\nu(N) = \sum_i \{\mid p_i \mid < Q[\bar{v}/\bar{x}, \lambda_i/x]; \bar{q} = P_{i,\bar{r}} \rho P_{i,\bar{r}}/p_i > \in N \mid\}.$$

By the assumption $P \approx Q$, we have for any context D, $< P[\bar{v}/\bar{x}, \lambda_i/x]; D > \in N$ if and only if $< Q[\bar{v}/\bar{x}, \lambda_i/x]; D > \in N$. Thus $\mu(N) = \nu(N)$.

Symmetrically, we can prove that if $< a.Q[\bar{v}/\bar{x}]; C > \xrightarrow{\alpha} \nu$ for some α and ν, then there exists a transition $< a.P[\bar{v}/\bar{x}]; C > \xrightarrow{\alpha} \mu$ such that $\mu \equiv_{\approx} \nu$. Then the result of this theorem holds by using Theorem 36. □

For the sake of simplicity, in the rest of this subsection we only consider closed quantum processes. The same results can be extended easily to the case of quantum processes with free classical variables.

Theorem 39 *If $P \approx Q$ then $P[f] \approx Q[f]$ for any relabeling function f.*

Proof. Let

$$\mathcal{R}' = \{(< P[f]; C >, < Q[f]; D >) \mid < P; C > \approx < Q; D >, \text{ and } f \text{ is a relabeling function}\} \quad (8)$$

and $\mathcal{R} = (\mathcal{R}' \cup \approx)^*$ be the equivalence closure (*i.e.* the reflexive, symmetric and transitive closure) of $\mathcal{R}' \cup \approx$. We prove in the following that $\mathcal{R}$ is a weak probabilistic bisimulation on Con.

Suppose $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$. We may assume that $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}'$ because the extension to the equivalence closure is straightforward. So we can suppose further that $\mathcal{C} =< P[f]; C >$ and $\mathcal{D} =< Q[f]; D >$ for some $< P; C > \approx < Q; D >$, and f is a relabeling function.

(i) If $< P[f]; C > \xrightarrow{\alpha} \mu$, then by **Rel** rule, there exists a transition $< P; C > \xrightarrow{\beta} \mu_1 = \boxplus p_i \bullet < P_i; C_i >$ such that $\alpha = \beta[f]$ and $\mu = \boxplus p_i \bullet < P_i[f]; C_i >$. By the assumption that $< P; C > \approx < Q; D >$, we have $< Q; D > \stackrel{\widehat{\beta}}{\Rightarrow}_C \nu_1 = \boxplus q_j \bullet < Q_j; D_j >$ such that $\mu_1 \equiv_{\approx} \nu_1$. Then by **Rel** rule, it holds that

$$< Q[f]; D > \stackrel{\widehat{\alpha}}{\Rightarrow}_C \nu = \boxplus q_j \bullet < Q_j[f]; D_j >$$

and furthermore, $\mu \equiv_{\mathcal{R}} \nu$ by the fact that $\mu_1 \equiv_{\approx} \nu_1$ and the definition of $\mathcal{R}$.

(ii) If $< P[f]; C > \not\rightarrow$ and $< Q[f]; D > \not\rightarrow$, then we have $< P; C > \not\rightarrow$ and $< Q; D > \not\rightarrow$. Hence $C = D$ from the assumption that $< P; C > \approx < Q; D >$.

From (i) and (ii) we know that $\mathcal{R}$ is a weak probabilistic bisimulation on Con. Since $P \approx Q$, we have $< P; C > \approx < Q; C >$ for any quantum context C, and so $(< P[f]; C >, < Q[f]; C >) \in \mathcal{R}$. Hence $< P[f]; C > \approx < Q[f]; C >$, and $P[f] \approx Q[f]$ from the arbitrariness of C. □

Theorem 40 *If $P \approx Q$ then* **if** b **then** $P \approx$ **if** b **then** Q *for any boolean expression b.*

Proof. Obvious. □

Theorems 38 – 40 imply that weak probabilistic bisimilarity is preserved by prefix, relabeling, and conditional choice. However, it is not preserved by restriction. An example is as follows. Let U_1, U_2, V_1, V_2 be unitary transformations such that $U_2U_1 = V_2V_1$ but $U_1 \neq V_1$. Let

$$P = U_1[q].c!0.U_2[q].\mathbf{nil}, \quad Q = V_1[q].c!0.V_2[q].\mathbf{nil}.$$

It is easy to check that $P \approx Q$ but $P\backslash\{c\} \not\approx Q\backslash\{c\}$.

Now we turn to the congruence property of weak probabilistic bisimilarity under the parallel combinator. First, we have some lemmas.

Lemma 41 *For any configuration $< P; \bar{q} = \rho >$ and any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\bar{q}-qv(P)}$, we have*

(1) $< P; \bar{q} = \rho > \stackrel{\mathsf{c}?r:\sigma}{\rightarrow} < P'; r, \bar{q} = \sigma \otimes \rho >$ if and only if $< P; \bar{q} = \mathcal{E}(\rho) > \stackrel{\mathsf{c}?r:\sigma}{\rightarrow} < P'; r, \bar{q} = \sigma \otimes \mathcal{E}(\rho) >$,

(2) $< P; \bar{q} = \rho > \stackrel{\alpha}{\rightarrow} \boxplus p_i \bullet < P_i; \bar{q} = \rho_i >$ if and only if $< P; \bar{q} = \mathcal{E}(\rho) > \stackrel{\alpha}{\rightarrow} \boxplus p_i \bullet < P_i; \bar{q} = \mathcal{E}(\rho_i) >$, where α is not of the form $c?r : \sigma$.

Proof. (1) is obvious. For (2), we need only to prove the case where $\alpha = \tau$ and the transition is due to a measurement. In this case, if $< P; \bar{q} = \rho > \stackrel{\alpha}{\rightarrow} \boxplus p_i \bullet < P_i; \bar{q} = \rho_i >$, then $\rho_i = P_{i,\bar{r}}\rho P_{i,\bar{r}}/p_i$ for some projector $P_{i,\bar{r}}$ and $p_i = \mathrm{tr}(P_{i,\bar{r}}\rho)$, where $\bar{r} \subseteq qv(P)$. So we have

$$< P; \bar{q} = \mathcal{E}(\rho) > \stackrel{\alpha}{\rightarrow} \boxplus q_i \bullet < P_i; \bar{q} = P_{i,\bar{r}}\mathcal{E}(\rho)P_{i,\bar{r}}/q_i >$$

where $q_i = \mathrm{tr}(P_{i,\bar{r}}\mathcal{E}(\rho))$. Notice that $\mathcal{E}$ is acting on $\mathcal{H}_{\bar{q}-qv(P)}$ and $\bar{r} \subseteq qv(P)$. We deduce that

$$q_i = \mathrm{tr}(P_{i,\bar{r}}\mathcal{E}(\rho)) = \mathrm{tr}\mathcal{E}(P_{i,\bar{r}}\rho P_{i,\bar{r}}) = \mathrm{tr}(P_{i,\bar{r}}\rho) = p_i$$

and $P_{i,\bar{r}}\mathcal{E}(\rho)P_{i,\bar{r}}/q_i = \mathcal{E}(P_{i,\bar{r}}\rho P_{i,\bar{r}}/q_i)$. That completes the proof of the necessity part. The proof of the sufficiency part is similar. □

Lemma 42 *If $< P; \bar{q} = \rho > \approx < Q; \bar{q}' = \rho' >$, then $\bar{q} = \bar{q}'$, and $\mathrm{tr}_{\bar{r}}\rho = \mathrm{tr}_{\bar{r}}\rho'$ where $\bar{r} = qv(P) \cup qv(Q)$.*

Proof. Suppose $\mathcal{G}_1$ and $\mathcal{G}_2$ are the transition graphs of $< P; \bar{q} = \rho >$ and $< Q; \bar{q}' = \rho' >$, respectively. Take a leaf $< P'; C' >$ (so $< P'; C' > \not\rightarrow$) of $\mathcal{G}_1$ such that there exists a directed path from $< P; \bar{q} = \rho >$ to $< P'; C' >$ along which none of the actions has the form $\mathsf{c}?q$. Intuitively, this path denotes an execution where any quantum input action is realized by inputting a new qubit from outside the context. As a result, the quantum system in $\bar{q} - qv(P)$ is kept untouched in this path.

From the assumption that $< P; \bar{q} = \rho > \approx < Q; \bar{q}' = \rho' >$, we can find a leaf $< Q'; D' >$ of $\mathcal{G}_2$ such that $< P'; C' > \approx < Q'; D' >$ (so $C' = D'$), and furthermore, there exists a directed path from $< Q; \bar{q}' = \rho' >$ to $< Q'; D' >$ which has the same observable actions as the path taken in $\mathcal{G}_1$. Notice that the set of quantum variables in the accompanied

context cannot be changed by τ actions. We deduce $\bar{q} = \bar{q}'$ from the fact that $C' = D'$. Furthermore, we can show $\mathrm{tr}_{\bar{r}}\rho = \mathrm{tr}_{\bar{r}}\sigma$ since the quantum systems outside $\bar{r}$ are untouched during these two execution paths. □

Lemma 43 *Suppose* $< P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >$, $r \notin \bar{q}$ *and* $\sigma \in \mathcal{D}(\mathcal{H}_2)$. *Then*

(1) $< P; r, \bar{q} = \sigma \otimes \rho > \approx < Q; r, \bar{q} = \sigma \otimes \rho' >$.

(2) If P *and* Q *are free of quantum input and* $\mathcal{E}$ *is a super-operator acting on* $\mathcal{H}_{\bar{q}-qv(P)-qv(Q)}$, *then* $< P; r, \bar{q} = \sigma \otimes \mathcal{E}(\rho) > \approx < Q; r, \bar{q} = \sigma \otimes \mathcal{E}(\rho') >$.

Proof. We only prove (1). The proof of (2) is simpler since P and Q are free of quantum input and as a result, the super-operator $\mathcal{E}$ commutes with the quantum operations performed by P and Q. Let

$$\mathcal{R}' = \{(< P; r, \bar{q} = \sigma \otimes \rho >, < Q; r, \bar{q} = \sigma \otimes \rho' >) \mid < P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >, \\ r \notin \bar{q}, \text{ and } \sigma \in \mathcal{D}(\mathcal{H}_2)\}. \tag{9}$$

We prove in the following that $\mathcal{R} = (\mathcal{R}' \cup \approx)^*$ is a weak probabilistic bisimulation.

Suppose $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$. We may assume further that $\mathcal{C} =< P; r, \bar{q} = \sigma \otimes \rho >$ and $\mathcal{D} =< Q; r, \bar{q} = \sigma \otimes \rho' >$ for some $< P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >$, $r \notin \bar{q}$, and $\sigma \in \mathcal{D}(\mathcal{H}_2)$.

(i) If $< P; r, \bar{q} = \sigma \otimes \rho > \xrightarrow{\alpha} \mu$, there are two cases to consider.

Case 1: $\alpha = \mathsf{c}?r$ for some $\mathsf{c} \in qChan$. Then $\mu =< P'; r, \bar{q} = \sigma \otimes \rho >$ for some P'. By **Q-Inp1** rule, we have $< P; \bar{q} = \rho > \xrightarrow{\mathsf{c}?r:\sigma} \mu$. Now from the assumption $< P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >$, there exists a transition $< Q; \bar{q} = \rho' > \overset{\mathsf{c}?r:\sigma}{\Rightarrow}_C \nu$ such that $\mu \equiv_\approx \nu$. Thus it holds $< Q; r, \bar{q} = \sigma \otimes \rho' > \overset{\mathsf{c}?r}{\Rightarrow}_C \nu$, and $\mu \equiv_{\mathcal{R}} \nu$ from the fact that $\approx \subseteq \mathcal{R}$.

Case 2: $\alpha \neq \mathsf{c}?r$ for any $\mathsf{c} \in qChan$. Then we have $< P; \bar{q} = \rho > \xrightarrow{\alpha} \mu_1 = \boxplus p_i \bullet < P_i; \bar{q}' = \rho_i >$ such that $r \notin \bar{q}'$ and $\mu = \boxplus p_i \bullet < P_i; r, \bar{q}' = \sigma \otimes \rho_i >$. From the assumption $< P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >$, there exists a transition $< Q; \bar{q} = \rho' > \overset{\widehat{\alpha}}{\Rightarrow}_C \nu_1 = \boxplus q_j \bullet < Q_j; \bar{q}' = \rho'_j >$ such that $\mu_1 \equiv_\approx \nu_1$. So we have

$$< Q; r, \bar{q} = \sigma \otimes \rho' > \overset{\widehat{\alpha}}{\Rightarrow}_C \nu = \boxplus q_j \bullet < Q_j; r, \bar{q}' = \sigma \otimes \rho'_j >,$$

and $\mu \equiv_{\mathcal{R}} \nu$ from $\mu_1 \equiv_\approx \nu_1$ and the definition of $\mathcal{R}$.

(ii) If $< P; r, \bar{q} = \sigma \otimes \rho > \not\rightarrow$ and $< Q; r, \bar{q} = \sigma \otimes \rho' > \not\rightarrow$, then we have $< P; \bar{q} = \rho > \not\rightarrow$ and $< Q; \bar{q} = \rho' > \not\rightarrow$. Hence $\rho = \rho'$ from the assumption that $< P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >$, and then $\sigma \otimes \rho = \sigma \otimes \rho'$.

From (i) and (ii) we know that $\mathcal{R}$ is a weak probabilistic bisimulation on Con. That completes the proof of (1). □

From the above lemmas, we are now ready to prove that weak probabilistic bisimilarity is preserved by the parallel combinator in two special cases, as the following two theorems state.

Theorem 44 *If* $P \approx Q$, *and* P *and* Q *are free of quantum input, then* $P \| R \approx Q \| R$.

Proof. Let

$$\mathcal{R}' = \{(< P \| R; \bar{q} = \mathcal{E}(\rho) >, < Q \| R; \bar{q} = \mathcal{E}(\rho') >) \mid < P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >, \\ P \text{ and } Q \text{ are free of quantum input}, \\ \text{and } \mathcal{E} \text{ is a super-operator on } \mathcal{H}_{\bar{q}-qv(P)-qv(Q)}\}.$$

We prove in the following that $\mathcal{R} = (\mathcal{R}' \cup \approx)^*$ is a weak probabilistic bisimulation. Let $(< P \| R; \bar{q} = \mathcal{E}(\rho) >, < Q \| R; \bar{q} = \mathcal{E}(\rho') >) \in \mathcal{R}'$.

(i) Suppose $< P \| R; \bar{q} = \mathcal{E}(\rho) > \stackrel{\alpha}{\rightarrow} \mu$. Since P is free of quantum input, we have four cases to consider.

Case 1: There exists a transition $< P; \bar{q} = \rho > \stackrel{\alpha}{\rightarrow} \mu_1 = \boxplus p_i \bullet < P_i; \bar{q} = \rho_i >$ where $qv(P_i) \subseteq qv(P)$ for each i, and

$$\mu = \boxplus p_i \bullet < P_i \| R; \bar{q} = \mathcal{E}(\rho_i) > .$$

Here we have used Lemma 41 (2). From the assumption $< P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >$, it holds that $< Q; \bar{q} = \rho' > \stackrel{\widehat{\alpha}}{\Rightarrow}_C \nu_1 = \boxplus q_j \bullet < Q_j; \bar{q} = \rho'_j >$ and $\mu_1 \equiv_{\approx} \nu_1$. Using Lemma 41 (2) again, we derive

$$< Q \| R; \bar{q} = \mathcal{E}(\rho') > \stackrel{\widehat{\alpha}}{\Rightarrow}_C \nu = \boxplus q_j \bullet < Q_j \| R; \bar{q} = \mathcal{E}(\rho'_j) >,$$

and $\mu \equiv_{\mathcal{R}} \nu$ from the fact that $qv(P_i) \subseteq qv(P)$ for each i, $\mu_1 \equiv_{\approx} \nu_1$, and the definition of $\mathcal{R}$.

Case 2: There exists a transition $< R; \bar{q} = \mathcal{E}(\rho) > \stackrel{\mathsf{c}?r:\sigma}{\rightarrow} < R'; r, \bar{q} = \sigma \otimes \mathcal{E}(\rho) >$ for some $\mathsf{c} \in qChan$, $r \notin \bar{q}$, $\sigma \in \mathcal{D}(\mathcal{H}_2)$, and $\mu =< P \| R'; r, \bar{q} = \sigma \otimes \mathcal{E}(\rho) >$. Then from **Q-Inp1** and **Inp-Int** rules, we have $< R; \bar{q} = \mathcal{E}(\rho') > \stackrel{\mathsf{c}?r:\sigma}{\rightarrow} < R'; r, \bar{q} = \sigma \otimes \mathcal{E}(\rho') >$ and so

$$< Q \| R; \bar{q} = \mathcal{E}(\rho') > \stackrel{\mathsf{c}?r:\sigma}{\rightarrow} < Q \| R'; r, \bar{q} = \sigma \otimes \mathcal{E}(\rho') > .$$

Furthermore, we can prove $(< P \| R'; r, \bar{q} = \sigma \otimes \mathcal{E}(\rho) >, < Q \| R'; r, \bar{q} = \sigma \otimes \mathcal{E}(\rho') >) \in \mathcal{R}$ by Lemma 43 (2).

Case 3: There exists a transition $< R; \bar{q} = \mathcal{E}(\rho) > \stackrel{\alpha}{\rightarrow} \boxplus p_i \bullet < R_i; \bar{q} = \mathcal{E}_i(\mathcal{E}(\rho)) >$ where α is not of the form $\mathsf{c}?r : \sigma$, $\mathcal{E}_i$ is a super-operator on $\mathcal{L}(\mathcal{H}_{qv(R)})$, and $\mu = \boxplus p_i \bullet < P \| R_i; \bar{q} = \mathcal{E}_i(\mathcal{E}(\rho)) >$. Here we have used Lemma 14. Then from Lemma 42, we derive $< R; \bar{q} = \mathcal{E}(\rho') > \stackrel{\alpha}{\rightarrow} \boxplus p_i \bullet < R_i; \bar{q} = \mathcal{E}_i(\mathcal{E}(\rho')) >$. Thus

$$< Q \| R; \bar{q} = \mathcal{E}(\rho') > \stackrel{\alpha}{\rightarrow} \nu = \boxplus p_i \bullet < Q \| R_i; \bar{q} = \mathcal{E}_i(\mathcal{E}(\rho')) > .$$

Notice that for any i, we have $(< P \| R_i; \bar{q} = \mathcal{E}_i(\mathcal{E}(\rho)) >, < Q \| R_i; \bar{q} = \mathcal{E}_i(\mathcal{E}(\rho')) >) \in \mathcal{R}$ since the composite map $\mathcal{E}^i \circ \mathcal{E}$ is also a super-operator acting on $\mathcal{H}_{\bar{q}-qv(P)-qv(Q)}$. Then it follows that $\mu \equiv_{\mathcal{R}} \nu$.

Case 4: $\alpha = \tau$, and the action is caused by a communication between P and R. Without loss of any generality, we assume that

$$< P; \bar{q} = \mathcal{E}(\rho) > \stackrel{c?v}{\rightarrow} < P'; \bar{q} = \mathcal{E}(\rho) >, \quad < R; \bar{q} = \mathcal{E}(\rho) > \stackrel{c!v}{\rightarrow} < R'; \bar{q} = \mathcal{E}(\rho) >$$

where $qv(P') = qv(P)$ and $\mu = < P' \| R'; \bar{q} = \mathcal{E}(\rho) >$. Then $< P; \bar{q} = \rho > \stackrel{c?v}{\rightarrow} < P'; \bar{q} = \rho >$, and from the assumption $< P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >$, we derive that

$$< Q; \bar{q} = \rho' > \stackrel{c?v}{\Rightarrow}_C \boxplus p_i \bullet < Q_i; \bar{q} = \rho'_i >,$$

and for any i, $< P'; \bar{q} = \rho > \approx < Q_i; \bar{q} = \rho'_i >$. Notice that from $< R; \bar{q} = \mathcal{E}(\rho) > \stackrel{c!v}{\rightarrow} < R'; \bar{q} = \mathcal{E}(\rho) >$ we can deduce that $< R; C > \stackrel{c!v}{\rightarrow} < R'; C >$ for any context C. Thus

$$< Q \| R; \bar{q} = \rho' > \stackrel{\tau}{\Rightarrow}_C \nu = \boxplus p_i \bullet < Q_i \| R'; \bar{q} = \rho'_i >$$

by using **C-Com** rule. Furthermore, we have $\mu \equiv_{\mathcal{R}} \nu$ since $(< P'\|R'; \bar{q} = \mathcal{E}(\rho) >, < Q_i\|R'; \bar{q} = \mathcal{E}(\rho_i') >) \in \mathcal{R}$ for each i, which in turn can be be proved by the facts that $qv(P') = qv(P)$ and $< P'; \bar{q} = \rho > \approx < Q_i; \bar{q} = \rho_i' >$.

(ii) If $< P\|R; \bar{q} = \mathcal{E}(\rho) > \not\to$ and $< Q\|R; \bar{q} = \mathcal{E}(\rho') > \not\to$, then we have $< P; \bar{q} = \rho > \not\to$ and $< Q; \bar{q} = \rho' > \not\to$. Hence $\rho = \rho'$ from the assumption $< P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho' >$. So we derive $\mathcal{E}(\rho) = \mathcal{E}(\rho')$.

From (i) and (ii) we know that $\mathcal{R}$ is a weak probabilistic bisimulation on Con. For any quantum context $\bar{q} = \rho$, by $P \approx Q$ we have $< P; \bar{q} = \rho > \approx < Q; \bar{q} = \rho >$ and then $(< P\|R; \bar{q} = \rho >, < Q\|R; \bar{q} = \rho >) \in \mathcal{R}$ since the identity transformation is also a super-operator on $\mathcal{H}_{\bar{q}-qv(P)-qv(Q)}$. Then it follows that $< P\|R; \bar{q} = \rho > \approx < Q\|R; \bar{q} = \rho >$, and so $P\|R \approx Q\|R$ from the arbitrariness of the context. □

The constraint that P and Q are free of quantum input is vital for the proof of this theorem: it guarantees that for any derivative $< P'; C >$ (node in the transition graph) of $< P; \bar{q} = \rho >$, $qv(P') \subseteq qv(P)$, and then, any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\bar{q}-qv(P)}$ is also a super-operator acting on $\mathcal{H}_{\bar{q}-qv(P')}$. As a result, any quantum unitary transformation or measurement performed by $< P'; C >$ commutes with $\mathcal{E}$. When P and Q are not free of quantum input, an example (see Example 46 below) will be presented to show why the proof technique used in this theorem fails.

Although we only consider in Theorem 44 a special case where neither P nor Q will ever have the power to input a qubit, this case covers an important scenario called LOCC (local operations and classical communication) in quantum information field. When communicating parties are spatially separated, they are usually restricted to performing local (quantum) operations on their own subsystems and transmitting classical information (say, the outcomes of measurements) to coordinate the local operations. This restriction is partially due to technological consideration: noiseless long-distance quantum communication is often very difficult to realize. LOCC restriction is also widely required in the study of quantum entanglement [23,24].

Theorem 45 *If $P \approx Q$, then $P\|R \approx Q\|R$ provided that R is free of unitary transformation and quantum measurement.*

Proof. Let

$$\mathcal{R}' = \{(< P\|R; C >, < Q\|R; D >) \mid < P; C > \approx < Q; D >, \\ R \text{ is free of unitary transformation and quantum measurement}\}.$$

We prove in the following that $\mathcal{R} = (\mathcal{R}' \cup \approx)^*$ is a weak probabilistic bisimulation. Suppose $(< P\|R; C >, < Q\|R; D >) \in \mathcal{R}'$.

(i) If $< P\|R; C > \stackrel{\alpha}{\to} \mu$, there are four cases to consider.

Case 1: There exists a transition $< P; C > \stackrel{\alpha}{\to} \mu_1 = \boxplus p_i \bullet < P_i; C_i >$ and $\mu = \boxplus p_i \bullet < P_i\|R; C_i >$. By the assumption that $< P; C > \approx < Q; D >$, we have $< Q; D > \stackrel{\widehat{\alpha}}{\Rightarrow}_C \nu_1 = \boxplus q_j \bullet < Q_j; D_j >$ such that $\mu_1 \equiv_{\approx} \nu_1$. So it holds

$$< Q\|R; D > \stackrel{\widehat{\alpha}}{\Rightarrow}_C \nu = \boxplus q_j \bullet < Q_j\|R; D_j > .$$

Furthermore, we can prove $\mu \equiv_{\mathcal{R}} \nu$ from $\mu_1 \equiv_{\approx} \nu_1$ and the definition of $\mathcal{R}$.

Case 2: There exists a transition $< R; \bar{q} = \rho > \stackrel{\mathsf{c}?r;\sigma}{\to} < R'; r, \bar{q} = \sigma \otimes \rho >$ for some $\mathsf{c} \in qChan$, $r \notin \bar{q}$, $\sigma \in \mathcal{D}(\mathcal{H}_2)$, and $\mu = < P\|R'; r, \bar{q} = \sigma \otimes \rho >$. Here we

assume that C and D are of the forms $\bar{q} = \rho$ and $\bar{q} = \rho'$, respectively. Then from **Q-Inp1** and **Inp-Int** rules, we have

$$< Q\|R; \bar{q} = \rho' > \stackrel{\mathsf{c}?r:\sigma}{\rightarrow} < Q\|R'; r, \bar{q} = \sigma \otimes \rho' >,$$

and $(< P\|R'; r, \bar{q} = \sigma \otimes \rho >, < Q\|R'; r, \bar{q} = \sigma \otimes \rho' >) \in \mathcal{R}$ from Lemma 43 (1) and the fact that R' is also free of unitary transformation and quantum measurement.

Case 3: There exists a transition $< R; C > \stackrel{\alpha}{\rightarrow} < R'; C >$ where α is not of the form $\mathsf{c}?r : \sigma$, and $\mu = < P\|R'; C >$. Here we have used the assumption that R is free of unitary transformation and quantum measurement. Then it holds that $< R; D > \stackrel{\alpha}{\rightarrow} < R'; D >$ and then

$$< Q\|R; D > \stackrel{\alpha}{\rightarrow} < Q\|R'; D > .$$

Furthermore, we have $(< P\|R'; C >, < Q\|R'; D >) \in \mathcal{R}$ by the definition of $\mathcal{R}$.

Case 4: $\alpha = \tau$, and the action is caused by a (classical or quantum) communication between P and R. We assume that

$$< P; C > \stackrel{\mathsf{c}?r}{\rightarrow} < P'; C >, \quad < R; C > \stackrel{\mathsf{c}!r}{\rightarrow} < R'; C >$$

and $\mu = < P'\|R'; C >$. Other cases are similar. From the assumption that $< P; C > \approx < Q; D >$, we have

$$< Q; D > \stackrel{\mathsf{c}?r}{\Rightarrow}_C \boxplus p_i \bullet < Q_i; D_i > \text{ and for any } i \ , < P'; C > \approx < Q_i; D_i > .$$

Notice that from $< R; C > \stackrel{\mathsf{c}!r}{\rightarrow} < R'; C >$ we can deduce that $< R; G > \stackrel{\mathsf{c}!r}{\rightarrow} < R'; G >$ for any context G involving the qubit r. Thus from **Q-Com** rule,

$$< Q\|R; D > \stackrel{\tau}{\Rightarrow}_C \nu = \boxplus p_i \bullet < Q_i\|R'; D_i > .$$

In order to show $\mu \equiv_{\mathcal{R}} \nu$, we need only to prove that for any i, $(< P'\|R'; C > , < Q_i\|R'; D_i >) \in \mathcal{R}$, which is direct from the fact that $< P'; C > \approx < Q_i; D_i >$.

(ii) If $< P\|R; C > \not\rightarrow$ and $< Q\|R; D > \not\rightarrow$, then we have $< P; C > \not\rightarrow$ and $< Q; D > \not\rightarrow$. Hence $C = D$ from the assumption $< P; C > \approx < Q; D >$.

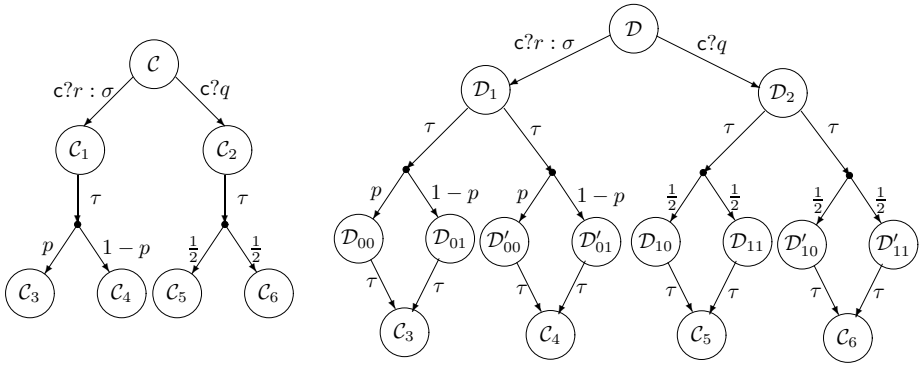
From (i) and (ii) we know that $\mathcal{R}$ is a weak probabilistic bisimulation on Con. So by $P \approx Q$, we can deduce that $< P; C > \approx < Q; C >$ for any context C. Then $(< P\|R; C > , < Q\|R; C >) \in \mathcal{R}$ and hence $< P\|R; C > \approx < Q\|R; C >$. Finally, we derive $P\|R \approx Q\|R$ by the arbitrariness of C. □

As we know, the standard technique in classical process algebra for proving that bisimilarity is preserved by static combinators such as relabeling, restriction, and parallel combinators is to construct a relation consisting of pairs of configurations having the considered static structure, and prove that it is a bisimulation. This technique is also used in the proofs of Theorems 38, 39, and 44. It will fail, however, to prove the congruence property under parallel combinator when general quantum processes are considered. The following example illustrates how entanglement between different quantum systems and the non-commutativity of quantum operations make the technique fail. Particularly, we will construct quantum processes P, Q, R, and context C, such that $< P; C > \approx < Q; C >$ but $< P\|R; C > \not\approx < Q\|R; C >$.

Example 46 Let $M_{0,1}$, σ_0, σ_1, and $|+\rangle$ be given as in Section 2 and Example 22. Suppose $P = \mathsf{c}?q.M_{0,1}[q;x].\mathbf{nil}$, and

$$Q = \mathsf{c}?q.(M_{0,1}[q;x].\sigma_x[q].\mathbf{nil} + M_{0,1}[q;x].\sigma_{1-x}[q].\mathbf{nil})$$

is the process which inputs a qubit and then nondeterministically sets it to $|0\rangle$ or $|1\rangle$. Let $\mathcal{C} =< P; q = |+\rangle\langle+| >$ and $\mathcal{D} =< Q; q = |+\rangle\langle+| >$. Then the transition graphs of $\mathcal{C}$ and $\mathcal{D}$ can be depicted respectively as



where $p = \langle 0|\sigma|0\rangle$ and

$$\begin{aligned}
&\mathcal{C}_1 =< M_{0,1}[r;x].\mathbf{nil}; r, q = \sigma \otimes |+\rangle\langle+| >, && \mathcal{C}_2 =< M_{0,1}[q;x].\mathbf{nil}; q = |+\rangle\langle+| >,\\
&\mathcal{C}_3 =< \mathbf{nil}; r, q = |0\rangle\langle 0| \otimes |+\rangle\langle+| >, && \mathcal{C}_4 =< \mathbf{nil}; r, q = |1\rangle\langle 1| \otimes |+\rangle\langle+| >,\\
&\mathcal{C}_5 =< \mathbf{nil}; q = |0\rangle\langle 0| >, && \mathcal{C}_6 =< \mathbf{nil}; q = |1\rangle\langle 1| >,\\
&\mathcal{D}_1 =< Q'[r/q]; r, q = \sigma \otimes |+\rangle\langle+| >, && \mathcal{D}_2 =< Q'; q = |+\rangle\langle+| >,\\
&\mathcal{D}_{0i} =< \sigma_i[r].\mathbf{nil}; r, q = |i\rangle\langle i| \otimes |+\rangle\langle+| >, && \mathcal{D}'_{0i} =< \sigma_{1-i}[r].\mathbf{nil}; r, q = |i\rangle\langle i| \otimes |+\rangle\langle+| >,\\
&\mathcal{D}_{1i} =< \sigma_i[q].\mathbf{nil}; q = |i\rangle\langle i| >, && \mathcal{D}'_{1i} =< \sigma_{1-i}[q].\mathbf{nil}; q = |i\rangle\langle i| >,
\end{aligned}$$

and

$$Q' = M_{0,1}[q;x].\sigma_x[q].\mathbf{nil} + M_{0,1}[q;x].\sigma_{1-x}[q].\mathbf{nil}.$$

Take

$$\mathcal{R} = \{(\mathcal{C}, \mathcal{D}), (\mathcal{C}_1, \mathcal{D}_1), (\mathcal{C}_2, \mathcal{D}_2), (\mathcal{C}_3, \mathcal{D}_{0i}), (\mathcal{C}_4, \mathcal{D}'_{0i}), (\mathcal{C}_5, \mathcal{D}_{1i}), (\mathcal{C}_6, \mathcal{D}'_{1i}) : i = 0, 1\}.$$

It is easy to check that $\mathcal{R}$ is indeed a weak probabilistic bisimulation. Thus $\mathcal{C} \approx \mathcal{D}$.

Now let $R = \mathsf{c}?r.CNOT[q,r].\mathsf{c}!q.\mathbf{nil}$. Then we have

$$< P \| R; q = |+\rangle\langle+| > \not\approx < Q \| R; q = |+\rangle\langle+| >$$

because $< P \| R; q = |+\rangle\langle+| >$ has a transition sequence

$$\begin{aligned}
< P \| R; q = |+\rangle\langle+| > &\stackrel{\mathsf{c}?r:|0\rangle\langle 0|}{\to} < P \| (CNOT[q,r].\mathsf{c}!q.\mathbf{nil}); r, q = [|0\rangle|+\rangle] >\\
&\stackrel{\tau}{\to} < P \| \mathsf{c}!q.\mathbf{nil}; r, q = [\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)] >\\
&\stackrel{\tau}{\to} < M_{0,1}[q;x].\mathbf{nil} \| \mathbf{nil}; r, q = [\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)] >
\end{aligned}$$

$$\xrightarrow{\tau} \quad \frac{1}{2}\bullet < \mathbf{nil}\|\mathbf{nil}; r, q = [|00\rangle] > \\ \boxplus\frac{1}{2}\bullet < \mathbf{nil}\|\mathbf{nil}; r, q = [|11\rangle] >$$

while the only form of combined weak $\mathsf{c}?r : |0\rangle\langle 0|$-transitions of $< Q\|R; q = |+\rangle\langle +| >$ is

$$< Q\|R; q = [|+\rangle] > \stackrel{\mathsf{c}?r:|0\rangle\langle 0|}{\Rightarrow}_C s\bullet < \mathbf{nil}\|\mathbf{nil}; r, q = [|00\rangle] > \\ \boxplus(1-s)\bullet < \mathbf{nil}\|\mathbf{nil}; r, q = [|01\rangle] >$$

where $s \in [0, 1]$. □

5.2. *Equality relation between quantum processes*

As in classical process algebra, $\approx$ is not preserved by summation combinator '+'. To deal with it, we introduce the notion of equality between quantum processes.

Definition 47 *Two configurations $\mathcal{C}$ and $\mathcal{D}$ are said to be equal, denoted by $\mathcal{C} \simeq \mathcal{D}$, if for any $\alpha \in Act$,*

(1) whenever $\mathcal{C} \stackrel{\alpha}{\to} \mu$ then there exists ν such that $\mathcal{D} \stackrel{\alpha}{\Rightarrow}_C \nu$ and $\mu \equiv_{\approx} \nu$,

(2) whenever $\mathcal{D} \stackrel{\alpha}{\to} \nu$ then there exists μ such that $\mathcal{C} \stackrel{\alpha}{\Rightarrow}_C \mu$ and $\mu \equiv_{\approx} \nu$,

(3) if $\mathcal{C} \not\to$ and $\mathcal{D} \not\to$, then $Contex(\mathcal{C}) = Contex(\mathcal{D})$.

The only difference between the definitions of $\approx$ and $\simeq$ is that in the latter $\mathcal{D} \stackrel{\widehat{\alpha}}{\Rightarrow}_C \nu$ is replaced by $\mathcal{D} \stackrel{\alpha}{\Rightarrow}_C \nu$, *i.e.*, the matching action for a τ-move has to be a real τ-move.

Furthermore, we lift the definition of equality to quantum processes as follows. For $P, Q \in qProc$, and $\bar{x}$ is the set of free classical variables contained in P and Q, $P \simeq Q$ if $P[\bar{v}/\bar{x}] \simeq Q[\bar{v}/\bar{x}]$ for any indexed set $\bar{v}$ of values.

The following properties are direct from definition. So we omit the proofs here.

Theorem 48 *$P \sim Q$ implies $P \simeq Q$, and $P \simeq Q$ implies $P \approx Q$.*

Theorem 49 *If $P \approx Q$ then $a.P \simeq a.Q$ for any $a \in \{c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, U[\bar{q}], M[\bar{q}; x]\}$;*

Theorem 50 *For any $P, Q \in qProc$, $P \simeq Q$ if and only if $P + R \approx Q + R$ for all $R \in qProc$.*

Finally, a congruence property similar to Theorem 28 is also satisfied by the quality relation.

Theorem 51 *If $P \simeq Q$ then*

(1) $a.P \simeq a.Q$, for any $a \in \{c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, U[\bar{q}], M[\bar{q}; x]\}$,

(2) $P + R \simeq Q + R$, for any $R \in qProc$,

(3) $P\|R \simeq Q\|R$, provided that R is free of unitary transformation and measurement, or P and Q are free of quantum input,

(4) $P[f] \simeq Q[f]$, for any relabeling function f,

*(5) **if** b **then** $P \simeq$ **if** b **then** Q for any boolean expression b.*

Proof. (2) is direct from Theorem 50. Others are similar to the proofs of corresponding results for $\approx$. □

6. Conclusions and further work

In this paper, we propose a framework qCCS to model and reason about the behaviors of quantum concurrent systems. This framework is a natural quantum extension of

classical value-passing CCS. To make qCCS consistent with the laws of quantum mechanics, some syntactical restrictions on valid quantum processes are introduced. The operational semantics of qCCS is given in terms of probabilistic labeled transition system. This semantics has many different features compared with the proposals in literature in describing input and output of quantum systems which are correlated with other systems. We make the design decision of keeping the probability information resulting from quantum measurements instead of resolving probabilistic choice in each intermediate step as is done in [16] and [10]. Based on this operational semantics, we define the notions of strong (weak) probabilistic bisimulation and equality between quantum processes and examine some properties such as congruence of them.

The congruence property we proved in this paper is, however, a weak one in which bisimilarity is preserved by the parallel combinator when some constraints are put on paralleled processes. New techniques must be invented when general processes are considered, since we have presented an example to show why standard proof techniques do not work because of the entanglement between quantum systems and the non-commutativity of quantum operations. A potential way to tackle this problem, motivated by Theorem 50, is to define a new relation, say $\sim'$, between quantum processes such that $P \sim' Q$ if and only if for any R, $P\|R \sim Q\|R$. Obviously we have $\sim' \subseteq \sim$, and $\sim'$ is also an equivalence relation. Furthermore, we can show that this relation is preserved by all combinators defined in this paper except for restriction. So the problem of whether strong probabilistic bisimilarity is preserved by the parallel combinator is equivalent to the problem of whether or not $\sim' = \sim$.

Another direction along this line is to give up the notion of bisimulation and instead search for other coarser order relations among quantum processes which are preserved by the combinators defined in this paper. For example, we can drop the symmetry of bisimulation and instead define a notion of simulation which relates processes P and Q if for any context C, each action of $< P; C >$ can be simulated by a (combined) action of $< Q; C >$, and the resulted configurations also satisfy this order relation.

Recursive definitions are very useful in modeling infinite behavior of processes. Furthermore, uniqueness of solutions of recursion equations provides a powerful tool for reasoning about the correctness of implementations with respect to specifications. However, there are some technical difficulties in introducing recursive constructs into qCCS. For example, if we allow the process defined by

$$A := \mathsf{c}!q.A \tag{10}$$

to be valid, then problems will occur when we attempt to assign free quantum variables to A: on one hand, from Definition 1 (5), to make $\mathsf{c}!q.A$ meaningful we must have $q \notin qv(A)$; on the other hand, also from Definition 1 (5), we know $q \in qv(\mathsf{c}!q.A)$. This is a contradiction because we will naturally require $qv(\mathsf{c}!q.A) \subseteq qv(A)$ in definition equation (10). However, the difficulty does not exist in the following recursively defined quantum process

$$A := \mathsf{c}?q.U[q].\mathsf{c}!q.A \tag{11}$$

which consequently inputs a qubit through quantum channel c, applies a predefined unitary transformation U on it, and outputs it through c. Here we can freely let $qv(A) = \emptyset$.

In order to provide some useful mathematical tools for describing approximate correctness and evolution of concurrent systems, one of the authors has tried to develop topology in process algebras [37]. In particular, he and Wirsing [36] introduced the notions of λ-bisimulation and approximate bisimulation in CCS equipped with a metric on its set of action names, and further applied them to probabilistic processes [38]. To extend these notions to the quantum setting is a direction worthy of future investigation.

Acknowledgement

We thank the referees for their helpful comments and suggestions, which improved the presentation and the quality of this paper.

The authors thank the colleagues in the Quantum Computation and Quantum Information Research Group for useful discussion. This work was partially supported by the FANEDD under Grant No. 200755, the 863 Project under Grant No. 2006AA01Z102, and the Natural Science Foundation of China (Grant Nos. 60503001, 60621062, and 60433050). Y. Feng was also partly supported by Tsinghua Basic Research Foundation under Grant No. 052220204.

References

[1] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68:3121, 1992.

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

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

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

[5] S. Bettelli, T. Calarco, and L. Serafini. Toward an architecture for quantum programming. *European Physical Journal D*, 25(2):181–200, 2003.

[6] P. J. Bussey. Communication and non-communication in einstein-rosen experiments. *Physics Letters A*, 123:1–3, 1987.

[7] A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67:661, 1991.

[8] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982.

[9] S. J. Gay. Quantum programming languages: survey and bibliography. *Mathematical Structures in Computer Science*, 16(04):581–600, 2006.

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

[11] G. C. Ghirardi and T. Weber. Quantum mechanics and faster-than-light communication methodological considerations. *Nuovo Cimento B*, 11(78 B):9–20, 1983.

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

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

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

[15] M. Hennessy and A. Ingólfsdóttir. A theory of communicating processes value-passing. *Information and Computation*, 107(2):202–236, 1993.
[16] P. Jorrand and M. Lalire. Toward a quantum process algebra. In P. Selinger, editor, *Proceedings of the 2nd International Workshop on Quantum Programming Languages, 2004*, page 111, 2004.
[17] E. H. Knill. Conventions for quantum pseudocode. *LANL report LAUR-96-2724*, 1996.
[18] K. Kraus. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Springer, Berlin, 1983.
[19] Marie Lalire. A probabilistic branching bisimulation for quantum processes. 2005. arXiv:quant-ph/0508116 v1 16 Aug 2005.
[20] Marie Lalire. Relations among quantum processes: Bisimilarity and congruence. *Mathematical Structures in Computer Science*, 16(3):407–428, 2006.
[21] K. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94:456–471, 1991.
[22] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, parts i and ii. *Information and Computation*, 100:1–77, 1992.
[23] M. Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83:436–439, 1999.
[24] Michael Nielsen and Isaac Chuang. *Quantum computation and quantum information*. Cambridge university press, 2000.
[25] B. Ömer. *A procedural formalism for quantum computing*. Master thesis, Department of Theoretical Physics, Technical University of Vienna, 1998. http://tph.tuwien.ac.at/oemer/qcl.html.
[26] B. Ömer. *Structured Quantum Programming*. PhD thesis, Department of Theoretical Physics, Technical University of Vienna, 2003.
[27] A. Poppe, A. Fedrizzi, T. Lorunser, O. Maurhardt, R. Ursin, H. R. Bohm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger. Practical quantum key distribution with polarization entangled photons. 2004. arXiv:quant-ph/0404115.
[28] J. W. Sanders and P Zuliani. Quantum programming. *Mathematics of Program Construction*, 1837:80–99, 2000.
[29] R. Segala and N. Lynch. Probabilistic simulations for probabilitsic processes. In *Proc. CONCUR'94, Theories of Concurrency Unification and Extension, Lecture Notes in Computer Science*, volume 836, pages 481–496, 1994.
[30] R. Segala and N. Lynch. Probabilistic simulations for probabilistic processes. *Nordic Journal of Computing*, 2(2):250–273, 1995.
[31] P. Selinger. A brief survey of quantum programming languages. *Functional and Logic Programming*, 2998:1–6, 2004.
[32] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.
[33] Peter W. Shor. Algorithms for quantum computation: discrete log and factoring. In *Proceedings of the 35th IEEE FOCS*, pages 124–134, 1994.
[34] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Princeton, NJ, 1955.
[35] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.
[36] M . S. Ying and M. Wirsing. Approximate bisimilarity. In T. Rus, editor, *Algebraic Methodology and Software Technology, 8th International Conference*, volume 1816 of *Lecture Notes in Computer Science*, pages 309–321, Iowa City, USA, 2000.
[37] M. S. Ying. *Topology in Process Calculus: Approximate Correctness and Infinite Evolution of Concurrent Programs*. Springer-Verlag New York, 2001.
[38] M. S. Ying. Additive models of probabilistic processes. *Theoretical Computer Science*, 275:481–519, 2002.
[39] P. Zuliani. *Quantum Programming*. PhD thesis, Oxford University, 2001.
[40] P Zuliani. Quantum programming with mixed states. In *Proceedings of the 3rd International Workshop on Quantum Programming Languages*, Chicago, 2005.