Bisimulation for Quantum Processes

YUAN FENG, RUNYAO DUAN, and MINGSHENG YING,
University of Technology, Sydney, Australia, and Tsinghua University, China

Quantum cryptographic systems have been commercially available, with a striking advantage over classical systems that their security and ability to detect the presence of eavesdropping are provable based on the principles of quantum mechanics. On the other hand, quantum protocol designers may commit more faults than classical protocol designers since human intuition is poorly adapted to the quantum world. To offer formal techniques for modeling and verification of quantum protocols, several quantum extensions of process algebra have been proposed. An important issue in quantum process algebra is to discover a quantum generalization of bisimulation preserved by various process constructs, in particular, parallel composition, where one of the major differences between classical and quantum systems, namely quantum entanglement, is present. Quite a few versions of bisimulation have been defined for quantum processes in the literature, but in the best case they are only proved to be preserved by parallel composition of purely quantum processes where no classical communication is involved.

Many quantum cryptographic protocols, however, employ the LOCC (Local Operations and Classical Communication) scheme, where classical communication must be explicitly specified. So, a notion of bisimulation preserved by parallel composition in the circumstance of both classical and quantum communication is crucial for process algebra approach to verification of quantum cryptographic protocols. In this article we introduce novel notions of strong bisimulation and weak bisimulation for quantum processes, and prove that they are congruent with respect to various process algebra combinators including parallel composition even when both classical and quantum communication are present. We also establish some basic algebraic laws for these bisimulations. In particular, we show the uniqueness of the solutions to recursive equations of quantum processes, which proves useful in verifying complex quantum protocols. To capture the idea that a quantum process approximately implements its specification, and provide techniques and tools for approximate reasoning, a quantified version of strong bisimulation, which defines for each pair of quantum processes a bisimulation-based distance characterizing the extent to which they are strongly bisimilar, is also introduced.

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

General Terms: Languages, Theory, Verification

Additional Key Words and Phrases: Quantum communication, quantum computing, quantum process algebra, bisimulation, congruence

---

This work is an extended version of a paper presented at POPL 2011.
This work was supported by Australian ARC grants DP110103473, DP130102764, and FT100100218. The authors are also partially supported by the Overseas Team Program of the Academy of Mathematics and Systems Science, Chinese Academy of Sciences.
Authors' address: Y. Feng (corresponding author), R. Duan, and M. Ying, Center of Quantum Computation and Intelligent Systems (QCIS), Faculty of Information Technology, University of Technology, Sydney, City Campus, 15 Broadway, Ultimo, NSW 2007 Australia and State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China; email: yuan.feng@uts.edu.au.

DOI 10.1145/2400676.2400680 http://doi.acm.org/10.1145/2400676.2400680

ACM Reference Format:
Feng, Y., Duan, R., and Ying, M. 2012. Bisimulation for quantum processes. ACM Trans. Program. Lang. Syst. 34, 4, Article 17 (December 2012), 43 pages.
DOI = 10.1145/2400676.2400680 http://doi.acm.org/10.1145/2400676.2400680

1. INTRODUCTION

Quantum computing offers the potential of considerable speedup over classical computing for some important problems such as prime factoring [Shor 1994] and unsorted database search [Grover 1997]. However, functional quantum computers which can harness this potential in dealing with practical applications are extremely difficult to implement. On the other hand, quantum cryptography, of which the security and ability to detect the presence of eavesdropping are provable based on the principles of quantum mechanics, has been developed so rapidly that quantum cryptographic systems are already commercially available by a number of companies such as Id Quantique, Cerberis, MagiQ Technologies, SmartQuantum, and NEC.

As is well known, it is very difficult to guarantee the correctness of classical communication protocols at the design stage, and some simple protocols were finally found to have fundamental flaws. Since human intuition is poorly adapted to the quantum world, quantum protocol designers may commit more faults than classical protocol designers, especially when more and more complicated quantum protocols can be implemented by future physical technology. With the purpose of cloning the success classical process algebras achieved in analyzing and verifying classical communication protocols and even distributed computing, various quantum process algebras have been proposed independently by several research groups. Jorrand and Lalire [2004] defined a language QPAlg (Quantum Process Algebra) by extending a classical CCS-like process algebra. A branching bisimulation which identifies quantum processes associated with graphs having the same branching structure was also presented [Lalire 2006]. The bisimulation is, however, not congruent: it is not preserved by parallel composition. Gay and Nagarajan [2005] defined a language CQP (Communicating Quantum Processes), which combines the communication primitives of pi-calculus [Milner et al. 1992] with primitives for unitary transformations and measurements. One distinctive feature of CQP is a type system which guarantees the physical realizability of quantum processes. However, no notion of equivalence between processes was presented.

Authors of the current article proposed a model named qCCS [Feng et al. 2007] for quantum communicating systems by adding quantum input/output and quantum operation/measurement primitives to classical value-passing CCS [Hennessy 1991; Hennessy and Ingólfsdóttir 1993]. The semantics of quantum input and output was carefully designed to describe the communication of quantum systems which have been entangled with other systems. A bisimulation was defined for finite processes, and a simplified version of congruence property was proved, in which parallel composition is only permitted when the participating processes are free of quantum input, or free of quantum operations and measurements. In Ying et al. [2009] the same authors studied a purely quantum version of qCCS where no classical data is explicitly involved, aiming at providing a suitable framework to observe the interaction of computation and communication in quantum systems. A strong bisimulation was defined for this purely quantum qCCS and shown to be fully preserved by parallel composition. However, it is worth noting that the bisimulation proposed in Ying et al. [2009] cannot be directly extended to general qCCS where classical data as well as probabilistic behaviors are included.

In this article, we combine the two models proposed in Feng et al. [2007] and Ying et al. [2009] together to involve both classical data and quantum data. This

general model, which we still call qCCS for coherence, accommodates all classical process constructors (especially recursive definitions) as well as quantum primitives. As a consequence, both sequential and distributed quantum computing, quantum communication protocols, and quantum cryptographic systems can be formally modeled and rigorously analyzed in the framework of qCCS. We also design strong/weak bisimulations and approximate strong bisimulation for quantum processes, all turning out to be congruent with respect to various process constructors of qCCS. These bisimulations have several distinctive features compared with those proposed in the literature: First, the bisimulations in this article take local quantum operations into account in a weak manner, but at the same time fit well with recursive definitions. Lalire's bisimulation cannot distinguish different operations on a quantum system which will never be output: quantum states are only compared when they are input or output. Bisimulation defined in Feng et al. [2007] works well only for finite processes since quantum states are required to be compared after all the actions have been performed. Note that no state comparison is needed in Ying et al. [2009] since all local quantum operations are regarded as visible actions, and the resulted bisimulation is a very strong one; it distinguishes two different sequences of local operations even when they have the same effect as a whole. Secondly, entanglement between the input/output system and the remaining systems is fully considered in our definition of bisimulations. Bisimulation presented in Lalire [2006] totally ignores this correlation by only considering the reduced state of the input/output system. In Feng et al. [2007] this consideration is implicitly made by the state comparison after the processes terminating. Again, it does not work for infinite processes. Finally, but most importantly, the strong bisimilarity and the equivalence derived from the weak bisimulation are both congruent, making them suitable for equational reasoning in verifying quantum communication and cryptographic systems. Lalire's bisimulation is not preserved by parallel composition. The bisimulation in Feng et al. [2007] is not preserved by restriction, and whether it is preserved by parallel composition still remains open, although the positive answer is affirmed in two special cases. The strong bisimulation proposed in Ying et al. [2009] is indeed a congruence. However, since no classical data is involved in that model, many important quantum communication protocols such as superdense coding and teleportation cannot be described. This restricts the scope of its application.

This article is an extension and completion of our primary results reported at POPL [Feng et al. 2011]. The main difference is that in the current article: (1) a section on strong bisimulation is added where internal actions are treated in the same way as visible actions; (2) a notion of approximate strong bisimulation is introduced to characterize the extent to which two quantum processes are bisimilar; and (3) the proofs of the main results are presented, wheras they were omitted in Feng et al. [2011] because of the limitation of space. The rest of the article is organized as follows. In Section 2, we review some basic notions from linear algebra and quantum mechanics. The syntax and operational semantics of qCCS are presented in Section 3. To illustrate the expressiveness of qCCS, we describe with it the well-known quantum superdense coding and teleportation protocols. We also show how to encode quantum unitary gates and measurement gates, which are two basic elements of quantum circuits, by qCCS. Section 4 defines the notion of strong bisimulation for configurations as well as quantum processes. Various properties such as congruence property, monoid laws, static laws, the expansion law, as well as uniqueness of solutions of process equations, are also examined. In Section 5, a notion of approximate strong bisimulation is proposed and its corresponding metric between quantum processes defined. It is proved that the approximate strong bisimulation is also congruent and the corresponding metric nonexpansive with respect to all process constructors in qCCS. Section 6 is devoted to

proposing a weak bisimulation, and an equivalence relation based on the weak bisimularity is also defined and proved to be fully preserved by all process constructors of qCCS. The validity of examples in Section 3 is proved by using the notion of weak bisimilarity defined in this section. We outline the main results in Section 7 and point out some problems for further study. In particular, we discuss the difficulty of defining an approximate weak bisimulation for quantum processes.

2. PRELIMINARIES

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

2.1. Basic Linear Algebra

An *inner product space* $\mathcal{H}$ is a vector space equipped with an inner product function

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

such that:

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

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

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

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

where the set $\{|i\rangle\}$ constitute an orthonormal basis of $\mathcal{H}$, $spec(A)$ denotes the set of eigenvalues of A, and E_i is the projector to the corresponding eigenspace of λ_i. A linear operator $A \in \mathcal{L}(\mathcal{H})$ is *unitary* if $A^\dagger A = A A^\dagger = I_\mathcal{H}$ where $I_\mathcal{H}$ is the identity operator on $\mathcal{H}$. In this article, we will use some well-known unitary operators listed as follows: the quantum control-not operator performed on two qubits with the matrix representation

$$CN = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

under the computational basis, and the 1-qubit Hadamard operator H and Pauli operators $\sigma^0, \sigma^1, \sigma^2, \sigma^3$ defined respectively as

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

$$\sigma^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ \sigma^3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

The *trace* of $A \in \mathcal{L}(\mathcal{H})$ is defined as $\mathrm{tr}(A) = \sum_i \langle i|A|i\rangle$ for some given orthonormal basis $\{|i\rangle\}$ of $\mathcal{H}$. It is worth noting that trace function is actually independent of the 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. Their *tensor product* $\mathcal{H}_1 \otimes \mathcal{H}_2$ is defined as a vector space consisting of linear combinations of the vectors $|\psi_1\psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$. Here the tensor product of two vectors is defined by a new vector such that

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

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

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

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

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

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

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* [Kraus 1983] of completely positive operators states that a linear operator $\mathcal{E}$ is completely positive if and only if there is some set of operators $\{E_i\}$ with appropriate dimension such that

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

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

2.2. Basic Quantum Mechanics

According to von Neumann's formalism of quantum mechanics [von Neumann 1955], an isolated physical system is associated with a Hilbert space which is called the *state space* of the system. A *pure state* of a quantum system is a normalized vector in its state space, and a *mixed state* is represented by a density operator on the state space. Here a density operator ρ on Hilbert space $\mathcal{H}$ is a positive linear operator such that $\mathrm{tr}(\rho) = 1$. Another equivalent representation of density operator is probabilistic ensemble of pure states. In particular, given an ensemble $\{(p_i, |\psi_i\rangle)\}$ where $p_i \geq 0$, $\sum_i p_i = 1$, and $|\psi_i\rangle$ are pure states, then $\rho = \sum_i p_i[|\psi_i\rangle]$ is a density operator. Here $[|\psi_i\rangle]$ denotes the abbreviation of $|\psi_i\rangle\langle\psi_i|$. Conversely, each density operator can be generated by an ensemble of pure states in this way. The set of density operators on $\mathcal{H}$ is defined as

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

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

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

which appears repeatedly in our examples of this article. This kind of state is called *entangled state*. To see the strangeness of entanglement, suppose a measurement $M = \lambda_0[|0\rangle] + \lambda_1[|1\rangle]$ is applied on the first qubit of $|\Psi\rangle$ (see the following for the definition of quantum measurements). Then after the measurement, the second qubit will definitely collapse into state $|0\rangle$ or $|1\rangle$ depending on whether the outcome λ_0 or λ_1 is observed. In other words, the measurement on the first qubit changes the state of the second qubit in some way. This is an outstanding feature of quantum mechanics which has no counterpart in the classical world, and is the key to many quantum information processing tasks such as teleportation [Bennett et al. 1993] and superdense coding [Bennett and Wiesner 1992].

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

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

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

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

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

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

its spectral decomposition. Obviously, the projectors $\{E_m : m \in spec(M)\}$ form a quantum measurement. If the state of a quantum system is ρ, then the probability

that result m occurs when measuring M on the system is $p(m) = \mathrm{tr}(E_m\rho)$, and the postmeasurement state of the system is $E_m\rho E_m/p(m)$. Note that for each outcome m, the map

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

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

Let M be a projective measurement with Eq. (1) its spectral decomposition. We call M nondegenerate if for any $m \in spec(M)$, the corresponding projector E_m is 1-dimensional; that is, all eigenvalues of M are nondegenerate. Nondegenerate measurement is obviously a very special case of general quantum measurement. However, when an ancilla system lying at a fixed state is provided, nondegenerate measurements together with unitary operators are sufficient to implement general measurements. For convenience of the readers, we elaborate the simulation process here. Suppose we are given a quantum system, which we call the principle system in the following, and want to perform a measurement $\{M_m\}$ on it. To do this, we introduce an ancilla system having an orthonormal basis $\{|m\rangle\}$ in one-to-one correspondence with the possible outcomes of the measurement. Let the fixed state of the ancilla system be $|0\rangle$. We define an operator U such that for any $|\psi\rangle$,

$$U|\psi\rangle|0\rangle = \sum_m M_m|\psi\rangle|m\rangle.$$

It is direct to check that U can be extended to a unitary operator which we also denote by U, from the completeness equation of $\{M_m\}$. Now we perform a nondegenerate projective measurement $M = \sum_m m|m\rangle\langle m|$ on the ancilla system. Let ρ be the state of the principle system before measurement, and $\sum_i p_i|\psi_i\rangle\langle\psi_i|$ be the spectral decomposition of ρ. Then for each i, $(I \otimes |m\rangle\langle m|)U|\psi_i\rangle|0\rangle = M_m|\psi_i\rangle|m\rangle$. Thus with probability

$$p(m) = \mathrm{tr}[(I \otimes |m\rangle\langle m|)U[\rho \otimes |0\rangle\langle 0|]U^\dagger] = \sum_i p_i\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \mathrm{tr}(M_m^\dagger M_m\rho)$$

the outcome m occurs, and the postmeasurement states of the principle-ancilla joint system and the principle system, when m is observed, are given by

$$\frac{(I \otimes |m\rangle\langle m|)U[\rho \otimes |0\rangle\langle 0|]U^\dagger(I \otimes |m\rangle\langle m|)}{\sqrt{p(m)}} = \frac{M_m\rho M_m^\dagger \otimes |m\rangle\langle m|}{\mathrm{tr}(M_m^\dagger M_m\rho)}$$

and $M_m\rho M_m^\dagger/\mathrm{tr}(M_m^\dagger M_m\rho)$, respectively, which coincide exactly with the case when the measurement $\{M_m\}$ is directly applied on the principle system.

We shall need a notion of distance between quantum states in defining approximate strong bisimulation between quantum processes. For any positive operator A, if $A = \sum_{\lambda_i \in spec(A)} \lambda_i E_i$ is a spectral decomposition of A, then we define

$$\sqrt{A} = \sum_{\lambda_i \in spec(A)} \sqrt{\lambda_i} E_i.$$

Furthermore, for any operator A, we set $|A| = \sqrt{A^\dagger A}$. Then the trace distance of $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ is defined to be

$$d(\rho, \sigma) = \frac{1}{2}\mathrm{tr}|\rho - \sigma|.$$

Trace distance is one of the most popular metrics used by the quantum information community. Here we collect some properties of the trace distance that are useful in this article.

THEOREM 2.1 [NIELSEN AND CHUANG 2000, THEOREM 9.1]. *Let* $\rho, \sigma \in \mathcal{D}(\mathcal{H})$. *Then*

$$d(\rho, \sigma) = \max_{\{M_i\}} d(\{p_i\}, \{q_i\})$$

where the maximization is over all quantum measurement $\{M_i\}$, *and* $p_i = \mathrm{tr}(\rho M_i^\dagger M_i)$ *and* $q_i = \mathrm{tr}(\sigma M_i^\dagger M_i)$ *are the probabilities of obtaining outcome i when the initial states are* ρ *and* σ, *respectively. The trace distance between two probabilistic distributions* $\{p_i\}$ *and* $\{q_i\}$ *is defined as* $d(\{p_i\}, \{q_i\}) = \frac{1}{2}\sum_i |p_i - q_i|$.

THEOREM 2.2 [NIELSEN AND CHUANG 2000, THEOREM 9.2]. *Let* $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, *and* $\mathcal{E}$ *a trace-preserving super-operator on* $\mathcal{H}$. *Then* $d[\mathcal{E}(\rho), \mathcal{E}(\sigma)] \leq d(\rho, \sigma)$.

The notion of trace distance can be extended to super-operators in a natural way [Kitaev 1997]. For any super-operators $\mathcal{E}_1$ and $\mathcal{E}_2$ on $\mathcal{H}$, their diamond trace distance is defined to be

$$d_\diamond(\mathcal{E}_1, \mathcal{E}_2) = \sup\{d[(\mathcal{E}_1 \otimes I_{\mathcal{H}'})(\rho), (\mathcal{E}_2 \otimes I_{\mathcal{H}'})(\rho)] : \rho \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H}')\},$$

where $\mathcal{H}'$ ranges over all finite-dimensional Hilbert spaces. The quantity $d_\diamond(\mathcal{E}_1, \mathcal{E}_2)$ characterizes the maximal probability that the outputs of $\mathcal{E}_1$ and $\mathcal{E}_2$ can be distinguished for the same input where auxiliary systems are allowed.

3. BASIC DEFINITIONS OF QCCS

In this section, we give the basic definitions of qCCS which is a combination of those proposed in Feng et al. [2007] and Ying et al. [2009], involving classical data as well as quantum data, and all classical process constructors (especially the recursive definition) as well as quantum primitives. The reader is referred to Feng et al. [2007] and Ying et al. [2009] for further examples and explanations of the language.

3.1. Syntax

We assume three types of data in qCCS: Bool for booleans, real numbers Real for classical data, and qubits Qbt for quantum data. Let $cVar$, ranged over by $x, y, \ldots$, be the set of classical variables, and $qVar$, ranged over by $q, r, \ldots$, the set of quantum variables. It is assumed that $cVar$ and $qVar$ are both countably infinite. We assume a set Exp of classical data expressions over `Real`, which includes $cVar$ as a subset and is ranged over by $e, e', \ldots$, and a set of boolean-valued expressions $BExp$, ranged over by $b, b', \ldots$, with the usual set of boolean operators **true**, **false**, $\neg$, $\wedge$, $\vee$, and $\rightarrow$. In particular, we let $e \bowtie e'$ be a boolean expression for any $e, e' \in Exp$ and $\bowtie \in \{>, <, \geq, \leq, =\}$. We further assume that only classical variables can occur free in both data expressions and boolean expressions. Let $cChan$ be the set of classical channel names, ranged over by $c, d, \ldots$, and $qChan$ the set of quantum channel names, ranged over by $\mathsf{c}, \mathsf{d}, \ldots$. 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 $f(qChan) \subseteq qChan$.

We often abbreviate the indexed set $\{q_1, \ldots, q_n\}$ to $\widetilde{q}$ when $q_1, \ldots, q_n$ are distinct quantum variables and the dimension n is understood. Sometimes we also use $\widetilde{q}$ to denote the string $q_1 \ldots q_n$. We assume a set of process constant schemes, ranged over by $A, B, \ldots$. Assigned to each process constant scheme A there is a nonnegative integer $ar(A)$. If $\widetilde{q}$ is a tuple of distinct quantum variables with $|\widetilde{q}| = ar(A)$, then $A(\widetilde{q})$ is called a process constant.

Based on these notations, we now propose the syntax of qCCS as follows.

Definition 3.1 (*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) $A(\widetilde{q}) \in qProc$, and $qv(A(\widetilde{q})) = \widetilde{q}$;
(3) $\tau.P \in qProc$, and $qv(\tau.P) = qv(P)$;
(4) $c?x.P \in qProc$, and $qv(c?x.P) = qv(P)$;
(5) $c!e.P \in qProc$, and $qv(c!e.P) = qv(P)$;
(6) $\mathsf{c}?q.P \in qProc$, and $qv(\mathsf{c}?q.P) = qv(P) - \{q\}$;
(7) If $q \notin qv(P)$ then $\mathsf{c}!q.P \in qProc$, and $qv(\mathsf{c}!q.P) = qv(P) \cup \{q\}$;
(8) $\mathcal{E}[\widetilde{q}].P \in qProc$, and $qv(\mathcal{E}[\widetilde{q}].P) = qv(P) \cup \widetilde{q}$;
(9) $M[\widetilde{q}; x].P \in qProc$, and $qv(M[\widetilde{q}; x].P) = qv(P) \cup \widetilde{q}$;
(10) $P + Q \in qProc$, and $qv(P + Q) = qv(P) \cup qv(Q)$;
(11) If $qv(P) \cap qv(Q) = \emptyset$ then $P \| Q \in qProc$, and $qv(P \| Q) = qv(P) \cup qv(Q)$;
(12) $P[f] \in qProc$, and $qv(P[f]) = qv(P)$;
(13) $P \backslash L \in qProc$, and $qv(P \backslash L) = qv(P)$;
(14) $\mathbf{if}\ b\ \mathbf{then}\ P \in qProc$, and $qv(\mathbf{if}\ b\ \mathbf{then}\ P) = qv(P)$,

where $P, Q \in qProc$, $c \in cChan$, $x \in cVar$, $\mathsf{c} \in qChan$, $q \in qVar$, $\widetilde{q} \subseteq qVar$, $e \in Exp$, τ is the silent action, $A(\widetilde{q})$ is a process constant, f is a relabeling function, $L \subseteq Chan$, $b \in BExp$, $\mathcal{E}$ and M are respectively a trace-preserving super-operator and a nondegenerate projective measurement applying on the Hilbert space associated with the systems $\widetilde{q}$. Furthermore, for each process constant $A(\widetilde{q})$, there is a defining equation

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

where $P \in qProc$ with $qv(P) \subseteq \widetilde{q}$. When $\widetilde{q} = \emptyset$, we simply denote $A(\widetilde{q})$ as A.

For the sake of simplicity, we only consider nondegenerate measurements in this article. This will not sacrifice the expressiveness of qCCS since as stated in Section 2, nondegenerate measurements can implement general quantum measurements with the help of unitary operators which, as special case of trace-preserving super-operators, can also be described in qCCS.

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

3.2. Operational Semantics

To present the operational semantics of qCCS, some further notations are necessary. For each quantum variable $q \in qVar$, we assume a 2-dimensional Hilbert space $\mathcal{H}_q$ to be the state space of the q-system. For any $S \subseteq qVar$, we denote

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

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

Suppose P is a closed quantum process. A pair of the form $\langle P, \rho \rangle$ is called a configuration, where $\rho \in \mathcal{D}(\mathcal{H})$ is a density operator on $\mathcal{H}$. The set of configurations is denoted by Con. We sometimes let $\mathcal{C}, \mathcal{D}, \ldots$ range over Con to ease notations.

$$\textbf{Tau}: \frac{}{\langle \tau.P, \rho\rangle \xrightarrow{\tau} \langle P, \rho\rangle}$$

$$\textbf{C-Inp}: \frac{}{\langle c?x.P, \rho\rangle \xrightarrow{c?v} \langle P\{v/x\}, \rho\rangle}, \quad v \in \mathsf{Real}$$

$$\textbf{C-Outp}: \frac{}{\langle c!e.P, \rho\rangle \xrightarrow{c!v} \langle P, \rho\rangle}, \quad v = [\![e]\!]$$

$$\textbf{C-Com}: \frac{\langle P_1, \rho\rangle \xrightarrow{c?v} \langle P_1', \rho\rangle, \quad \langle P_2, \rho\rangle \xrightarrow{c!v} \langle P_2', \rho\rangle}{\langle P_1 \| P_2, \rho\rangle \xrightarrow{\tau} \langle P_1' \| P_2', \rho\rangle}$$

$$\textbf{Q-Inp}: \frac{}{\langle \mathsf{c}?q.P, \rho\rangle \xrightarrow{\mathsf{c}?r} \langle P\{r/q\}, \rho\rangle}, \quad r \notin qv(\mathsf{c}?q.P)$$

$$\textbf{Q-Outp}: \frac{}{\langle \mathsf{c}!q.P, \rho\rangle \xrightarrow{\mathsf{c}!q} \langle P, \rho\rangle}$$

$$\textbf{Q-Com}: \frac{\langle P_1, \rho\rangle \xrightarrow{\mathsf{c}?r} \langle P_1', \rho\rangle, \quad \langle P_2, \rho\rangle \xrightarrow{\mathsf{c}!r} \langle P_2', \rho\rangle}{\langle P_1 \| P_2, \rho\rangle \xrightarrow{\tau} \langle P_1' \| P_2', \rho\rangle}$$

$$\textbf{Oper}: \frac{}{\langle \mathcal{E}[\widetilde{r}].P, \rho\rangle \xrightarrow{\tau} \langle P, \mathcal{E}_{\widetilde{r}}(\rho)\rangle}$$

$$\textbf{Meas}: \frac{}{\langle M[\widetilde{r}; x].P, \rho\rangle \xrightarrow{\tau} \sum_{i\in I} p_i \langle P\{\lambda_i/x\}, E^i_{\widetilde{r}} \rho E^{i\dagger}_{\widetilde{r}}/p_i\rangle}$$

where M has the spectral decomposition $M = \sum_{i\in I} \lambda_i E^i$ and $p_i = \mathrm{tr}(E^{i\dagger}_{\widetilde{r}} \rho)$

Fig. 1. Inference rules for qCCS (Part 1).

Let $D(Con)$ be the set of finite-support probability distributions over Con; that is,

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

For any $\mu \in D(Con)$, we denote by $supp(\mu)$ the support set of μ, that is, 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 $\mathcal{C}$. Sometimes we find it convenient to denote a distribution μ 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 $\mathcal{C}_i$ are distinct configurations, $supp(\mu) = \{\mathcal{C}_i : i \in I\}$, 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 μ such that $supp(\mu) = \bigcup_i supp(\mu_i)$, and for any $\mathcal{D} \in supp(\mu)$, $\mu(\mathcal{D}) = \sum_i p_i \mu_i(\mathcal{D})$.

It is worth pointing out the difference between the two notations $\boxplus_{i\in I} p_i \bullet \mathcal{C}_i$ and $\sum_{i\in I} p_i \mathcal{C}_i$: the former is the explicit form of a distribution, so it is required that $p_i > 0$ for each $i \in I$, and $\mathcal{C}_i \neq \mathcal{C}_j$ for $i \neq j$; while the latter is the combined distribution of the simple distributions $\mathcal{C}_i$ with the probability weights p_i, so p_i may be zero for some $i \in I$, and $\mathcal{C}_i$s are not necessarily distinct.

$$\textbf{Inp-Int}: \frac{\langle P_1,\rho\rangle \xrightarrow{\mathsf{c}?r} \langle P_1',\rho\rangle}{\langle P_1\|P_2,\rho\rangle \xrightarrow{\mathsf{c}?r} \langle P_1'\|P_2,\rho\rangle}, \quad r\notin qv(P_2)$$

$$\textbf{Oth-Int}: \frac{\langle P_1,\rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i',\rho_i\rangle}{\langle P_1\|P_2,\rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i'\|P_2,\rho_i\rangle}, \quad \alpha\neq \mathsf{c}?r$$

$$\textbf{Sum}: \frac{\langle P,\rho\rangle \xrightarrow{\alpha} \mu}{\langle P+Q,\rho\rangle \xrightarrow{\alpha} \mu}$$

$$\textbf{Rel}: \frac{\langle P,\rho\rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle P_i,\rho_i\rangle}{\langle P[f],\rho\rangle \xrightarrow{f(\alpha)} \boxplus p_i \bullet \langle P_i[f],\rho_i\rangle}$$

$$\textbf{Res}: \frac{\langle P,\rho\rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle P_i,\rho_i\rangle}{\langle P\backslash L,\rho\rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle P_i\backslash L,\rho_i\rangle}, \quad cn(\alpha)\not\subseteq L$$

$$\textbf{Cho}: \frac{\langle P,\rho\rangle \xrightarrow{\alpha} \mu}{\langle \textbf{if } b \textbf{ then } P,\rho\rangle \xrightarrow{\alpha} \mu}, \quad [\![b]\!]=\text{true}$$

$$\textbf{Def}: \frac{\langle P\{\widetilde{r}/\widetilde{q}\},\rho\rangle \xrightarrow{\alpha} \mu}{\langle A(\widetilde{r}),\rho\rangle \xrightarrow{\alpha} \mu}, \quad A(\widetilde{q}) \stackrel{def}{=} P$$

Fig. 2. Inference rules for qCCS (Part 2).

Let $\mu = \boxplus_{i\in I} p_i \bullet \langle P_i, \rho_i\rangle$. We denote by $qv(\mu)$ the free variables of μ; that is, $qv(\mu) = \bigcup_{i\in I} qv(P_i)$. We write $\mathrm{tr}(\mu) = \sum_{i\in I} p_i \mathrm{tr}(\rho_i)$, and $\mathcal{E}(\mu) = \boxplus_{i\in I} p_i \bullet \langle P_i, \mathcal{E}(\rho_i)\rangle$ when $\mathcal{E}$ is a super-operator.

Let

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

For each $\alpha \in Act$, we define the bound quantum variables $bv(\alpha)$ of α as $bv(\mathsf{c}?r) = \{r\}$ and $bv(\alpha) = \emptyset$ if α is not a quantum input. The channel names used in action α is denoted by $cn(\alpha)$; that is, $cn(c?v) = cn(c!v) = \{c\}$, $cn(\mathsf{c}?r) = cn(\mathsf{c}!r) = \{\mathsf{c}\}$, and $cn(\tau) = \emptyset$.

The semantics of qCCS is given by the probabilistic labeled transition system $(Con, Act, \longrightarrow)$, where $\longrightarrow \subseteq Con \times Act \times D(Con)$ is the smallest relation satisfying the rules defined in Figures 1 and 2 (for brevity, we write $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ instead of $(\langle P, \rho\rangle, \alpha, \mu) \in \longrightarrow$. The symmetric forms for Rules **Inp-Int**, **Oth-Int**, and **Sum** are omitted).

The transition relation $\longrightarrow$ can be lifted to $D(Con)\times Act\times D(Con)$ by writing $\mu \xrightarrow{\alpha} \nu$ if for any $\mathcal{C} \in supp(\mu)$, $\mathcal{C} \xrightarrow{\alpha} \nu_{\mathcal{C}}$ for some $\nu_{\mathcal{C}}$, and $\nu = \sum_{\mathcal{C}\in supp(\mu)} \mu(\mathcal{C})\nu_{\mathcal{C}}$.

For any $S \subseteq qVar$ we denote by $\overline{S}$ the complement set of S in $qVar$. The following lemmas can be easily observed from the inference rules defined previously.

LEMMA 3.2. *If* $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$, *then* $qv(\mu) \subseteq qv(P) \cup bv(\alpha)$.

PROOF. By induction on the inference rules. □

LEMMA 3.3. *If* $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$, *then:*

(1) $\mathrm{tr}(\rho) = \mathrm{tr}(\mu)$;
(2) there exist a set of trace-preserving super-operators $\{\mathcal{E}_i : i \in I\}$ *and a set of projectors* $\{E_i : i \in I\}$, *both acting on* $\mathcal{H}_{qv(P)}$ *and* $\sum_{i\in I} E_i = I$, *such that for any* $\sigma \in \mathcal{D}(\mathcal{H})$,

$$\langle P, \sigma\rangle \xrightarrow{\alpha} \sum_{i\in I} q_i^\sigma \langle P_i, \mathcal{E}_i(\sigma)\rangle$$

where $q_i^\sigma = \mathrm{tr}(E_i\sigma)$;
(3) for any trace-preserving super-operator $\mathcal{E}$ *acting on* $\mathcal{H}_{\overline{qv(P)}}$, $\langle P, \mathcal{E}(\rho)\rangle \xrightarrow{\alpha} \mathcal{E}(\mu)$.

PROOF. By induction on the inference rules. The only case deserving an explanation is for (2) when the action is caused by a measurement prefix $M[\widetilde{q}; x]$. Since only nondegenerate projective measurements are considered in qCCS, we can suppose that $M = \sum_{i\in I} \lambda_i |\psi_i\rangle\langle\psi_i|$ for some orthonormal basis $\{|\psi_i\}$ in the state space of $\widetilde{q}$. Then from the inference rule **Meas**, we have

$$\langle P, \sigma\rangle \xrightarrow{\alpha} \sum_{i\in I} \mathrm{tr}(|\psi_i\rangle\langle\psi_i|\sigma)\langle P\{\lambda_i/x\}, |\psi_i\rangle\langle\psi_i|_{\widetilde{q}} \otimes \sigma'\rangle,$$

where $\sigma' = \mathrm{tr}_{\widetilde{q}}(\sigma)$. By letting $\mathcal{E}_i$ be the trace-preserving super-operator which sets the quantum systems $\widetilde{q}$ to $|\psi_i\rangle$, $E_i = |\psi_i\rangle\langle\psi_i|$, and $P_i = P\{\lambda_i/x\}$, the result follows. □

3.3. Examples

To illustrate the expressiveness of qCCS, we give some examples.

Example 3.4. Superdense coding [Bennett and Wiesner 1992] is a quantum protocol using which two bits of classical information can be faithfully transmitted by sending only one qubit, provided that a maximally entangled state is shared a priori between sender and receiver. The protocol goes as follows. Let $|\Psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ be the entangled state shared between the sender Alice and the receiver Bob. Alice applies a Pauli operator on her qubit of $|\Psi\rangle$ according to which information among the four possibilities she wishes to transmit, and sends her qubit to Bob. With the two qubits in hand, Bob performs a perfect discrimination among the possible states (they are actually the four Bell states $\{\sigma^i \otimes I|\Psi\rangle : i = 0, 1, 2, 3\}$ where σ^i are defined in Section 2) and retrieves the information Alice has sent.

We now show how to describe the protocol of superdense coding with qCCS. Let M be a 2-qubit measurement such that $M = \sum_{i=0}^{3} i|\tilde{i}\rangle\langle\tilde{i}|$, where $\tilde{i}$ is the binary expansion of i. Let CN be the controlled-not operator and H Hadamard operator. Then the quantum processes participated in superdense coding protocol can be defined as follows.

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

For any $\rho \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}})$ and $v \in \{0,1,2,3\}$, we have the transitions

$$\begin{aligned}
&\langle Sdc, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{c?v} &\left\langle \left(\left(\sum_{0\le i\le 3} (\mathbf{if}\ v = i\ \mathbf{then}\ \sigma^i[q_1].\mathsf{e}!q_1.\mathbf{nil}) \right) \| Bob_s \right) \backslash \{\mathsf{e}\}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho \right\rangle \\
\xrightarrow{\tau} &\langle (\mathsf{e}!q_1.\mathbf{nil} \| Bob_s) \backslash \{\mathsf{e}\}, \sigma^v_{q_1}([|\Psi\rangle]) \otimes \rho\rangle \\
\xrightarrow{\tau} &\langle (\mathbf{nil} \| CN[q_1,q_2].H[q_1].M[q_1,q_2;x].d!x.\mathbf{nil}) \backslash \{\mathsf{e}\}, \sigma^v_{q_1}([|\Psi\rangle]) \otimes \rho\rangle \\
\xrightarrow{\tau} &\langle (\mathbf{nil} \| H[q_1].M[q_1,q_2;x].d!x.\mathbf{nil}) \backslash \{\mathsf{e}\}, CN_{q_1,q_2}(\sigma^v_{q_1}([|\Psi\rangle])) \otimes \rho\rangle \\
\xrightarrow{\tau} &\langle (\mathbf{nil} \| M[q_1,q_2;x].d!x.\mathbf{nil}) \backslash \{\mathsf{e}\}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle \qquad (2) \\
\xrightarrow{\tau} &\langle (\mathbf{nil} \| d!v.\mathbf{nil}) \backslash \{\mathsf{e}\}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{d!v} &\langle (\mathbf{nil} \| \mathbf{nil}) \backslash \{\mathsf{e}\}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle.
\end{aligned}$$

Here Eq. (2) is calculated as follows.

$$H_{q_1}\left(CN_{q_1,q_2}\left(\sigma^v_{q_1}([|\Psi\rangle])\right)\right) = \begin{cases} H_{q_1}\left(CN_{q_1,q_2}\left(\left[\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right]\right)\right) = [|00\rangle], \text{ if } v = 0 \\ H_{q_1}\left(CN_{q_1,q_2}\left(\left[\frac{|10\rangle+|01\rangle}{\sqrt{2}}\right]\right)\right) = [|01\rangle], \text{ if } v = 1 \\ H_{q_1}\left(CN_{q_1,q_2}\left(\left[\frac{|00\rangle-|11\rangle}{\sqrt{2}}\right]\right)\right) = [|10\rangle], \text{ if } v = 2 \\ H_{q_1}\left(CN_{q_1,q_2}\left(\left[\frac{|01\rangle-|10\rangle}{\sqrt{2}}\right]\right)\right) = [|11\rangle], \text{ if } v = 3 \end{cases}$$

Example 3.5. Quantum teleportation [Bennett et al. 1993] is one of the most important protocols in quantum information theory which can make use of a maximally entangled state shared between sender and receiver to teleport an unknown quantum state by sending only classical information. It serves as a key ingredient in many other communication protocols. The protocol goes as follows. Let $|\Psi\rangle_{q_1,q_2}$ be the entanglement state shared between the sender Alice and the receiver Bob, with Alice holding q_1 and Bob holding q_2. Let q be the quantum system whose state Alice wants to transmit to Bob. Alice first applies a quantum control-not operations on q and q_1, with q the control qubit and q_1 the target, followed by a Hadamard operator H on q. She then measures q and q_1 according to the computational basis, and sends the measurement outcome to Bob. Upon receiving the classical bits from Alice, Bob applies a corresponding Pauli operator on his qubit q_2 to recover the original state of q.

Let M, CN, H, and σ^i, $i = 0, \ldots, 3$ be as defined in Example 3.4. Then the quantum processes participated in teleportation protocol can be defined as follows.

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

For any $\rho \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}})$, we have

$$
\begin{aligned}
& \langle \mathit{Tel}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{\mathsf{c}?r} \ & \langle (CN[r,q_1].H[r].M[r,q_1;x].e!x.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{\tau} \ & \langle (H[r].M[r,q_1;x].e!x.\mathbf{nil} \| Bob_t)\backslash\{e\}, CN_{r,q_1}([|\Psi\rangle]_{q_1,q_2} \otimes \rho)\rangle \\
\xrightarrow{\tau} \ & \langle (M[r,q_1;x].e!x.\mathbf{nil} \| Bob_t)\backslash\{e\}, \sum_{0\le j\le 3} \frac{1}{4}[|\widetilde{j}\rangle]_{r,q_1} \otimes \sigma^j_{q_2}(\rho)\rangle \qquad (3) \\
\xrightarrow{\tau} \ & 1/4 \bullet \langle (e!0.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|00\rangle]_{r,q_1} \otimes \rho\rangle \\
& \boxplus 1/4 \bullet \langle (e!1.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|01\rangle]_{r,q_1} \otimes \sigma^1_{q_2}(\rho)\rangle \\
& \boxplus 1/4 \bullet \langle (e!2.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|10\rangle]_{r,q_1} \otimes \sigma^2_{q_2}(\rho)\rangle \\
& \boxplus 1/4 \bullet \langle (e!3.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|11\rangle]_{r,q_1} \otimes \sigma^3_{q_2}(\rho)\rangle,
\end{aligned}
$$

and for $0 \le j \le 3$,

$$
\begin{aligned}
& \left\langle (e.j.\mathbf{nil} \| Bob_t)\backslash\{e\}, \left[|\widetilde{j}\rangle\right]_{r,q_1} \otimes \sigma^j_{q_2}(\rho)\right\rangle \\
\xrightarrow{\tau} \ & \left\langle \left(\mathbf{nil} \| \sum_{0\le i\le 3} (\mathbf{if}\ j = i\ \mathbf{then}\ \sigma^i[q_2].\mathsf{d}!q_2.\mathbf{nil})\right)\backslash\{e\}, [|\widetilde{j}\rangle]_{r,q_1} \otimes \sigma^j_{q_2}(\rho)\right\rangle \\
\xrightarrow{\tau} \ & \left\langle (\mathbf{nil} \| \mathsf{d}!q_2.\mathbf{nil})\backslash\{e\}, \left[|\widetilde{j}\rangle\right]_{r,q_1} \otimes \rho\right\rangle \\
\xrightarrow{\mathsf{d}!q_2} \ & \left\langle (\mathbf{nil} \| \mathbf{nil})\backslash\{e\}, \left[|\widetilde{j}\rangle\right]_{r,q_1} \otimes \rho\right\rangle.
\end{aligned}
$$

Here Eq. (3) is calculated as follows. Notice that any $\rho \in \mathcal{D}\left(\mathcal{H}_{\overline{\{q_1,q_2\}}}\right)$ can be decomposed as $\rho = \sum_{0\le i\le 3} \gamma_i [|\psi_i\rangle]_r \otimes \rho_i$ where $|\psi_0\rangle = |0\rangle$, $|\psi_1\rangle = |1\rangle$, $|\psi_2\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and $|\psi_3\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Then it is easy to derive that

$$
\begin{aligned}
H_r(CN_{r,q_1}([|\Psi\rangle]_{q_1,q_2} \otimes \rho)) \ = \ & \frac{\gamma_0}{4}[|000\rangle + |011\rangle + |100\rangle + |111\rangle]_{r,q_1,q_2} \otimes \rho_0 \\
& + \frac{\gamma_1}{4}[|001\rangle + |010\rangle - |101\rangle - |110\rangle]_{r,q_1,q_2} \otimes \rho_1 \\
& + \frac{\gamma_2}{4}[|00+\rangle + |01+\rangle + |10-\rangle - |11-\rangle]_{r,q_1,q_2} \otimes \rho_2 \\
& + \frac{\gamma_3}{4}[|00-\rangle - |01-\rangle + |10+\rangle + |11+\rangle]_{r,q_1,q_2} \otimes \rho_3 \\
= \ & \frac{1}{4}[|00\rangle]_{r,q_1} \otimes \rho + \frac{1}{4}[|01\rangle]_{r,q_1} \otimes \sigma^1_{q_2}(\rho) \\
& + \frac{1}{4}[|10\rangle]_{r,q_1} \otimes \sigma^2_{q_2}(\rho) + \frac{1}{4}[|11\rangle]_{r,q_1} \otimes \sigma^3_{q_2}(\rho).
\end{aligned}
$$

Example 3.6 (*Encode Quantum Circuits with qCCS*). Quantum circuits consist of two different types of gates: unitary gates and quantum measurements. We now show how to encode them using qCCS. To ease the notations, we allow quantum channels to input and output multiple qubits. We write the quantum channel c as c^n if n qubits can be communicated through c simultaneously. In other words, the quantum capacity of c^n is n qubits.

— Unitary gate. Suppose U is a unitary operator acting on n qubits. Then the unitary gate which implements U can be defined as a process constant $\mathcal{U}(U)$, $qv(\mathcal{U}(U)) = \emptyset$, with the defining equation

$$\mathcal{U}(U) \stackrel{def}{=} \mathsf{c}^n?\widetilde{q}.U[\widetilde{q}].\mathsf{d}^n!\widetilde{q}.\mathcal{U}(U).$$

We set $ar(\mathcal{U}(U)) = n$.

— Measurement gate. Suppose M is a quantum measurement acting on n qubits. Then the measurement gate which implements M can be defined as

$$\mathcal{M}(M) \stackrel{def}{=} \mathsf{c}^n?\widetilde{q}.M[\widetilde{q};x].e!x.\mathsf{d}^n!\widetilde{q}.\mathcal{M}(M).$$

We set $ar(\mathcal{M}(M)) = n$.

For any $\rho \in \mathcal{D}(\mathcal{H})$, we have

$$\begin{aligned}\langle \mathcal{U}(U), \rho\rangle &\stackrel{\mathsf{c}^n?\widetilde{r}}{\longrightarrow} \langle U[\widetilde{r}].\mathsf{d}^n!\widetilde{r}.\mathcal{U}(U), \rho\rangle\\ &\stackrel{\tau}{\longrightarrow} \langle \mathsf{d}^n!\widetilde{r}.\mathcal{U}(U), U_{\widetilde{r}}\rho U_{\widetilde{r}}^\dagger\rangle\\ &\stackrel{\mathsf{d}^n!\widetilde{r}}{\longrightarrow} \langle \mathcal{U}(U), U_{\widetilde{r}}\rho U_{\widetilde{r}}^\dagger\rangle\end{aligned}$$

and

$$\begin{aligned}\langle \mathcal{M}(M), \rho\rangle &\stackrel{\mathsf{c}^n?\widetilde{r}}{\longrightarrow} \langle M[\widetilde{r};x].e!x.\mathsf{d}^n!\widetilde{r}.\mathcal{M}(M), \rho\rangle\\ &\stackrel{\tau}{\longrightarrow} \boxplus_{i\in I} p_i \bullet \langle e!\lambda_i.\mathsf{d}^n!\widetilde{r}.\mathcal{M}(M), E_{\widetilde{r}}^i\rho E_{\widetilde{r}}^i/p_i\rangle\end{aligned}$$

where $M = \sum_{i\in I}\lambda_i E^i$ and $p_i = \mathrm{tr}(E_{\widetilde{r}}^i\rho)/\mathrm{tr}(\rho)$. Now for each $i \in I$,

$$\begin{aligned}\langle e!\lambda_i.\mathsf{d}^n!\widetilde{r}.\mathcal{M}(M), E_{\widetilde{r}}^i\rho E_{\widetilde{r}}^i/p_i\rangle &\stackrel{e!\lambda_i}{\longrightarrow} \langle \mathsf{d}^n!\widetilde{r}.\mathcal{M}(M), E_{\widetilde{r}}^i\rho E_{\widetilde{r}}^i/p_i\rangle\\ &\stackrel{\mathsf{d}^n!\widetilde{r}}{\longrightarrow} \langle \mathcal{M}(M), E_{\widetilde{r}}^i\rho E_{\widetilde{r}}^i/p_i\rangle.\end{aligned}$$

Suppose $\mathcal{G}_1$ and $\mathcal{G}_2$ are two (unitary or measurement) gates with $ar(\mathcal{G}_1) = ar(\mathcal{G}_2) = n$. The sequential composition of $\mathcal{G}_1$ and $\mathcal{G}_2$ can be defined as

$$\mathcal{G}_1 \circ \mathcal{G}_2 \stackrel{def}{=} (L_s \| \mathcal{G}_1[\mathsf{e}^n/\mathsf{c}^n, \mathsf{f}^n/\mathsf{d}^n] \| \mathcal{G}_2[\mathsf{f}^n/\mathsf{c}^n, \mathsf{g}^n/\mathsf{d}^n] \| R_s)\backslash\{c, \mathsf{e}^n, \mathsf{f}^n, \mathsf{g}^n\},$$

where $L_s \stackrel{def}{=} \mathsf{c}^n?\widetilde{q}.\mathsf{e}^n!\widetilde{q}.c?x.L_s$ and $R_s \stackrel{def}{=} \mathsf{g}^n?\widetilde{q}.\mathsf{d}^n!\widetilde{q}.c!0.R_s$.

If $ar(\mathcal{G}_1) = m$ and $ar(\mathcal{G}_2) = n$, then the parallel composition of $\mathcal{G}_1$ and $\mathcal{G}_2$ is defined as

$$\mathcal{G}_1 \otimes \mathcal{G}_2 \stackrel{def}{=} (L_p \| \mathcal{G}_1[\mathsf{e}_1^m/\mathsf{c}^m, \mathsf{f}_1^m/\mathsf{d}^m] \| \mathcal{G}_2[\mathsf{e}_2^n/\mathsf{c}^n, \mathsf{f}_2^n/\mathsf{d}^n] \| R_p)\backslash\{c, \mathsf{e}_1^m, \mathsf{f}_1^m, \mathsf{e}_2^n, \mathsf{f}_2^n\},$$

where $L_p \stackrel{def}{=} \mathsf{c}^{m+n}?\widetilde{q}.\mathsf{e}_1^m!l(\widetilde{q}).\mathsf{e}_2^n!r(\widetilde{q}).c?x.L_p$, $R_p \stackrel{def}{=} \mathsf{f}_1^m?\widetilde{r_1}.\mathsf{f}_2^n?\widetilde{r_2}.\mathsf{d}^{m+n}!(\widetilde{r_1}\widetilde{r_2}).c!0.R_p$, $l(\widetilde{q})$ denotes the prefix of $\widetilde{q}$ with length m while $r(\widetilde{q})$ the postfix of $\widetilde{q}$ with length n, and $\widetilde{r_1}\widetilde{r_2}$ is the concatenation of $\widetilde{r_1}$ and $\widetilde{r_2}$.

4. STRONG BISIMULATION BETWEEN QUANTUM PROCESSES

This section is devoted to a strong bisimulation between quantum processes. Firstly, we need a definition from Baier and Kwiatkowska [2000] which lifts a relation on Con to a relation on $D(Con)$.

Definition 4.1. Let $\mathcal{R} \subseteq Con \times Con$, and $\mu, \nu \in D(Con)$. A weight function for (μ, ν) with respect to $\mathcal{R}$ is a function $\delta : supp(\mu) \times supp(\nu) \to [0, 1]$ which satisfies

(1) For all $\mathcal{C} \in supp(\mu)$ and $\mathcal{D} \in supp(\nu)$,

$$\sum_{\mathcal{D} \in supp(\nu)} \delta(\mathcal{C}, \mathcal{D}) = \mu(\mathcal{C}), \qquad \sum_{\mathcal{C} \in supp(\mu)} \delta(\mathcal{C}, \mathcal{D}) = \nu(\mathcal{D});$$

(2) If $\delta(\mathcal{C}, \mathcal{D}) > 0$, then $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$.

We write $\mu \mathcal{R} \nu$ if there exists a weight function for (μ, ν) with respect to $\mathcal{R}$.

LEMMA 4.2 [BAIER AND KWIATKOWSKA 2000]. *Suppose $\mu, \nu, \omega \in D(Con)$, $\mathcal{R}, \mathcal{R}' \subseteq Con \times Con$.*

(1) $\mu \mathcal{R} \nu$ if and only if $\nu \mathcal{R}^{-1} \mu$.
(2) If $\mu \mathcal{R} \nu$ and $\nu \mathcal{R}' \omega$, then $\mu (\mathcal{R} \circ \mathcal{R}') \omega$.
(3) If $\mathcal{R} \subseteq \mathcal{R}'$, then $\mu \mathcal{R} \nu$ implies $\mu \mathcal{R}' \nu$.

The following lemma gives an equivalent characterization of the lifted relation on $D(Con)$ directly from the original one on Con, without resorting to a weight function:[1]

LEMMA 4.3. *Let $\mu, \nu \in D(Con)$ and $\mathcal{R} \subseteq Con \times Con$. Then $\mu \mathcal{R} \nu$ if and only if $\mu = \sum_{i \in I} p_i \mathcal{C}_i$ and $\nu = \sum_{i \in I} p_i \mathcal{D}_i$ such that $\mathcal{C}_i \mathcal{R} \mathcal{D}_i$ for each $i \in I$. In particular, if $\mathcal{C} \mathcal{R} \nu$ then $\mathcal{C} \mathcal{R} \mathcal{D}$ for each $\mathcal{D} \in supp(\nu)$.*

PROOF. This is simply a special case of Lemma 5.2 presented in Section 5. □

With the notion of lifted relations, we can define strong bisimulation between configurations as follows.

Definition 4.4. A relation $\mathcal{R} \subseteq Con \times Con$ is called a strong bisimulation if for any $\langle P, \rho \rangle, \langle \boldsymbol{Q}, \sigma \rangle \in Con$, $\langle P, \rho \rangle \mathcal{R} \langle \boldsymbol{Q}, \sigma \rangle$ implies that $q\nu(P) = q\nu(\boldsymbol{Q})$, $\mathrm{tr}_{q\nu(P)}(\rho) = \mathrm{tr}_{q\nu(\boldsymbol{Q})}(\sigma)$, and:

(1) whenever $\langle P, \rho \rangle \xrightarrow{\mathsf{c?}q} \langle P', \rho \rangle$, then $\langle \boldsymbol{Q}, \sigma \rangle \xrightarrow{\mathsf{c?}q} \langle \boldsymbol{Q}', \sigma \rangle$ for some $\boldsymbol{Q}'$ such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{q\nu(P') - \{q\}}}$, $\langle P', \mathcal{E}(\rho) \rangle \mathcal{R} \langle \boldsymbol{Q}', \mathcal{E}(\sigma) \rangle$;
(2) whenever $\langle P, \rho \rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle \boldsymbol{Q}, \sigma \rangle \xrightarrow{\alpha} \nu$ and $\mu \mathcal{R} \nu$;
(3) whenever $\langle \boldsymbol{Q}, \sigma \rangle \xrightarrow{\mathsf{c?}q} \langle \boldsymbol{Q}', \sigma \rangle$, then $\langle P, \rho \rangle \xrightarrow{\mathsf{c?}q} \langle P', \rho \rangle$ for some P' such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{q\nu(\boldsymbol{Q}') - \{q\}}}$, $\langle P', \mathcal{E}(\rho) \rangle \mathcal{R} \langle \boldsymbol{Q}', \mathcal{E}(\sigma) \rangle$;
(4) whenever $\langle \boldsymbol{Q}, \sigma \rangle \xrightarrow{\alpha} \nu$ where α is not a quantum input, then there exists μ such that $\langle P, \rho \rangle \xrightarrow{\alpha} \mu$ and $\mu \mathcal{R} \nu$.

Then the strong bisimilarity between configurations is the largest strong bisimulation, and strong bisimilarity between processes can be defined by comparing two processes in the same environment.

Definition 4.5.

(1) Two quantum configurations $\langle P, \rho \rangle$ and $\langle \boldsymbol{Q}, \sigma \rangle$ are strongly bisimilar, denoted by $\langle P, \rho \rangle \sim \langle \boldsymbol{Q}, \sigma \rangle$, if there exists a strong bisimulation $\mathcal{R}$ such that $\langle P, \rho \rangle \mathcal{R} \langle \boldsymbol{Q}, \sigma \rangle$.

[1]While completing this article, we were aware of that the same equivalent characterization was established independently by Yuxin Deng and Wenjie Du in Deng and Du [2011]. They actually adopted Lemma 4.3 as the definition of lifted relations, and treated the weight function approach in Definition 4.1 as a property.

(2) Two quantum processes P and Q are strongly bisimilar, denoted by $P \sim Q$, if for any quantum state $\rho \in \mathcal{D}(\mathcal{H})$ and any indexed set $\widetilde{v}$ of classical values, $\langle P\{\widetilde{v}/\widetilde{x}\}, \rho\rangle \sim \langle Q\{\widetilde{v}/\widetilde{x}\}, \rho\rangle$. Here $\widetilde{x}$ is the set of free classical variables contained in P and Q.

Some design decisions made in Definition 4.4 deserve justification and explanation.

— Recall that in the definition of bisimulations proposed in Feng et al. [2007], a clause

$$\text{If } \langle P, \rho\rangle \not\longrightarrow \text{ and } \langle Q, \sigma\rangle \not\longrightarrow, \text{ then } \rho = \sigma \tag{4}$$

is presented to guarantee that the quantum operations applied by P and Q, which give rise only to invisible actions, have the same effect. That definition, however, does not fit well with recursive definitions since recursively defined processes will generally never reach a terminating process.
In Definition 4.4, we solve this problem by requiring instead that

$$\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma). \tag{5}$$

Obviously, when $\langle P, \rho\rangle \not\longrightarrow$ and $\langle Q, \sigma\rangle \not\longrightarrow$, and P and Q do not hold any quantum variables, Eqs. (4) and (5) are equivalent. However, Eq. (5) can deal with processes which have infinite behaviors. For example, let

$$A \stackrel{def}{=} \mathsf{c}?q.Set_0[q].\tau.\mathsf{c}!q.A$$

and

$$B \stackrel{def}{=} \mathsf{c}?q.M_{0,1}[q;x].\sum_{i=0}^{1}(\textbf{if } x = \lambda_i \textbf{ then } \sigma^i[q].\mathsf{c}!q.B),$$

where Set_0 is the trace-preserving super-operator which sets the target qubit to $|0\rangle$, and $M_{0,1}$ is the 1-qubit measurement according to the computational basis; that is, $M_{0,1} = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$. Intuitively, B can be regarded as an implementation of A, specifying how to set the input qubit to $|0\rangle$. We now show $A \sim B$ indeed holds under our definition of strong bisimulation. Let

$$Con_\rho = \{\langle A, \rho\rangle, \langle B, \rho\rangle\}$$
$$Con_{q,\rho} = \{\langle A_{1q}, \rho\rangle, \langle A_{2q}, \rho_0\rangle, \langle A_{3q}, \rho_0\rangle, \langle B_{1q}, \rho\rangle, \langle B_{2qj}, \rho_j\rangle, \langle B_{3q}, \rho_0\rangle : j = 0, 1\}$$

where $A_{1q} = Set_0[q].\tau.\mathsf{c}!q.A$, $A_{2q} = \tau.\mathsf{c}!q.A$, $A_{3q} = \mathsf{c}!q.A$,

$$B_{1q} = M_{0,1}[q;x].\sum_{i=0}^{1}(\textbf{if } x = \lambda_i \textbf{ then } \sigma^i[q].\mathsf{c}!q.B),$$

$$B_{2qj} = \sum_{i=0}^{1}(\textbf{if } \lambda_j = \lambda_i \textbf{ then } \sigma^i[q].\mathsf{c}!q.B),$$

$B_{3q} = \mathsf{c}!q.B$, and $\rho_j = [|j\rangle]_q \otimes \mathrm{tr}_q\rho$. Let $\mathcal{R} \subseteq Con \times Con$ such that $\langle P, \sigma\rangle\mathcal{R}\langle Q, \eta\rangle$ if and only if there exist $q \in qVar$ and $\rho \in \mathcal{D}(\mathcal{H})$ such that $\langle P, \sigma\rangle$ and $\langle Q, \eta\rangle$ are simultaneously included in Con_ρ or $Con_{q,\rho}$. It is not difficult to prove that $\mathcal{R}$ is a strong bisimulation. Thus $A \sim B$.

— Furthermore, by replacing Eq. (4) with Eq. (5), the derived bisimilarity will be preserved by restriction. Take the example in Feng et al. [2007]. Let U_1, U_2, V_1, and V_2 be unitary operators such that $U_2U_1 = V_2V_1$ but $U_1 \neq V_1$. Let

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

Then P and Q are strongly bisimilar but $P\backslash\{c\}$ and $Q\backslash\{c\}$ are not if Eq. (4) is required in the definition. However, in our Definition 4.4, $P\backslash\{c\}$ and $Q\backslash\{c\}$ are also strongly bisimilar since in Eq. (5) we only need to consider the reduced states on the

systems $\overline{qv(P)} = \overline{qv(Q)}$. The "unfinished" quantum operations, which are blocked by the restriction, are not taken into account when comparing the accompanying quantum states.

— Another question one may ask is that why we require $qv(P) = qv(Q)$ in the definition, which excludes the pair

$$P = I[q].\mathbf{nil} \quad \text{and} \quad Q = \tau.\mathbf{nil}$$

to be strongly bisimilar. The reason is, although P and Q have the same effect (they both do nothing at all) on the environment, they are indeed different under parallel composition. For example, if $q \in qv(R)$, then the process $Q \| R$ is valid while $P \| R$ is not.

— In clause (1), we require $\langle P', \mathcal{E}(\rho)\rangle \mathcal{R} \langle Q', \mathcal{E}(\sigma)\rangle$ for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$. The reason for this rather strange requirement is as follows. To check whether two configurations are bisimilar, we have to feed them with all possible inputs. In classical process algebra, this is realized by requiring that the input value is arbitrarily chosen. In quantum process algebra, however, since the state of all environmental systems is fixed for a given configuration, only requiring the arbitrariness of the input system is not sufficient. Note that the state preparation operation and the swap operation are both special trace-preserving super-operators. Our definition actually allows the possibility of inputing an arbitrary system which lies in an arbitrary state. Furthermore, this requirement is also essential in proving the congruence property of the derived bisimilarity (see Theorems 4.8 and 6.16 that follow shortly).

The following properties can be directly derived from the definitions and Lemma 4.3.

THEOREM 4.6. *$\sim$ is a strong bisimulation on Con, and it is an equivalence relation.*

THEOREM 4.7. *For any configurations $\langle P, \rho\rangle$ and $\langle Q, \sigma\rangle$, $\langle P, \rho\rangle \sim \langle Q, \sigma\rangle$ if and only if $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$, and:*

(1) whenever $\langle P, \rho\rangle \xrightarrow{\mathrm{c?}q} \langle P', \rho\rangle$, then $\langle Q, \sigma\rangle \xrightarrow{\mathrm{c?}q} \langle Q', \sigma\rangle$ for some Q' such that for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$, $\langle P', \mathcal{E}(\rho)\rangle \mathcal{R} \langle Q', \mathcal{E}(\sigma)\rangle$;

(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q, \sigma\rangle \xrightarrow{\alpha} \nu$ and $\mu \sim \nu$;

and the symmetric conditions of (1) and (2).

The strong bisimilarity for configurations is preserved by all *static* constructors and the summation.

THEOREM 4.8. *If $\langle P, \rho\rangle \sim \langle Q, \sigma\rangle$ then:*

(1) $\langle P + R, \rho\rangle \sim \langle Q + R, \sigma\rangle$, provided that $\langle R, \rho\rangle \sim \langle R, \sigma\rangle$;
(2) $\langle P \| R, \rho\rangle \sim \langle Q \| R, \sigma\rangle$;
(3) $\langle P[f], \rho\rangle \sim \langle Q[f], \sigma\rangle$;
(4) $\langle P \backslash L, \rho\rangle \sim \langle Q \backslash L, \sigma\rangle$;
(5) $\langle \mathbf{if}\ b\ \mathbf{then}\ P, \rho\rangle \sim \langle \mathbf{if}\ b\ \mathbf{then}\ Q, \sigma\rangle$.

PROOF. Items (1) and (3)–(5) are easy from Theorem 4.7. Item (2) is simpler than Theorem 6.16 (1) in Section 6, thus we omit the proof here. □

The strong configuration bisimilarity is not preserved, however, by *dynamic* constructors such as prefix. A counterexample is as follows. Let $P = M_{0,1}[q; x].\mathbf{nil}$ where

$M_{0,1} = \lambda_0[|0\rangle] + \lambda_1[|1\rangle]$ is the 1-qubit measurement according to the computational basis, $Q = I[q].\mathbf{nil}$, and $\rho = [|0\rangle]_q \otimes \sigma$ where $\sigma \in \mathcal{D}(\mathcal{H}_{\overline{q}})$. Then $\langle P, \rho\rangle \sim \langle Q, \rho\rangle$, but $\langle H[q].P, \rho\rangle \not\sim \langle H[q].Q, \rho\rangle$ where H is the Hadamard operator.

Nevertheless, similar to classical value-passing CCS, strong bisimilarity for quantum processes is preserved by all the combinators of qCCS.

THEOREM 4.9. *If $P \sim Q$ then:*

(1) $a.P \sim a.Q$, $a \in \{\tau, c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, \mathcal{E}[\widetilde{q}], M[\widetilde{q}; x]\}$;
(2) $P + R \sim Q + R$;
(3) $P \| R \sim Q \| R$;
(4) $P[f] \sim Q[f]$;
(5) $P \backslash L \sim Q \backslash L$;
(6) **if** b **then** $P \sim$ **if** b **then** Q.

PROOF. Item (1) is easy to check. The rest is direct from Theorem 4.8. □

The monoid laws and the static laws in classical CCS can also be generalized to qCCS.

THEOREM 4.10. *For any $P, Q, R \in qProc$, $K, L \subseteq Chan$, any relabeling functions f and f', and any action prefix a, we have:*

(1) $P + \mathbf{nil} \sim P$;
(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) $P \| (Q \| R) \sim (P \| Q) \| R$;
(8) $(a.P) \backslash L \sim a.P \backslash L$, *if* $cn(a) \not\subseteq L$;
(9) $(a.P)[f] \sim f(a).P[f]$;
(10) $(P + Q) \backslash L \sim P \backslash L + Q \backslash L$;
(11) $(P + Q)[f] \sim P[f] + Q[f]$;
(12) $P \backslash L \sim P$ *if* $cn(P) \cap L = \emptyset$, *where $cn(P)$ is the set of free channel names used in P*;
(13) $(P \backslash K) \backslash L \sim P \backslash (K \cup L)$;
(14) $(P \| Q) \backslash L \sim P \backslash L \| Q \backslash L$, *if* $cn(P) \cap cn(Q) \cap L = \emptyset$;
(15) $P[f] \backslash L \sim P \backslash f^{-1}(L)[f]$;
(16) $P[Id] \sim P$ *where Id is the identity relabeling function*;
(17) $P[f] \sim P[f']$ *if the restrictions of f and f' on $cn(P)$ coincide*;
(18) $P[f][f'] \sim P[f' \circ f]$;
(19) $(P \| Q)[f] \sim P[f] \| Q[f]$ *if the restriction of f on $cn(P) \cup cn(Q)$ is one-to-one.*

PROOF. Similar to Propositions 4.7 and 4.8 in Milner [1989]. □

We now establish the expansion law for quantum processes. In the following theorem, we simply write $P \xrightarrow{\alpha} P'$ if for any $\rho \in \mathcal{D}(\mathcal{H})$, $\langle P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho\rangle$.

THEOREM 4.11 (EXPANSION LAW). *Let*

$$P = (P_1[f_1] \| \cdots \| P_n[f_n]) \backslash L.$$

Then:

$$
\begin{aligned}
P \sim\ & \sum \Big\{ f_i(\alpha).(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_n[f_n])\backslash L : P_i \xrightarrow{\alpha} P_i' \text{ and } f_i(cn(\alpha)) \not\subseteq L \Big\} \\
&+ \sum \Big\{ f_i(c)?x.(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_n[f_n])\backslash L : P_i \xrightarrow{c?v} P_i'\{v/x\} \text{ for any } v, \text{ and } f_i(c) \notin L \Big\} \\
&+ \sum \Big\{ \mathcal{E}[\widetilde{q}].(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_n[f_n])\backslash L : \langle P_i, \rho\rangle \xrightarrow{\tau} \langle P_i', \mathcal{E}_{\widetilde{q}}(\rho)\rangle \text{ for any } \rho \Big\} \\
&+ \sum \Bigg\{ M[\widetilde{q}; x].(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_n[f_n])\backslash L : M = \sum_{j\in J} \lambda_j K^j \text{ and} \\
&\qquad \langle P_i, \rho\rangle \xrightarrow{\tau} \sum_{j\in J} p_j \langle P_i'\{\lambda_j/x\}, K_{\widetilde{q}}^j \rho K_{\widetilde{q}}^{j\dagger}/p_j\rangle \text{ for any } \rho \Bigg\} \\
&+ \sum \Big\{ \tau.(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_j'[f_j]\| \cdots \|P_n[f_n])\backslash L : \\
&\qquad P_i \xrightarrow{\alpha} P_i', P_j \xrightarrow{\beta} P_j', i < j,\ f_i(cn(\alpha)) = f_j(cn(\beta)), \text{and} \\
&\qquad\quad \text{among } \alpha \text{ and } \beta \text{ there is exactly one input and one output} \}
\end{aligned}
$$

provided that there is at least one summand at the right-hand side of the preceding equation.

PROOF. Similar to Proposition 4.9 in Milner [1989]. We put the restriction on the number of summands here for the following reason: in general $Q\backslash L \not\sim \mathbf{nil}$ even if all the free channel names used in Q are included in L, since $qv(\mathbf{nil}) = \emptyset$ while $qv(Q\backslash L) = qv(Q)$ is normally not empty. □

We now turn to examine the properties of strong bisimilarity under recursive definitions. To this end, we assume a set of process variable schemes, ranged over by $X, Y, \ldots$. Assigned to each process variable scheme X there is a nonnegative integer $ar(X)$. If $\widetilde{q}$ is an indexed set of distinct quantum variables with $|\widetilde{q}| = ar(X)$, then $X(\widetilde{q})$ is called a process variable.

Process expressions may be defined by adding the following clause into Definition 3.1 (and replacing the word "process" by the phrase "process expression" and "*qProc*" by "*qExp*"):

(15) $X(\widetilde{q}) \in qExp$, and $qv(X(\widetilde{q})) = \widetilde{q}$,

where $X(\widetilde{q})$ is a process variable. We use metavariables $E, F, \ldots$ to range over process expressions. Suppose that E is a process expression, and $\{X_i(\widetilde{q_i}) : i \in I\}$ is a family of process variables. If $\{P_i : i \in I\}$ is a family of processes such that $qv(P_i) \subseteq \widetilde{q_i}$ for all i, then we write

$$E\{P_i/X_i(\widetilde{q_i}) : i \in I\}$$

for the process obtained by replacing simultaneously $X_i(\widetilde{q_i})$ in E with P_i for all $i \in I$.

Definition 4.12. Let E and F be process expressions containing at most process variables $\{X_i(\widetilde{q_i}) : i \in I\}$. Then E and F are strongly bisimilar, denoted by $E \sim F$, if for all family $\{P_i : i \in I\}$ of quantum processes with $qv(P_i) \subseteq \widetilde{q_i}$, we have

$$E\{P_i/X_i(\widetilde{q_i}) : i \in I\} \sim F\{P_i/X_i(\widetilde{q_i}) : i \in I\}.$$

For simplicity, sometimes we denote $E\{P_i/X_i(\widetilde{q_i}) : i \in I\}$ as $E\{\widetilde{P}/\widetilde{X}\}$ or even $E(\widetilde{P})$ when it does not cause any confusion. The next theorem shows that $\sim$ is also preserved by recursive definitions.

THEOREM 4.13.

(1) If $A(\widetilde{q}) \stackrel{def}{=} P$, *then* $A(\widetilde{q}) \sim P$.
(2) Let $\{E_i : i \in I\}$ *and* $\{F_i : i \in I\}$ *be two families of process expressions containing at most process variables* $\{X_i(\widetilde{q_i}) : i \in I\}$, *and* $E_i \sim F_i$ *for each* $i \in I$. *If* $\{A_i(\widetilde{q_i}) : i \in I\}$ *and* $\{B_i(\widetilde{q_i}) : i \in I\}$ *be two families of process constants such that*

$$A_i(\widetilde{q_i}) \stackrel{def}{=} E_i\{A_j(\widetilde{q_j})/X_j(\widetilde{q_j}) : j \in I\}$$
$$B_i(\widetilde{q_i}) \stackrel{def}{=} F_i\{B_j(\widetilde{q_j})/X_j(\widetilde{q_j}) : j \in I\},$$

then $A_i(\widetilde{q_i}) \sim B_i(\widetilde{q_i})$ *for all* $i \in I$.

PROOF. (1) is obvious, and (2) is similar to Proposition 4.12 in Milner [1989]. □

Finally, the uniqueness of solutions of equations can be proved for process expressions in qCCS.

Definition 4.14. Given a process variable $X(\widetilde{q})$ and a process expression E, we say $X(\widetilde{q})$ is weakly guarded in E if each occurrence of $X(\widetilde{q})$ is within some subexpression $a.F$ of E where a is a prefix.

We also say that E is weakly guarded if each process variable is weakly guarded in E.

THEOREM 4.15. *Let* $\{E_i : i \in I\}$ *be a family of process expressions containing at most process variables* $\{X_i(\widetilde{q_i}) : i \in I\}$, *and each* $X_j(\widetilde{q_j})$ *is weakly guarded in each* E_i. *Let* $\{P_i : i \in I\}$ *and* $\{Q_i : i \in I\}$ *be two families of quantum processes such that* $qv(P_i) \cup qv(Q_i) \subseteq \widetilde{q_i}$ *for each i, and*

$$P_i \sim E_i\{P_j/X_j(\widetilde{q_j}) : j \in I\}$$
$$Q_i \sim E_i\{Q_j/X_j(\widetilde{q_j}) : j \in I\},$$

then $P_i \sim Q_i$ *for all* $i \in I$.

PROOF. Similar to Proposition 4.14 in Milner [1989]. □

5. APPROXIMATE STRONG BISIMULATION

In the previous section, only *exact* strong bisimulation is presented where two quantum processes are either bisimilar or nonbisimilar. Obviously, such a bisimulation cannot capture the idea that a quantum process approximately implements its specification. To measure the behavioral distance between processes, the notion of approximate bisimulation and the bisimulation distance for classical processes were introduced by various authors [Deng et al. 2006; Desharnais et al. 2004; Ying 2001, 2002]. Note that approximation, or imprecision, is especially essential for quantum process algebra since quantum operations constitute a continuum and exact bisimulation is not always practically suitable for their physical implementation. To provide techniques and tools for approximate reasoning, a quantified version of strong bisimulation, which defines for each pair of quantum processes a bisimulation-based distance characterizing the extent to which they are strongly bisimilar, has already been proposed for purely quantum processes in Ying et al. [2009]. In this section, we introduce an approximate variant of strong bisimulation presented in Section 4. To this end, we first present the approximate notion of weight functions defined in Definition 4.1.

Definition 5.1. Let $\mathcal{R}$ be a relation on Con, and $\mu, \nu \in D(Con)$. A λ-weight function for (μ, ν) with respect to $\mathcal{R}$ is a function $\delta : supp(\mu) \times supp(\nu) \to [0, 1]$ which satisfies:

(1) For any $\mathcal{C} \in supp(\mu)$ and $\mathcal{D} \in supp(\nu)$,

$$\sum_{\mathcal{D} \in supp(\nu)} \delta(\mathcal{C}, \mathcal{D}) \leq \mu(\mathcal{C}), \quad \sum_{\mathcal{C} \in supp(\mu)} \delta(\mathcal{C}, \mathcal{D}) \leq \nu(\mathcal{D}).$$

(2)

$$\sum_{\mathcal{C} \in supp(\mu)} \sum_{\mathcal{D} \in supp(\nu)} \delta(\mathcal{C}, \mathcal{D}) \geq 1 - \lambda.$$

(3) If $\delta(\mathcal{C}, \mathcal{D}) > 0$, then $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$.

We write $\mu \mathcal{R}_\lambda \nu$ if there exists a λ-weight function for (μ, ν) with respect to $\mathcal{R}$.

Similar to Lemma 4.3, we have the next lemma.

LEMMA 5.2. *Let $\mu, \nu \in D(Con)$. Then $\mu \mathcal{R}_\lambda \nu$ if and only if $\mu = \sum_{i \in I} p_i \mathcal{C}_i$ and $\nu = \sum_{i \in I} p_i \mathcal{D}_i$ such that*

$$\sum_{i \in I} \{|p_i : \mathcal{C}_i \mathcal{R} \mathcal{D}_i|\} \geq 1 - \lambda.$$

In particular, for any $\mathcal{C}, \mathcal{D} \in Con$ and $\lambda < 1$, $\mathcal{C} \mathcal{R}_\lambda \mathcal{D}$ if and only if $\mathcal{C} \mathcal{R} \mathcal{D}$.

PROOF. Let $\mu \mathcal{R}_\lambda \nu$, and δ is a λ-weight function for (μ, ν) with respect to $\mathcal{R}$. For any $\mathcal{C} \in supp(\mu)$, let $\lambda_\mathcal{C} = \mu(\mathcal{C}) - \sum_{\mathcal{D} \in supp(\nu)} \delta(\mathcal{C}, \mathcal{D})$. Then we have

$$\begin{aligned} \mu &= \sum_{\mathcal{C} \in supp(\mu)} \mu(\mathcal{C}) \mathcal{C} \\ &= \sum_{\mathcal{C}, \mathcal{D}} \delta(\mathcal{C}, \mathcal{D}) \mathcal{C} + \sum_{\mathcal{C} \in supp(\mu)} \lambda_\mathcal{C} \mathcal{C}. \end{aligned}$$

Similarly, we derive $\nu = \sum_{\mathcal{C}, \mathcal{D}} \delta(\mathcal{C}, \mathcal{D}) \mathcal{D} + \sum_{\mathcal{D} \in supp(\nu)} \lambda_\mathcal{D} \mathcal{D}$ where $\lambda_\mathcal{D} = \nu(\mathcal{D}) - \sum_{\mathcal{C} \in supp(\mu)} \delta(\mathcal{C}, \mathcal{D})$. Note that

$$\sum_{\mathcal{C} \in supp(\mu)} \lambda_\mathcal{C} = \sum_{\mathcal{D} \in supp(\nu)} \lambda_\mathcal{D} = 1 - \sum_{\mathcal{C}, \mathcal{D}} \delta(\mathcal{C}, \mathcal{D}).$$

We can further write

$$\begin{aligned} \mu &= \sum_{\mathcal{C}, \mathcal{D}} \delta(\mathcal{C}, \mathcal{D}) \mathcal{C} + \sum_{\mathcal{C}, \mathcal{D}} \frac{\lambda_\mathcal{C} \lambda_\mathcal{D}}{T} \mathcal{C}, \\ \nu &= \sum_{\mathcal{C}, \mathcal{D}} \delta(\mathcal{C}, \mathcal{D}) \mathcal{D} + \sum_{\mathcal{C}, \mathcal{D}} \frac{\lambda_\mathcal{C} \lambda_\mathcal{D}}{T} \mathcal{D}, \end{aligned}$$

where $T = 1 - \sum_{\mathcal{C} \mathcal{R} \mathcal{D}} \delta(\mathcal{C}, \mathcal{D})$. Let $I_j = supp(\mu) \times supp(\nu) \times \{j\}$ for $j = 0, 1$, and $I = I_0 \cup I_1$. Now for any $(\mathcal{C}, \mathcal{D}, j) \in I$, let $p_{(\mathcal{C}, \mathcal{D}, j)}$ be $\delta(\mathcal{C}, \mathcal{D})$ if $j = 0$, and $\lambda_\mathcal{C} \lambda_\mathcal{D} / T$ if $j = 1$. Furthermore, let $\mathcal{C}_{(\mathcal{C}, \mathcal{D}, j)} = \mathcal{C}$ and $\mathcal{D}_{(\mathcal{C}, \mathcal{D}, j)} = \mathcal{D}$. Then

$$\begin{aligned} \sum_{(\mathcal{C}, \mathcal{D}, j) \in I} \{|p_{(\mathcal{C}, \mathcal{D}, j)} : \mathcal{C}_{(\mathcal{C}, \mathcal{D}, j)} \mathcal{R} \mathcal{D}_{(\mathcal{C}, \mathcal{D}, j)}|\} &\geq \sum_{\mathcal{C} \mathcal{R} \mathcal{D}} \delta(\mathcal{C}, \mathcal{D}) \\ &= \sum_{\mathcal{C}, \mathcal{D}} \delta(\mathcal{C}, \mathcal{D}) \geq 1 - \lambda. \end{aligned}$$

That proves the necessity part.

Conversely, suppose $\mu = \sum_{i\in I} p_i\mathcal{C}_i$ and $\nu = \sum_{i\in I} p_i\mathcal{D}_i$ where $\sum_{i\in I}\{|p_i : \mathcal{C}_i\mathcal{R}\mathcal{D}_i|\} \geq 1-\lambda$. Let $I_{\mathcal{C}} = \{i \in I : \mathcal{C}_i = \mathcal{C}\}$ and $I_{\mathcal{D}} = \{i \in I : \mathcal{D}_i = \mathcal{D}\}$. We construct a function $\delta : supp(\mu) \times supp(\nu) \to [0,1]$ such that

$$\delta(\mathcal{C},\mathcal{D}) = \begin{cases} \sum\{|p_i : i \in I_{\mathcal{C}} \cap I_{\mathcal{D}}|\} & \text{if } \mathcal{C}\mathcal{R}\mathcal{D}, \\ 0 & \text{otherwise.} \end{cases}$$

Obviously, if $\delta(\mathcal{C},\mathcal{D}) > 0$, then $\mathcal{C}\mathcal{R}\mathcal{D}$. Furthermore, for any $\mathcal{C} \in supp(\mu)$,

$$\begin{aligned} \sum_{\mathcal{D}\in supp(\nu)} \delta(\mathcal{C},\mathcal{D}) &= \sum\{|p_i : i \in I_{\mathcal{C}}, \text{ and } \mathcal{C}_i\mathcal{R}\mathcal{D}_i|\} \\ &\leq \sum\{|p_i : i \in I_{\mathcal{C}}|\} = \mu(\mathcal{C}). \end{aligned}$$

Similarly, we have $\sum_{\mathcal{C}\in supp(\mu)} \delta(\mathcal{C},\mathcal{D}) \leq \nu(\mathcal{D})$. Finally, we calculate that

$$\begin{aligned} \sum_{\mathcal{C}\in supp(\mu)}\sum_{\mathcal{D}\in supp(\nu)} \delta(\mathcal{C},\mathcal{D}) &= \sum_{\mathcal{C}\in supp(\mu)}\sum\{|p_i : i \in I_{\mathcal{C}}, \text{ and } \mathcal{C}_i\mathcal{R}\mathcal{D}_i|\} \\ &= \sum\{|p_i : \mathcal{C}_i\mathcal{R}\mathcal{D}_i|\} \geq 1-\lambda. \end{aligned}$$

Thus δ is a λ-weight function for (μ,ν) with respect to $\mathcal{R}$, and then $\mu\mathcal{R}\nu$. □

The following lemma is an approximation correspondence of Lemma 4.2.

LEMMA 5.3. *Suppose $\mu,\nu,\omega \in \mathcal{D}(Con)$, $\mathcal{R},\mathcal{R}' \subseteq Con \times Con$.*

(1) If $\mathcal{R} \subseteq \mathcal{R}'$ and $\lambda \leq \lambda'$, then $\mu\mathcal{R}_\lambda\nu$ implies $\mu\mathcal{R}'_{\lambda'}\nu$.
(2) $\mu\mathcal{R}_\lambda\nu$ if and only if $\nu(\mathcal{R}^{-1})_\lambda\mu$.
(3) $\mu\mathcal{R}_\lambda\nu$ and $\nu\mathcal{R}'_{\lambda'}\omega$, then $\mu(\mathcal{R}\circ\mathcal{R}')_{\lambda+\lambda'}\omega$.

PROOF. (1) and (2) are direct from Definition 5.1 or Lemma 5.2. For (3), let δ be a λ-weight function for (μ,ν) with respect to $\mathcal{R}$, and δ' a λ'-weight function for (ν,ω) with respect to $\mathcal{R}'$. We construct $\Delta : supp(\mu)\times supp(\omega) \to [0,1]$ such that for any $\mathcal{C} \in supp(\mu)$ and $\mathcal{K} \in supp(\omega)$,

$$\Delta(\mathcal{C},\mathcal{K}) = \sum_{\mathcal{D}\in supp(\nu)} \frac{\delta(\mathcal{C},\mathcal{D})\delta'(\mathcal{D},\mathcal{K})}{\nu(\mathcal{D})}.$$

It is easy to check that $\sum_{\mathcal{K}\in supp(\omega)} \Delta(\mathcal{C},\mathcal{K}) \leq \mu(\mathcal{C})$ and $\sum_{\mathcal{C}\in supp(\mu)} \Delta(\mathcal{C},\mathcal{K}) \leq \omega(\mathcal{K})$. Futheremore, when $\Delta(\mathcal{C},\mathcal{K}) > 0$, then there exists $\mathcal{D} \in supp(\nu)$ such that both $\delta(\mathcal{C},\mathcal{D}) > 0$ and $\delta'(\mathcal{D},\mathcal{K}) > 0$. Thus $\mathcal{C}\mathcal{R}\mathcal{D}$ and $\mathcal{D}\mathcal{R}'\mathcal{K}$, and so $\mathcal{C}(\mathcal{R}\circ\mathcal{R}')\mathcal{K}$. Finally, we calculate

$$\begin{aligned} \sum_{\mathcal{C}\in supp(\mu)}\sum_{\mathcal{K}\in supp(\omega)} \Delta(\mathcal{C},\mathcal{K}) &= \sum_{\mathcal{C}\in supp(\mu)}\sum_{\mathcal{D}\in supp(\nu)} \frac{\delta(\mathcal{C},\mathcal{D})}{\nu(\mathcal{D})}(\nu(\mathcal{D}) - \lambda_{\mathcal{D}}) \\ &\geq 1-\lambda - \sum_{\mathcal{C}\in supp(\mu)}\sum_{\mathcal{D}\in supp(\nu)} \frac{\delta(\mathcal{C},\mathcal{D})}{\nu(\mathcal{D})}\lambda_{\mathcal{D}} \\ &\geq 1-\lambda - \sum_{\mathcal{D}\in supp(\nu)} \lambda_{\mathcal{D}} \geq 1-\lambda-\lambda' \end{aligned}$$

where $\lambda_{\mathcal{D}} = \nu(\mathcal{D}) - \sum_{\mathcal{K}\in supp(\omega)} \delta'(\mathcal{D},\mathcal{K})$, and the last inequality is calculated by

$$\sum_{\mathcal{D}\in supp(\nu)} \lambda_{\mathcal{D}} = 1 - \sum_{\mathcal{D}\in supp(\nu)} \sum_{\mathcal{K}\in supp(\omega)} \delta'(\mathcal{D},\mathcal{K}) \le \lambda'.$$

Thus Δ is indeed a $\lambda+\lambda'$-weighted function for (μ,ω) with respect to $\mathcal{R}\circ\mathcal{R}'$. □

With these notions, we can define the approximate strong bisimulation between configurations as follows.

Definition 5.4. A relation $\mathcal{R} \subseteq Con \times Con$ is called a λ-strong bisimulation if for any $\langle P,\rho\rangle, \langle Q,\sigma\rangle \in Con$, $\langle P,\rho\rangle \mathcal{R} \langle Q,\sigma\rangle$ implies that $qv(P) = qv(Q)$, $d[\mathrm{tr}_{qv(P)}(\rho), \mathrm{tr}_{qv(Q)}(\sigma)] \le \lambda$, and:

(1) whenever $\langle P,\rho\rangle \xrightarrow{\mathsf{c?}q} \langle P',\rho\rangle$, then $\langle Q,\sigma\rangle \xrightarrow{\mathsf{c?}q} \langle Q',\sigma\rangle$ for some Q' such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$, $\langle P',\mathcal{E}(\rho)\rangle \mathcal{R}_\lambda \langle Q',\mathcal{E}(\sigma)\rangle$;

(2) whenever $\langle P,\rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q,\sigma\rangle \xrightarrow{\alpha} \nu$ and $\mu \mathcal{R}_\lambda \nu$;

and the symmetric conditions of (1) and (2).

Note that by Lemma 5.2, the $\mathcal{R}_\lambda$ in clause (1) of Definition 5.4 can actually be replaced by $\mathcal{R}$. Obviously, when $\lambda = 0$, the preceding definition exactly coincides with the strong bisimulation defined in Definition 4.4.

The approximate strong bisimilarity between configurations and approximate strong bisimilarity between processes can be defined in a straightforward way.

Definition 5.5.

(1) Two quantum configurations $\langle P,\rho\rangle$ and $\langle Q,\sigma\rangle$ are λ-strongly bisimilar, denoted by $\langle P,\rho\rangle \overset{\lambda}{\sim} \langle Q,\sigma\rangle$, if there exists a λ-strong bisimulation $\mathcal{R}$ such that $\langle P,\rho\rangle \mathcal{R} \langle Q,\sigma\rangle$.

(2) Two quantum processes P and Q are λ-strongly bisimilar, denoted by $P \overset{\lambda}{\sim} Q$, if for any quantum state $\rho \in \mathcal{D}(\mathcal{H})$ and any indexed set $\widetilde{v}$ of classical values, $\langle P\{\widetilde{v}/\widetilde{x}\},\rho\rangle \overset{\lambda}{\sim} \langle Q\{\widetilde{v}/\widetilde{x}\},\rho\rangle$. Here $\widetilde{x}$ is the set of free classical variables contained in P and Q.

(3) The strong bisimulation distance between P and Q is defined by

$$D_{sb}(P,Q) = \inf\{\lambda \ge 0 : P \overset{\lambda}{\sim} Q\}.$$

When $P \overset{\lambda}{\not\sim} Q$ for any $\lambda \ge 0$, we simply set $D_{sb}(P,Q) = \infty$.

The following lemmas are useful in proving the latter properties of approximate strong bisimilarity.

LEMMA 5.6. *For any configurations $\langle P,\rho\rangle$ and $\langle Q,\sigma\rangle$, $\langle P,\rho\rangle \overset{\lambda}{\sim} \langle Q,\sigma\rangle$ if and only if $qv(P) = qv(Q)$, $d[\mathrm{tr}_{qv(P)}(\rho), \mathrm{tr}_{qv(Q)}(\sigma)] \le \lambda$, and:*

(1) whenever $\langle P,\rho\rangle \xrightarrow{\mathsf{c?}q} \langle P',\rho\rangle$, then $\langle Q,\sigma\rangle \xrightarrow{\mathsf{c?}q} \langle Q',\sigma\rangle$ for some Q' such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$, $\langle P',\mathcal{E}(\rho)\rangle \overset{\lambda}{\sim} \langle Q',\mathcal{E}(\sigma)\rangle$;

(2) whenever $\langle P,\rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q,\sigma\rangle \xrightarrow{\alpha} \nu$ and $\mu \overset{\lambda}{\sim}_\lambda \nu$;

and the symmetric conditions of (1) and (2).

PROOF. Easy from the definitions and Lemma 5.3(1). □

LEMMA 5.7.

(1) If R_i is a λ_i-strong bisimulation ($i = 1, 2$), then $\mathcal{R}_1 \circ \mathcal{R}_2$ is a $(\lambda_1 + \lambda_2)$-strong bisimulation.

(2) If $\langle P, \rho\rangle \overset{\lambda_1}{\sim} \langle Q, \sigma\rangle$ and $\langle Q, \sigma\rangle \overset{\lambda_2}{\sim} \langle R, \eta\rangle$, then $\langle P, \rho\rangle \overset{\lambda_1+\lambda_2}{\sim} \langle R, \eta\rangle$.

(3) If $P \overset{\lambda_1}{\sim} Q$ and $Q \overset{\lambda_2}{\sim} R$, then $P \overset{\lambda_1+\lambda_2}{\sim} R$.

(4) $\overset{\lambda_1}{\sim} \subseteq \overset{\lambda_2}{\sim}$ whenever $\lambda_1 \leq \lambda_2$.

PROOF. (1) can be deduced easily from Lemma 5.3(3). Then (2) follows from (1), and (3) from (2) directly. Finally, (4) is obvious by definition. □

The following theorem states that the infimum in Definition 5.5 (3) of strong bisimulation distance can be replaced by minimum; that is, the infimum is achievable.

THEOREM 5.8. *If $D_{sb}(P, Q) < \infty$, then $P \overset{D_{sb}(P,Q)}{\sim} Q$.*

PROOF. Suppose $\lambda = D_{sb}(P, Q) < \infty$. We need only to prove that

$$\mathcal{R} = \{(\langle P, \rho\rangle, \langle Q, \sigma\rangle) : \langle P, \rho\rangle \overset{\lambda_i}{\sim} \langle Q, \sigma\rangle \text{ for some decreasing sequence } \lambda_1 > \lambda_2 > \cdots > 0, \text{ and } \lim_{i\to\infty} \lambda_i = \lambda\}$$

is a λ-strong bisimulation. For any $\langle P, \rho\rangle \mathcal{R} \langle Q, \sigma\rangle$, since $\langle P, \rho\rangle \overset{\lambda_i}{\sim} \langle Q, \sigma\rangle$ we have $qv(P) = qv(Q)$, and $d(\mathrm{tr}_{qv(P)}\rho, \mathrm{tr}_{qv(Q)}\sigma) \leq \lambda_i$ for any $i \geq 1$. Thus $d(\mathrm{tr}_{qv(P)}\rho, \mathrm{tr}_{qv(Q)}\sigma) \leq \lambda$. Furthermore,

(1) if $\langle P, \rho\rangle \xrightarrow{c?q} \langle P', \rho\rangle$, then for any $i \geq 1$, $\langle Q, \sigma\rangle \xrightarrow{c?q} \langle Q'_i, \sigma\rangle$ such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$, $\langle P', \mathcal{E}(\rho)\rangle \overset{\lambda_i}{\sim} \langle Q'_i, \mathcal{E}(\sigma)\rangle$. Since by the semantics of qCCS, all configurations are image-finite; that is, the set

$$\mathcal{K} = \left\{\langle Q'_i, \sigma\rangle : \langle Q, \sigma\rangle \xrightarrow{c?q} \langle Q'_i, \sigma\rangle\right\}$$

is finite, there exists a $\langle Q', \sigma\rangle \in \mathcal{K}$ and a decreasing subsequence $\{\lambda_{n_i}\}$ of $\{\lambda_i\}$ such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$ and for any $i \geq 1$, $\langle P', \mathcal{E}(\rho)\rangle \overset{\lambda_{n_i}}{\sim} \langle Q', \mathcal{E}(\sigma)\rangle$. Thus $\langle P', \mathcal{E}(\rho)\rangle \mathcal{R} \langle Q', \mathcal{E}(\sigma)\rangle$.

(2) if $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then for any $i \geq 1$, $\langle Q, \sigma\rangle \xrightarrow{\alpha} \nu_i$ and $\mu \overset{\lambda_i}{\sim}_{\lambda_i} \nu_i$. Again, since $\langle Q, \sigma\rangle$ is image-finite, there exists a $\nu \in D(Con)$ and a decreasing subsequence $\{\lambda_{n_i}\}$ of $\{\lambda_i\}$ such that $\langle Q, \sigma\rangle \xrightarrow{\alpha} \nu$, and for any $i \geq 1$, $\mu \overset{\lambda_{n_i}}{\sim}_{\lambda_{n_i}} \nu$. In the following, we show that this indeed implies $\mu \mathcal{R}_\lambda \nu$.
For any $i \geq 1$, let $\delta_i : supp(\mu) \times supp(\nu) \to [0, 1]$ be a λ_{n_i}-weight function for (μ, ν) with respect to $\overset{\lambda_{n_i}}{\sim}$. Since $\{\delta_i : i \geq 1\}$ can be regarded as a bounded sequence in the Euclidean space $\mathbb{R}^N$ where $N = |supp(\mu)| \cdot |supp(\nu)|$, there exists a convergent subsequence $\{\delta_{m_i}\}$ of $\{\delta_i\}$. Let $\delta = \lim_{i\to\infty} \delta_{m_i}$. Obviously, δ is again a function from $supp(\mu) \times supp(\nu)$ to $[0, 1]$. Suppose $\delta(\mathcal{C}, \mathcal{D}) > 0$. Then there exists $N \geq 1$ such that for any $i \geq N$, $\delta_{m_i}(\mathcal{C}, \mathcal{D}) > 0$, and so $\mathcal{C} \overset{\lambda_{n_{m_i}}}{\sim} \mathcal{D}$. Thus by the definition of $\mathcal{R}$, we have $\mathcal{C}\mathcal{R}\mathcal{D}$. With this, we can easily check that δ is a λ-weight function for (μ, ν) with respect to $\mathcal{R}$.

Symmetric results can be shown when $\langle Q, \sigma\rangle$ performs an action. Thus $\mathcal{R}$ is a λ-strong bisimulation, from which we derive easily that $P \overset{\lambda}{\sim} Q$. □

A direct consequence of the previous theorem is that the strong bisimulation distance between two quantum processes vanishes if and only they are strongly bisimilar.

COROLLARY 5.9. *For any $P, Q \in qProc$, $P \sim Q$ if and only if $D_{sb}(P, Q) = 0$.*

PROOF. Direct from Theorem 5.8, by noting that $\sim = \overset{0}{\sim}$. □

Similar to strong bisimilarity, the approximation strong bisimilarity is also congruent with respect to various process constructors of qCCS.

THEOREM 5.10. *For any $\lambda \geq 0$, $\overset{\lambda}{\sim}$ is a congruent relation on $qProc$. That is, if $P \overset{\lambda}{\sim} Q$ then:*

(1) $a.P \overset{\lambda}{\sim} a.Q$, $a \in \{\tau, c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, \mathcal{E}[\widetilde{q}], M[\widetilde{q}; x]\}$;
(2) $P + R \overset{\lambda}{\sim} Q + R$;
(3) $P \| R \overset{\lambda}{\sim} Q \| R$;
(4) $P[f] \overset{\lambda}{\sim} Q[f]$;
(5) $P \backslash L \overset{\lambda}{\sim} Q \backslash L$;
(6) **if** b **then** $P \overset{\lambda}{\sim}$ **if** b **then** Q.

We now show that all the process constructors of qCCS are nonexpansive according to the pseudometric D_{sb}. To this end, we need a lemma.

LEMMA 5.11. *$\langle P, \rho\rangle \overset{\lambda}{\sim} \langle P, \sigma\rangle$ provided that $d(\rho, \sigma) \leq \lambda$.*

PROOF. We need only to show the following relation

$$\mathcal{R} = \{(\langle P, \rho\rangle, \langle P, \sigma\rangle) : d(\rho, \sigma) \leq \lambda\}$$

is a λ-strong bisimulation. Let $\langle P, \rho\rangle \mathcal{R} \langle P, \sigma\rangle$. Then $d[\mathrm{tr}_{q\upsilon(P)}\rho, \mathrm{tr}_{q\upsilon(P)}\sigma] \leq d(\rho, \sigma) \leq \lambda$ by Theorem 2.2. Furthermore,

— if $\langle P, \rho\rangle \xrightarrow{\mathsf{c}?q} \langle P', \rho\rangle$, then $\langle P, \sigma\rangle \xrightarrow{\mathsf{c}?q} \langle P', \sigma\rangle$. For any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{q\upsilon(P')-\{q\}}$, we have $d[\mathcal{E}(\rho), \mathcal{E}(\sigma)] \leq d(\rho, \sigma) \leq \lambda$, again by Theorem 2.2. Thus $\langle P', \mathcal{E}(\rho)\rangle \mathcal{R} \langle P', \mathcal{E}(\sigma)\rangle$ by definition.
— if $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ is caused by a measurement prefix $M[\widetilde{q}; x]$ where $M = \sum_{i\in I} \lambda_i |\psi_i\rangle\langle\psi_i|$, then we have $\mu = \sum_{i\in I} p_i \langle P\{\lambda_i/x\}, \rho_i\rangle$, $p_i = \mathrm{tr}(|\psi_i\rangle\langle\psi_i|\rho)$, $\rho_i = |\psi_i\rangle\langle\psi_i|_{\widetilde{q}} \otimes \mathrm{tr}_{\widetilde{q}}\rho$, and

$$\langle P, \sigma\rangle \xrightarrow{\alpha} \nu = \sum_{i\in I} q_i \langle P\{\lambda_i/x\}, \sigma_i\rangle$$

with $q_i = \mathrm{tr}(|\psi_i\rangle\langle\psi_i|\sigma)$ and $\sigma_i = |\psi_i\rangle\langle\psi_i|_{\widetilde{q}} \otimes \mathrm{tr}_{\widetilde{q}}\sigma$. Let $\delta : supp(\mu) \times supp(\nu) \to [0, 1]$ such that

$$\delta(\mathcal{C}, \mathcal{D}) = \begin{cases} \min\{p_i, q_i\} & \text{if } \mathcal{C} = \langle P\{\lambda_i/x\}, \rho_i\rangle \text{ and } \mathcal{D} = \langle P\{\lambda_i/x\}, \sigma_i\rangle, \\ 0 & \text{otherwise.} \end{cases}$$

Then for any $\mathcal{C} \in supp(\mu)$ and $\mathcal{D} \in supp(\nu)$,

$$\sum_{\mathcal{D}\in supp(\nu)} \delta(\mathcal{C}, \mathcal{D}) = \sum_{\mathcal{C}\in supp(\mu)} \delta(\mathcal{C}, \mathcal{D}) = \min\{\mu(\mathcal{C}), \nu(\mathcal{D})\},$$

and

$$\sum_{\mathcal{C}\in supp(\mu)}\sum_{\mathcal{D}\in supp(\nu)}\delta(\mathcal{C},\mathcal{D})=\sum_{i\in I}\min\{p_i,q_i\}\geq 1-\lambda,$$

where the last inequality is from the following argument. Note that

$$2\sum_{i\in I}\min\{p_i,q_i\}=\sum_{i\in I}p_i+\sum_{i\in I}q_i-\sum_{i\in I}|p_i-q_i|.$$

It follows that $d(\{p_i\},\{q_i\})=1-\sum_{i\in I}\min\{p_i,q_i\}$. Furthermore, since $\{|\psi_i\rangle\langle\psi_i|:i\in I\}$ constitute a quantum measurement on $\widetilde{q}$, we have $d(\{p_i\},\{q_i\})\leq d(\rho,\sigma)$ from Theorem 2.1.

Now we have shown that δ is a λ-weight function for (μ,ν) with respect to $\mathcal{R}$. Then $\mu\mathcal{R}_\lambda\nu$ by definition.

— if $\langle P,\rho\rangle\xrightarrow{\alpha}\mu$ where α is not a quantum input and the transition is not caused by a measurement, then $\mu=\langle P',\mathcal{E}(\rho)\rangle$ for some P' and some trace-preserving super-operator $\mathcal{E}$. Then we have $\langle P,\sigma\rangle\xrightarrow{\alpha}\langle P',\mathcal{E}(\sigma)\rangle$, and $\langle P',\mathcal{E}(\rho)\rangle\mathcal{R}\langle P',\mathcal{E}(\sigma)\rangle$.

Symmetric results can be shown when $\langle P,\sigma\rangle$ performs an action. Thus $\mathcal{R}$ is a λ-strong bisimulation. □

THEOREM 5.12.

(1) The strong bisimulation distance D_{sb} is a pseudometric on qProc;
(2) For any processes P and Q, we have:
(a) $D_{sb}(\mathcal{E}[\widetilde{q}].P,\mathcal{F}[\widetilde{q}].Q)\leq d_\diamond(\mathcal{E},\mathcal{F})+D_{sb}(P,Q)$;
(b) $D_{sb}(a.P,a.Q)\leq D_{sb}(P,Q)$ where $a\in\{\tau,c?x,c!e,\mathsf{c}?q,\mathsf{c}!q,\mathcal{E}[\widetilde{q}],M[\widetilde{q};x]\}$;
(c) $D_{sb}(P+R,Q+R)\leq D_{sb}(P,Q)$;
(d) $D_{sb}(P\|R,Q\|R)\leq D_{sb}(P,Q)$;
(e) $D_{sb}(P[f],Q[f])\leq D_{sb}(P,Q)$;
(f) $D_{sb}(P\backslash L,Q\backslash L)\leq D_{sb}(P,Q)$;
(g) $D_{sb}(\mathbf{if}\ b\ \mathbf{then}\ P,\mathbf{if}\ b\ \mathbf{then}\ Q)\leq D_{sb}(P,Q)$.

PROOF. (1) We need only to prove that D_{sb} satisfies the triangle inequality

$$D_{sb}(P,Q)+D_{sb}(Q,R)\geq D_{sb}(P,R).$$

For any $\lambda_1>D_{sb}(P,Q)$ and $\lambda_2>D_{sb}(Q,R)$, we have $P\overset{\lambda_1}{\sim}Q$ and $Q\overset{\lambda_2}{\sim}R$ by definition. Then $P\overset{\lambda_1+\lambda_2}{\sim}R$ from Lemma 5.7(3). So $D_{sb}(P,R)\leq\lambda_1+\lambda_2$, and the result holds from the arbitrariness of λ_1 and λ_2.

(2a) The case when $D_{sb}(P,Q)=\infty$ is obvious. Now suppose $D_{sb}(P,Q)<\infty$. For any $\lambda>D_{sb}(P,Q)$, we have $\langle P,\sigma\rangle\overset{\lambda}{\sim}\langle Q,\sigma\rangle$ for any $\sigma\in\mathcal{D}(\mathcal{H})$. To prove the result, it suffices to show $\mathcal{E}[\widetilde{q}].P\overset{\lambda'}{\sim}\mathcal{F}[\widetilde{q}].Q$ where $\lambda'=\lambda+d_\diamond(\mathcal{E},\mathcal{F})$.

We first derive $qv(P)=qv(Q)$ from $\langle P,\rho\rangle\overset{\lambda}{\sim}\langle Q,\rho\rangle$, and then $qv(\mathcal{E}[\widetilde{q}].P)=qv(\mathcal{F}[\widetilde{q}].Q)$. For any $\rho\in\mathcal{D}(\mathcal{H})$, we have $\langle\mathcal{E}[\widetilde{q}].P,\rho\rangle\xrightarrow{\tau}\langle P,\mathcal{E}_{\widetilde{q}}(\rho)\rangle$ and $\langle\mathcal{F}[\widetilde{q}].Q,\rho\rangle\xrightarrow{\tau}\langle Q,\mathcal{F}_{\widetilde{q}}(\rho)\rangle$. Note that $d[\mathcal{E}_{\widetilde{q}}(\rho),\mathcal{F}_{\widetilde{q}}(\rho)]\leq d_\diamond(\mathcal{E},\mathcal{F})$. Then $\langle P,\mathcal{E}_{\widetilde{q}}(\rho)\rangle\overset{d_\diamond(\mathcal{E},\mathcal{F})}{\sim}\langle P,\mathcal{F}_{\widetilde{q}}(\rho)\rangle$ by Lemma 5.11. Furthermore, we have $\langle P,\mathcal{E}_{\widetilde{q}}(\rho)\rangle\overset{\lambda'}{\sim}\langle Q,\mathcal{F}_{\widetilde{q}}(\rho)\rangle$ from Lemma 5.7(2). Thus $\langle\mathcal{E}[\widetilde{q}].P,\rho\rangle\overset{\lambda'}{\sim}\langle\mathcal{F}[\widetilde{q}].Q,\rho\rangle$ by Lemma 5.6, and $\mathcal{E}[\widetilde{q}].P\overset{\lambda'}{\sim}\mathcal{F}[\widetilde{q}].Q$ from the arbitrariness of ρ.

(2b)–(2g) are direct from Theorem 5.10. We omit the proofs here. □

Note that in classical process algebra, a notion of approximate bisimulation has been proposed for deterministic processes from which any action causes at most one probabilistic transition [Giacalone et al. 1990]. This approximate bisimulation, however, does not yield a pseudometric for general probabilistic processes, as shown by van Breugel [2010]. The problem is, Giacalone et al.'s bisimulation is preassumed to be an equivalence relation, which, in some sense, violates the intuition that approximate bisimulation is not transitive: P approximates Q and Q approximates R do not necessarily imply that P approximates R. Our definition in this section, however, only requires an approximate bisimulation to be symmetric, thanks to the method, introduced by Baier and Kwiatkowska [2000], of lifting relations between processes to those between probability distributions. Thus we are able to obtain a pseudometric for quantum processes.

6. WEAK BISIMULATION BETWEEN QUANTUM PROCESSES

It is obvious that the (approximate) strong bisimulations proposed in previous sections are too overdiscriminative since even internal actions, caused by local quantum operations and (classical or quantum) communication, are required to be perfectly matched by bisimilar quantum processes. In this section, we turn to weak bisimulation, originated from Baier and Hermanns [1997], which abstracts from the internal actions. To do this, we first extend the transition relation defined in Section 3.

Definition 6.1. We define the relation $\Longrightarrow \subseteq D(Con) \times D(Con)$ as the smallest relation satisfying the following conditions:

(1) $\mathcal{C} \Longrightarrow \mathcal{C}$;
(2) if $\mathcal{C} \xrightarrow{\tau} \mu$ and $\mu \Longrightarrow \nu$, then $\mathcal{C} \Longrightarrow \nu$;
(3) if $\mu = \sum_{i\in I} p_i\mathcal{C}_i$, and for any $i \in I$, $\mathcal{C}_i \Longrightarrow \nu_i$ for some ν_i, then $\mu \Longrightarrow \sum_{i\in I} p_i\nu_i$.

Allowing different transitions with the same weak labels to be combined together is essential for the definition of weak bisimulation for probabilistic processes, as pointed out in Deng et al. [2005] and Desharnais et al. [2002, 2010]. That is the reason why we add clause (3) here in Definition 6.1.

For any $\mu, \nu \in D(Con)$ and $s = \alpha_1 \dots \alpha_n \in Act^*$, we say that μ can evolve into ν by a weak s-transition, denoted by $\mu \overset{s}{\Longrightarrow} \nu$, if there exist $\mu_1, \dots, \mu_{n+1}, \nu_1, \dots, \nu_n \in D(Con)$, such that $\mu \Longrightarrow \mu_1$, $\mu_{n+1} = \nu$, and for each $i = 1, \dots, n$, $\mu_i \xrightarrow{\alpha_i} \nu_i$ and $\nu_i \Longrightarrow \mu_{i+1}$.

Note that $\mu \Longrightarrow\xrightarrow{\alpha} \nu$ and $\mu \overset{\alpha}{\Longrightarrow} \nu$ are different since in the former the last action of every execution branch from μ to ν must be α while in the latter the action α appeared in each branch is not necessarily the last one.

The following lemma is a direct consequence of Proposition 6.1 in Deng et al. [2007].

LEMMA 6.2. *If $\mu \overset{s}{\Longrightarrow} \nu$, and $\mu = \sum_{i\in I} p_i\mu_i$ where $p_i > 0$ for each $i \in I$, then for any $i \in I$, $\mu_i \overset{s}{\Longrightarrow} \nu_i$ for some ν_i such that $\nu = \sum_{i\in I} p_i\nu_i$. Conversely, if for each $i \in I$, $\mu_i \overset{s}{\Longrightarrow} \nu_i$, then $\mu \overset{s}{\Longrightarrow} \nu$ where $\mu = \sum_{i\in I} p_i\mu_i$, $\nu = \sum_{i\in I} p_i\nu_i$, $p_i > 0$ for each $i \in I$, and $\sum_{i\in I} p_i = 1$.*

By Lemma 6.2, we can show the transitivity of weak transitions.

LEMMA 6.3. *If $\mu \Longrightarrow \nu$ and $\nu \Longrightarrow \omega$, then $\mu \Longrightarrow \omega$.*

PROOF. We prove by induction on the depth of the inference by which the action $\mu \Longrightarrow \nu$ is inferred, using clauses (1)–(3) in Definition 6.1:

— If $\nu = \mu$, then $\mu \Longrightarrow \omega$ holds trivially.
— Suppose $\mu = \mathcal{C}$, $\mathcal{C} \xrightarrow{\tau} \mu'$, and $\mu' \Longrightarrow \nu$. Then by induction, we derive $\mu' \Longrightarrow \omega$. Thus $\mu \Longrightarrow \omega$ by definition.
— Suppose $\mu = \sum_{i\in I} p_i\mathcal{C}_i$, for any $i \in I$, $\mathcal{C}_i \Longrightarrow \nu_i$ for some ν_i, and $\nu = \sum_{i\in I} p_i\nu_i$. Then by Lemma 6.2, we have $\nu_i \Longrightarrow \omega_i$ for some ω_i such that $\omega = \sum_{i\in I} p_i\omega_i$. Now by induction, $\mathcal{C}_i \Longrightarrow \omega_i$, and then $\mu \Longrightarrow \omega$ by Lemma 6.2. □

To conclude this subsection, we extend Lemma 3.3 to the weak transition case.

LEMMA 6.4. *If* $\langle P, \rho\rangle \overset{s}{\Longrightarrow} \mu$, *then:*

(1) $\mathrm{tr}(\rho) = \mathrm{tr}(\mu)$;
(2) there exist a set of trace-preserving super-operators $\{\mathcal{E}_i : i \in I\}$ *and a set of projectors* $\{E_i : i \in I\}$, *both acting on* $\mathcal{H}_{qv(P)\cup b\,v(s)}$ *where* $b\,v(\alpha_1 \ldots \alpha_n) = b\,v(\alpha_1) \cup \cdots \cup b\,v(\alpha_n)$, $\sum_{i\in I} E_i = I$, *such that for any* $\sigma \in \mathcal{D}(\mathcal{H})$,

$$\langle P, \sigma\rangle \overset{s}{\Longrightarrow} \sum_{i\in I} q_i^\sigma \langle P_i, \mathcal{E}_i(\sigma)\rangle$$

where $q_i^\sigma = \mathrm{tr}(E_i\sigma)$;
(3) for any trace-preserving super-operator $\mathcal{E}$ *acting on* $\mathcal{H}_{\overline{qv(P)\cup b\,v(s)}}$, *we have* $\langle P, \mathcal{E}(\rho)\rangle \overset{s}{\Longrightarrow} \mathcal{E}(\mu)$.

PROOF. Note that from Lemma 3.3 (1), if $\nu \xrightarrow{\alpha} \mu$ then $\mathrm{tr}(\nu) = \mathrm{tr}(\mu)$. So to prove (1), we need only to show $\mathrm{tr}(\nu) = \mathrm{tr}(\mu)$ provided that $\nu \Longrightarrow \mu$. We prove by induction on the depth of the inference by which the action $\nu \Longrightarrow \mu$ is inferred, using clauses (1)–(3) in Definition 6.1.

— If $\nu = \mu$, then $\mathrm{tr}(\nu) = \mathrm{tr}(\mu)$ holds trivially.
— Suppose $\nu = \langle P, \rho\rangle$, $\langle P, \rho\rangle \xrightarrow{\tau} \omega$, and $\omega \Longrightarrow \mu$. Then we have $\mathrm{tr}(\mu) = \mathrm{tr}(\omega) = \mathrm{tr}(\rho)$, where the first equation is derived by induction, and the second by Lemma 3.3(1).
— Suppose $\nu = \sum_{i\in I} p_i\mathcal{C}_i$, for any $i \in I$, $\mathcal{C}_i \Longrightarrow \nu_i$ for some ν_i, and $\mu = \sum_{i\in I} p_i\nu_i$. Then by induction, $\mathrm{tr}(\nu_i) = \mathrm{tr}(\mathcal{C}_i)$. Thus $\mathrm{tr}(\mu) = \sum_{i\in I} p_i\mathrm{tr}(\nu_i) = \sum_{i\in I} p_i\mathrm{tr}(\mathcal{C}_i) = \mathrm{tr}(\nu)$.

The proofs of (2) and (3) are more complicated, but the idea is similar. So we omit the detail here. □

6.1. Weak Bisimulation

Definition 6.5. A relation $\mathcal{R} \subseteq Con \times Con$ is called a weak bisimulation if for any $\langle P, \rho\rangle, \langle Q, \sigma\rangle \in Con$, $\langle P, \rho\rangle\mathcal{R}\langle Q, \sigma\rangle$ implies that $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$, and:

(1) whenever $\langle P, \rho\rangle \xrightarrow{c?q} \mu$, then $\langle Q, \sigma\rangle \Longrightarrow\!\!\xrightarrow{c?q} \nu$ for some ν such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu)\mathcal{R}\mathcal{E}(\nu)$;
(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q, \sigma\rangle \overset{\widehat{\alpha}}{\Longrightarrow} \nu$ and $\mu\mathcal{R}\nu$;

(3) whenever $\langle Q, \sigma\rangle \xrightarrow{c?q} \nu$, then $\langle P, \rho\rangle \Longrightarrow\!\!\xrightarrow{c?q} \mu$ for some μ such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\nu)-\{q\}}}$, $\mathcal{E}(\mu)\mathcal{R}\mathcal{E}(\nu)$;

(4) whenever $\langle Q, \sigma\rangle \xrightarrow[\widehat{\alpha}]{\alpha} \nu$ where α is not a quantum input, then there exists μ such that $\langle P, \rho\rangle \Longrightarrow \mu$ and $\mu\mathcal{R}\nu$.

Definition 6.6.

(1) Two quantum configurations $\langle P, \rho\rangle$ and $\langle Q, \sigma\rangle$ are weakly bisimilar, denoted by $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, if there exists a weak bisimulation $\mathcal{R}$ such that $\langle P, \rho\rangle\mathcal{R}\langle Q, \sigma\rangle$.

(2) Two quantum processes P and Q are weakly bisimilar, denoted by $P \approx Q$, if for any quantum state $\rho \in \mathcal{D}(\mathcal{H})$ and any indexed set $\widetilde{v}$ of classical values, $\langle P\{\widetilde{v}/\widetilde{x}\}, \rho\rangle \approx \langle Q\{\widetilde{v}/\widetilde{x}\}, \rho\rangle$. Here $\widetilde{x}$ is the set of free classical variables contained in P and Q.

To illustrate the power of weak bisimilarity defined before, we revisit the examples presented in Section 3.

Example 6.7 (*Superdense Coding Revisited*). This example is devoted to proving rigorously that the protocol presented in Example 3.4 indeed sends two bits of classical information from Alice to Bob by transmitting a qubit, with the help of a maximally entangled state. Let

$$Sdc_{spec} = c?x.Set_x[q_1, q_2].d!x.\mathbf{nil}$$

be the specification of superdense coding protocol, where

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

and Set_i, $i = 0, \ldots, 3$, is the 2-qubit super-operator which sets the target qubits to $|\widetilde{i}\rangle$; that is, for any $\rho \in \mathcal{D}(\mathcal{H})$,

$$Set_{i,q,q'}(\rho) = \left[|\widetilde{i}\rangle\right]_{q,q'} \otimes \mathrm{tr}_{q,q'}(\rho).$$

We have $Set_x[q_1, q_2]$ in the specification simply for technical reasons: to make $qv(Sdc_{spec}) = qv(Sdc)$, and to set q_1, q_2 to the required final states. For any $\rho \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}})$, and $v \in \{0, 1, 2, 3\}$,

$$\begin{aligned}
&\langle Sdc_{spec}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle\\
\xrightarrow{c?v}\ &\langle Set_v[q_1, q_2].d!v.\mathbf{nil}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle\\
\xrightarrow{\tau}\ &\langle d!v.\mathbf{nil}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle\\
\xrightarrow{d!v}\ &\langle \mathbf{nil}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle.
\end{aligned}$$

We can easily prove

$$\langle Sdc, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \approx \langle Sdc_{spec}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle$$

by checking that

$$\begin{aligned}\mathcal{R} = \ & \left\{(\langle Sdc, \rho_\Psi\rangle, \langle Sdc_{spec}, \rho_\Psi\rangle)\right\} \\ & \cup\Big\{(\langle P, \eta\rangle, \langle Set_v[q_1, q_2].d!v.\mathbf{nil}, \rho_\Psi\rangle) : v = 0, \ldots, 3, \\ & \quad \langle Sdc, \rho_\Psi\rangle \stackrel{c?v}{\Longrightarrow} \langle P, \eta\rangle, \text{ and } qv(P) \neq \emptyset\Big\} \\ & \cup\{(\langle(\mathbf{nil}\|d!v.\mathbf{nil})\backslash\{\mathsf{e}\}, \rho_{\tilde{v}}\rangle, \langle d!v.\mathbf{nil}, \rho_{\tilde{v}}\rangle) : v = 0, \ldots, 3\} \\ & \cup\{(\langle(\mathbf{nil}\|\mathbf{nil})\backslash\{\mathsf{e}\}, \rho_{\tilde{v}}\rangle, \langle\mathbf{nil}, \rho_{\tilde{v}}\rangle) : v = 0, \ldots, 3\}\end{aligned}$$

is a weak bisimulation, where $\rho_\psi = [|\psi\rangle]_{q_1,q_2} \otimes \rho$.

Note that $Sdc \approx Sdc_{spec}$ does not hold in general since superdense coding protocol needs the assistance of a maximally entangled state to realize the intended task.

Example 6.8 (*Teleportation Revisited*). This example is devoted to proving rigorously that the protocol presented in Example 3.5 indeed teleports any unknown quantum state from Alice to Bob, again with the help of a maximally entangled state. To employ our notion of weak bisimulation, we need to modify the original definition of Alice's protocol in Example 3.5 as follows:

$$Alice'_t = \mathsf{c}?q.CN[q, q_1].H[q].M[q, q_1; x].Set_\Psi[q, q_1].e!x.\mathbf{nil}$$

and $Tel' = (Alice'_t\|Bob_t)\backslash\{e\}$ where Set_Ψ is the 2-qubit super-operator which sets the target qubits to $|\Psi\rangle$. Let

$$Tel_{spec} = \mathsf{c}?q.SWAP_{1,3}[q, q_1, q_2].\mathsf{d}!q_2.\mathbf{nil}$$

be the specification of teleportation protocol, where $SWAP_{1,3}$ is a 3-qubit unitary operator which exchanges the states of the first and the third qubits, keeping the second qubit untouched. Again, we involve qubit q_1 here just for technical reason: to make $qv(Tel_{spec}) = qv(Tel')$. Then for any $\rho \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}})$ and $r \neq q_1, q_2$,

$$\begin{aligned} & \langle Tel_{spec}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\ \xrightarrow{\mathsf{c}?r} \ & \langle SWAP_{1,3}[r, q_1, q_2].\mathsf{d}!q_2.\mathbf{nil}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\ \xrightarrow{\tau} \ & \langle \mathsf{d}!q_2.\mathbf{nil}, [|\Psi\rangle]_{q_1,r} \otimes \rho\rangle \\ \xrightarrow{\mathsf{d}!q_2} \ & \langle\mathbf{nil}, [|\Psi\rangle]_{q_1,r} \otimes \rho\rangle.\end{aligned}$$

We can now prove

$$\langle Tel', [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \approx \langle Tel_{spec}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle$$

by checking that

$$\begin{aligned}\mathcal{R} = \ & \left\{\left(\left\langle Tel', \rho_\Psi^{q_1,q_2}\right\rangle, \left\langle Tel_{spec}, \rho_\Psi^{q_1,q_2}\right\rangle\right)\right\} \\ & \cup\Big\{\left(\langle P, \eta\rangle, \langle SWAP_{1,3}[r, q_1, q_2].\mathsf{d}!q_2.\mathbf{nil}, \sigma_\Psi^{q_1,q_2}\right) : \\ & \quad \left\langle Tel', \sigma_\Psi^{q_1,q_2}\right\rangle \stackrel{\mathsf{c}?r}{\Longrightarrow} \langle P, \eta\rangle, \sigma \in \mathcal{D}\left(\mathcal{H}_{\overline{\{q_1,q_2\}}}\right), qv(P) = \{r, q_1, q_2\}, \text{ and } r \neq q_1, q_2\Big\} \\ & \cup\Big\{\left(\langle P, \eta\rangle, \langle \mathsf{d}!q_2.\mathbf{nil}, \sigma_\Psi^{q_1,r}\right) : \left\langle Tel', \sigma_\Psi^{q_1,q_2}\right\rangle \stackrel{\mathsf{c}?r}{\Longrightarrow} \mu \text{ with } \langle P, \eta\rangle \in supp(\mu), \\ & \quad \sigma \in \mathcal{D}\left(\mathcal{H}_{\overline{\{q_1,r\}}}\right), qv(P) = \{q_2\}, \text{ and } r \neq q_1, q_2\Big\} \\ & \cup\left\{\left(\left\langle(\mathbf{nil}\|\mathbf{nil})\backslash\{e\}, \sigma_\Psi^{q_1,r}\right\rangle, \left\langle\mathbf{nil}, \sigma_\Psi^{q_1,r}\right\rangle\right) : \sigma \in \mathcal{D}\left(\mathcal{H}_{\overline{\{q_1,r\}}}\right)\right\}\end{aligned}$$

is a weak bisimulation, where $\sigma_\psi^{q,q'} = [|\psi\rangle]_{q,q'} \otimes \sigma$.

Again, $Tel' \approx Tel_{spec}$ does not hold in general since teleportation protocol is valid only when a maximally entangled state is provided and consumed.

Example 6.9 (*Encode Quantum Circuits by qCCS, Revisited*). Using the notations presented in Example 3.6, we can prove the following properties considering the sequential composition and parallel composition of quantum gates:

(1) $\mathcal{U}(U) \circ \mathcal{U}(V) \approx \mathcal{U}(VU)$, provided that $ar(\mathcal{U}(U)) = ar(\mathcal{U}(V))$;
(2) $\mathcal{U}(U) \circ \mathcal{M}(M) \approx \mathcal{M}(U^\dagger MU) \circ \mathcal{U}(U)$, provided that $ar(\mathcal{U}(U)) = ar(\mathcal{M}(M))$;
(3) $\mathcal{U}(U) \otimes \mathcal{U}(V) \approx \mathcal{U}(U \otimes V)$.

The proof is straightforward, and we only take (1) as an example. Suppose $ar(\mathcal{U}(U)) = ar(\mathcal{U}(V)) = n$. Let

$$\begin{aligned}
\mathcal{R} \;=\; & \{(\langle \mathcal{U}(U) \circ \mathcal{U}(V), \rho\rangle, \langle \mathcal{U}(VU), \rho\rangle) : \rho \in \mathcal{D}(\mathcal{H})\} \\
\cup\; & \{(\langle P, \sigma\rangle, \langle Q, \eta\rangle) : \langle \mathcal{U}(U) \circ \mathcal{U}(V), \rho\rangle \overset{\mathsf{c}^n\widetilde{r}}{\Longrightarrow} \langle P, \sigma\rangle \text{ and} \\
& \langle \mathcal{U}(VU), \rho\rangle \overset{\mathsf{c}^n\widetilde{r}}{\Longrightarrow} \langle Q, \eta\rangle \text{ where } \widetilde{r} \subseteq qVar \text{ and } \rho \in \mathcal{D}(\mathcal{H})\} \\
\cup\; & \{(\langle P, \sigma\rangle, \langle Q, \eta\rangle) : \langle \mathcal{U}(U) \circ \mathcal{U}(V), \rho\rangle \overset{\mathsf{c}^n\widetilde{r},\mathsf{d}^n!\widetilde{r}}{\Longrightarrow} \langle P, \sigma\rangle \text{ and} \\
& \langle \mathcal{U}(VU), \rho\rangle \overset{\mathsf{c}^n\widetilde{r},\mathsf{d}^n!\widetilde{r}}{\Longrightarrow} \langle Q, \eta\rangle \text{ where } \widetilde{r} \subseteq qVar \text{ and } \rho \in \mathcal{D}(\mathcal{H})\}.
\end{aligned}$$

It is easy to check that $\mathcal{R}$ is a weak bisimulation. So we have $\langle \mathcal{U}(U) \circ \mathcal{U}(V), \rho\rangle \approx \langle \mathcal{U}(VU), \rho\rangle$ for all $\rho \in \mathcal{D}(\mathcal{H})$ and then $\mathcal{U}(U) \circ \mathcal{U}(V) \approx \mathcal{U}(VU)$.

To conclude this subsection, we prove some properties of weak bisimilarity which are useful in the rest of this article.

LEMMA 6.10. *Let $\mathcal{R}$ be a weak bisimulation, and $\mu\mathcal{R}\nu$.*

(1) If $\mu \Longrightarrow \mu'$, then there exists ν' such that $\nu \Longrightarrow \nu'$ and $\mu'\mathcal{R}\nu'$.
(2) If $\mu \xrightarrow{\mathsf{c}?q} \mu'$, then there exists ν' such that $\nu \Longrightarrow \xrightarrow{\mathsf{c}?q} \nu'$ and for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{q\nu(\mu')-\{q\}}}$, $\mathcal{E}(\mu')\mathcal{R}\mathcal{E}(\nu')$.
(3) If $\mu \xrightarrow{\alpha} \mu'$, then there exists ν' such that $\nu \overset{\hat{\alpha}}{\Longrightarrow} \nu'$ and $\mu'\mathcal{R}\nu'$.

PROOF. Easy from Lemmas 6.2 and 6.3. □

THEOREM 6.11. *$\approx$ is a weak bisimulation on Con, and it is an equivalence relation.*

PROOF. Suppose each $\mathcal{R}_i$, $i = 1, 2, \ldots$, is a weak bisimulation on *Con*. From Lemmas 4.2 and 6.10, we can prove that the following relations are all weak bisimulations:

$$\begin{array}{ll}
(1)\ Id_{Con} & (2)\ \mathcal{R}_i^{-1} \\
(3)\ \mathcal{R}_1 \circ \mathcal{R}_2 & (4)\ \bigcup_i \mathcal{R}_i.
\end{array}$$

Then the result follows. □

The following lemma gives a recursive characterization of weak bisimilarity between configurations.

THEOREM 6.12. *For any configurations $\langle P, \rho\rangle$ and $\langle Q, \sigma\rangle$, $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$ if and only if $q\nu(P) = q\nu(Q)$, $\mathrm{tr}_{q\nu(P)}(\rho) = \mathrm{tr}_{q\nu(Q)}(\sigma)$, and:*

(1) whenever $\langle P, \rho\rangle \xrightarrow{\mathsf{c}?q} \mu$, then $\langle Q, \sigma\rangle \Longrightarrow \xrightarrow{\mathsf{c}?q} \nu$ for some ν such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{q\nu(\mu)-\{q\}}}$, $\mathcal{E}(\mu) \approx \mathcal{E}(\nu)$;

(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ *where* α *is not a quantum input, then there exists* ν *such that* $\langle Q, \sigma\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu$ *and* $\mu \approx \nu$*;*

and the symmetric conditions of (1) and (2).

PROOF. Similar to the corresponding result, Theorem 36, of Feng et al. [2007]. □

LEMMA 6.13. *If* $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$*, then for any super-operator* $\mathcal{E}$ *acting on* $\mathcal{H}_{\overline{qv(P)}}$*, we have* $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}(\mathcal{E}(\sigma))$*. In particular,* $\mathrm{tr}(\rho) = \mathrm{tr}(\sigma)$*.*

PROOF. Let $S = qv(P)$. From $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, we have $\mathrm{tr}_S(\rho) = \mathrm{tr}_S(\sigma)$. Note that $\mathcal{E}(\mathrm{tr}_S(\rho)) = \mathrm{tr}_S(\mathcal{E}(\rho))$ since $\mathcal{E}$ acts only on $\mathcal{H}_{\overline{S}}$, and $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}_{\overline{S}}(\mathrm{tr}_S(\mathcal{E}(\rho)))$. The result follows. □

As in classical process algebra, the notion of weak bisimulation up to $\approx$ is useful.

Definition 6.14. A relation $\mathcal{R} \subseteq Con \times Con$ is called a weak bisimulation up to $\approx$ if for any $\langle P, \rho\rangle, \langle Q, \sigma\rangle \in Con$, $\langle P, \rho\rangle \mathcal{R} \langle Q, \sigma\rangle$ implies that $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$, and:

(1) whenever $\langle P, \rho\rangle \xrightarrow{c?q} \mu$, then $\langle Q, \sigma\rangle \Longrightarrow\!\!\xrightarrow{c?q} \nu$ for some ν such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu)\mathcal{R}\circ \approx \mathcal{E}(\nu)$;

(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q, \sigma\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu$ and $\mu\mathcal{R}\circ \approx \nu$;

and the symmetric conditions of (1) and (2).

LEMMA 6.15. *If* $\mathcal{R}$ *is a weak bisimulation up to* $\approx$*, then* $\mathcal{R} \subseteq \approx$*.*

PROOF. Suppose $\mathcal{R}$ is a weak bisimulation up to $\approx$. We first prove that that $\mathcal{R}\circ \approx$ is a weak bisimulation. Let $\langle P, \rho\rangle \mathcal{R}\circ \approx \langle Q, \sigma\rangle$; that is, there exists $\langle R, \eta\rangle$ such that $\langle P, \rho\rangle \mathcal{R} \langle R, \eta\rangle$ and $\langle R, \eta\rangle \approx \langle Q, \sigma\rangle$. Then $qv(P) = qv(R) = qv(Q)$, and $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(R)}(\eta) = \mathrm{tr}_{qv(Q)}(\sigma)$.

Let $\langle P, \rho\rangle \xrightarrow{c?q} \mu$. Then $\langle R, \eta\rangle \Longrightarrow\!\!\xrightarrow{c?q} \omega$ such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu)\mathcal{R}\circ \approx \mathcal{E}(\omega)$. We further derive from Lemma 6.10 that $\langle Q, \sigma\rangle \Longrightarrow\!\!\xrightarrow{c?q} \nu$, and for any trace-preserving super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(\omega)-\{q\}}}$, $\mathcal{F}(\omega)\approx\mathcal{F}(\nu)$. Note that $qv(\mu) = qv(\omega)$. We have $\mathcal{E}'(\mu)\mathcal{R}\circ \approx \mathcal{E}'(\nu)$ for any trace-preserving super-operator $\mathcal{E}'$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, by Lemma 4.2.

Let $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ for some α not a quantum input. Then $\langle R, \eta\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu$ such that $\mu\mathcal{R}\circ \approx \nu$. Furthermore, from $\langle R, \eta\rangle \approx \langle Q, \sigma\rangle$ we have $\langle Q, \sigma\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \omega$ such that $\nu\approx\omega$, by Lemma 6.10. So we have $\mu\mathcal{R}\circ \approx \omega$ from Lemma 4.2.

The symmetric form when $\langle Q, \sigma\rangle$ performs an action can be similarly proved. So $\mathcal{R}\circ \approx$ is a weak bisimulation; that is, $\mathcal{R}\circ \approx \subseteq \approx$. Then the result holds by noting that the identity relation is a trivial weak bisimulation. □

6.2. Weak Bisimilarity Congruence

We now turn to prove the congruence properties of weak bisimilarity. First, we show that the weak bisimilarity for configurations is preserved by all static constructors.

THEOREM 6.16. *If* $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$ *then:*

(1) $\langle P\|R, \rho\rangle \approx \langle Q\|R, \sigma\rangle$*;*
(2) $\langle P[f], \rho\rangle \approx \langle Q[f], \sigma\rangle$*;*
(3) $\langle P\backslash L, \rho\rangle \approx \langle Q\backslash L, \sigma\rangle$*;*
(4) $\langle$**if** b **then** $P, \rho\rangle \approx \langle$**if** b **then** $Q, \sigma\rangle$.

PROOF. Let us prove (1); other cases are simpler. Let

$$\mathcal{R} = \{(\langle P\|R, \mathcal{E}(\rho)\rangle, \langle Q\|R, \mathcal{E}(\sigma)\rangle) : \langle P, \rho\rangle \approx \langle Q, \sigma\rangle, \text{ and } \mathcal{E} \text{ is a trace-preserving super-operator acting on } \mathcal{H}_{\overline{qv(P)}}\}.$$

It suffices to show that $\mathcal{R}$ is a weak bisimulation. Suppose $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$ where $\mathcal{C} = \langle P\|R, \mathcal{E}(\rho)\rangle$ and $\mathcal{D} = \langle Q\|R, \mathcal{E}(\sigma)\rangle$ for some $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, and $\mathcal{E}$ is a trace-preserving super-operator acting on $\mathcal{H}_{\overline{qv(P)}}$. Then $qv(P) = qv(Q)$ and $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$ by Theorem 6.12. Thus $qv(P\|R) = qv(Q\|R)$ and

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

Let $\langle P\|R, \mathcal{E}(\rho)\rangle \xrightarrow{\alpha} \mu$ for some α and μ. There are three cases to consider.

I: The transition is caused by P solely. We need to further consider two subcases:

(i) $\alpha = \mathsf{c}?q$ is a quantum input. Then there exists a transition $\langle P, \rho\rangle \xrightarrow{\mathsf{c}?q} \langle P', \rho\rangle$ and $\mu = \langle P'\|R, \mathcal{E}(\rho)\rangle$. By the assumption that $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, we have

$$\langle Q, \sigma\rangle \Longrightarrow \boxplus_{i\in I} p_i \bullet \langle Q_i', \sigma_i\rangle \xrightarrow{\mathsf{c}?q} \boxplus_{i\in I} p_i \bullet \langle Q_i, \sigma_i\rangle$$

such that for any trace-preserving super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$,

$$\langle P', \mathcal{F}(\rho)\rangle \approx \langle Q_i, \mathcal{F}(\sigma_i)\rangle \tag{6}$$

holds for any $i \in I$. Then $\langle Q, \mathcal{E}(\sigma)\rangle \Longrightarrow \boxplus_{i\in I} p_i \bullet \langle Q_i', \mathcal{E}(\sigma_i)\rangle$ by Lemma 6.4(3), from which we further derive

$$\langle Q, \mathcal{E}(\sigma)\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \boxplus_{i\in I} p_i \bullet \langle Q_i, \mathcal{E}(\sigma_i)\rangle$$

and

$$\langle Q\|R, \mathcal{E}(\sigma)\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \nu = \boxplus_{i\in I} p_i \bullet \langle Q_i\|R, \mathcal{E}(\sigma_i)\rangle.$$

For any trace-preserving super-operator $\mathcal{F}'$ acting on $\mathcal{H}_{\overline{qv(P'\|R)-\{q\}}}$, we obtain from Lemma 3.2 that the composite map $\mathcal{F}' \circ \mathcal{E}$ is a trace-preserving super-operator acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$. Now using Eq. (6) we have

$$\langle P', \mathcal{F}'(\mathcal{E}(\rho))\rangle \approx \langle Q_i, \mathcal{F}'(\mathcal{E}(\sigma_i))\rangle,$$

and thus $\langle P'\|R, \mathcal{F}'(\mathcal{E}(\rho))\rangle \mathcal{R} \langle Q_i\|R, \mathcal{F}'(\mathcal{E}(\sigma_i))\rangle$. That is, $\mathcal{F}'(\mu)\mathcal{R}\mathcal{F}'(\nu)$ as required.

(ii) α is not a quantum input. Then there exists a transition $\langle P, \rho\rangle \xrightarrow{\alpha} \mu_1 = \boxplus_{i\in I} p_i \bullet \langle P_i, \rho_i\rangle$ and $\mu = \boxplus_{i\in I} p_i \bullet \langle P_i\|R, \mathcal{E}(\rho_i)\rangle$ by Lemma 3.3(3). From the assumption that $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, we have

$$\langle Q, \sigma\rangle \overset{\widehat{\alpha}}{\Longrightarrow} \nu_1 = \boxplus_{j\in J} q_j \bullet \langle Q_j, \sigma_j\rangle$$

and $\mu_1 \approx \nu_1$ by Theorem 6.12. Noting that $\mathcal{E}$ is a trace-preserving super-operator on $\mathcal{H}_{\overline{qv(Q)}}$, we have $\langle Q, \mathcal{E}(\sigma)\rangle \overset{\widehat{\alpha}}{\Longrightarrow} \boxplus_{j\in J} q_j \bullet \langle Q_j, \mathcal{E}(\sigma_j)\rangle$ by Lemma 6.4(3). So it holds that

$$\langle Q\|R, \mathcal{E}(\sigma)\rangle \overset{\widehat{\alpha}}{\Longrightarrow} \nu = \boxplus_{j\in J} q_j \bullet \langle Q_j\|R, \mathcal{E}(\sigma_j)\rangle.$$

Now for each $i \in I$ and $j \in J$, $\langle P_i, \rho_i\rangle \approx \langle Q_j, \sigma_j\rangle$ implies $\langle P_i\|R, \mathcal{E}(\rho_i)\rangle \mathcal{R} \langle Q_j\|R, \mathcal{E}(\sigma_j)\rangle$ since from Lemma 3.2, $\mathcal{E}$ is also a trace-preserving

super-operator acting on $\mathcal{H}_{\overline{qv(P_i)}}$. Thus we have $\mu\mathcal{R}\nu$ by Lemma 4.3, by noting that $\mu_1 \approx \nu_1$.

II: The transition is caused by R solely. We also need to further consider three subcases:

(i) $\alpha = \mathsf{c}?q$ is a quantum input where $q \notin qv(P)$. Then we have $\langle R, \mathcal{E}(\rho)\rangle \xrightarrow{\mathsf{c}?q} \langle R', \mathcal{E}(\rho)\rangle$ for some R', and $\mu = \langle P\|R', \mathcal{E}(\rho)\rangle$. Thus $\langle R, \mathcal{E}(\sigma)\rangle \xrightarrow{\mathsf{c}?q} \langle R', \mathcal{E}(\sigma)\rangle$. By inference rule **Inp-Int**, we have

$$\langle Q\|R, \mathcal{E}(\sigma)\rangle \xrightarrow{\mathsf{c}?q} \langle Q\|R', \mathcal{E}(\sigma)\rangle$$

since $q \notin qv(Q)$. Now for any trace-preserving super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(P\|R')-\{q\}}}$, the composite map $\mathcal{F}\circ\mathcal{E}$ is a trace-preserving super-operator acting on $\mathcal{H}_{\overline{qv(P)}}$ from the fact that $qv(P\|R') - \{q\} \supseteq qv(P) - \{q\} = qv(P)$. Thus

$$\langle P\|R', \mathcal{F}(\mathcal{E}(\rho))\rangle\mathcal{R}\langle Q\|R', \mathcal{F}(\mathcal{E}(\sigma))\rangle$$

from the definition of $\mathcal{R}$.

(ii) $\alpha = \tau$, and the transition is caused by a measurement prefix $M[\widetilde{q}; x]$ where $M = \sum_{i\in I}\lambda_i|\psi_i\rangle\langle\psi_i|$. Then we have $\langle R, \mathcal{E}(\rho)\rangle \xrightarrow{\alpha} \sum_{i\in I} p_i\langle R_i, \mathcal{F}_i(\mathcal{E}(\rho))\rangle$ where $p_i = \mathrm{tr}(|\psi_i\rangle_{\widetilde{q}}\langle\psi_i|\mathcal{E}(\rho))$, $R_i = R\{\lambda_i/x\}$, $\mathcal{F}_i$ is the trace-preserving super-operator which sets the $\widetilde{q}$ systems to $|\psi_i\rangle\langle\psi_i|$; that is,

$$\mathcal{F}_i(\eta) = \sum_{k\in I} |\psi_i\rangle_{\widetilde{q}}\langle\psi_k|\eta|\psi_k\rangle_{\widetilde{q}}\langle\psi_i|$$

for any $\eta \in \mathcal{D}(\mathcal{H})$, and $\mu = \sum_{i\in I} p_i\langle P\|R_i, \mathcal{F}_i(\mathcal{E}(\rho))\rangle$. We further derive that

$$\langle Q\|R, \mathcal{E}(\sigma)\rangle \xrightarrow{\alpha} \nu = \sum_{i\in I} q_i\langle Q\|R_i, \mathcal{F}_i(\mathcal{E}(\sigma))\rangle$$

with $q_i = \mathrm{tr}(|\psi_i\rangle_{\widetilde{q}}\langle\psi_i|\mathcal{E}(\sigma))$.
Notice that for any i, the composite map $\mathcal{E}_i \circ \mathcal{E}$ is a super-operator acting on $\mathcal{H}_{\overline{qv(P)}}$ where $\mathcal{E}_i(\eta) = |\psi_i\rangle_{\widetilde{q}}\langle\psi_i|\eta|\psi_i\rangle_{\widetilde{q}}\langle\psi_i|$ for any $\eta \in \mathcal{D}(\mathcal{H})$. It follows that $p_i = q_i$ from Lemma 6.13. Furthermore, we have

$$(\langle P\|R_i, \mathcal{F}_i(\mathcal{E}(\rho))\rangle, \langle Q\|R_i, \mathcal{F}_i(\mathcal{E}(\sigma))\rangle) \in \mathcal{R}$$

since $\mathcal{F}_i\circ\mathcal{E}$ is a trace-preserving super-operator acting on $\mathcal{H}_{\overline{qv(P)}}$. Then it follows that $\mu\mathcal{R}\nu$ from Lemma 4.3.

(iii) α is not a quantum input and the transition is not caused by a measurement. Then there exists a transition $\langle R, \mathcal{E}(\rho)\rangle \xrightarrow{\alpha} \langle R', \mathcal{F}(\mathcal{E}(\rho))\rangle$ where $\mathcal{F}$ is a trace-preserving super-operator on $\mathcal{H}_{qv(R)}$, and $\mu = \langle P\|R', \mathcal{F}(\mathcal{E}(\rho))\rangle$. We also have $\langle R, \mathcal{E}(\sigma)\rangle \xrightarrow{\alpha} \langle R', \mathcal{F}(\mathcal{E}(\sigma))\rangle$. Thus $\langle Q\|R, \mathcal{E}(\sigma)\rangle \xrightarrow{\alpha} \langle Q\|R', \mathcal{F}(\mathcal{E}(\sigma))\rangle$, and

$$(\langle P\|R', \mathcal{F}(\mathcal{E}(\rho))\rangle, \langle Q\|R', \mathcal{F}(\mathcal{E}(\sigma))\rangle) \in \mathcal{R}$$

since $\mathcal{F}\circ\mathcal{E}$ is a trace-preserving super-operator acting on $\mathcal{H}_{\overline{qv(P)}}$.

III: The transition is caused by a communication between P and R. Without loss of generality, we assume that

$$\langle P, \rho\rangle \xrightarrow{\mathsf{c}?q} \langle P', \rho\rangle, \quad \langle R, \rho\rangle \xrightarrow{\mathsf{c}!q} \langle R', \rho\rangle,$$

and $\mu = \langle P'\|R', \mathcal{E}(\rho)\rangle$. Other cases are simpler. Then $q \notin qv(P)$ by the validity of $P\|R$, and $\langle R, \eta\rangle \xrightarrow{\mathsf{c}!q} \langle R', \eta\rangle$ for any $\eta \in \mathcal{D}(\mathcal{H})$. From the assumption that $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, we have

$$\langle Q, \sigma\rangle \Longrightarrow \boxplus_{i\in I} p_i \bullet \langle Q'_i, \sigma_i\rangle \xrightarrow{\mathsf{c}?q} \boxplus_{i\in I} p_i \bullet \langle Q_i, \sigma_i\rangle$$

such that for any $i \in I$ and any trace-preserving super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$, it holds that $\langle P', \mathcal{F}(\rho)\rangle \approx \langle Q_i, \mathcal{F}(\sigma_i)\rangle$. In particular, we have

$$\langle P', \mathcal{E}(\rho)\rangle \approx \langle Q_i, \mathcal{E}(\sigma_i)\rangle \tag{7}$$

since $qv(P) \supseteq qv(P') - \{q\}$. Noting that $\mathcal{E}$ is a trace-preserving super-operator on $\mathcal{H}_{\overline{qv(Q)}}$, we have $\langle Q, \mathcal{E}(\sigma)\rangle \Longrightarrow \boxplus_{i\in I} p_i \bullet \langle Q'_i, \mathcal{E}(\sigma_i)\rangle$ by Lemma 6.4(3), from which we derive further

$$\langle Q, \mathcal{E}(\sigma)\rangle \Longrightarrow\!\!\xrightarrow{\mathsf{c?}q} \boxplus_{i\in I} p_i \bullet \langle Q_i, \mathcal{E}(\sigma_i)\rangle,$$

and

$$\langle Q\|R, \mathcal{E}(\sigma)\rangle \Longrightarrow\!\!\xrightarrow{\tau} \nu = \boxplus_{i\in I} p_i \bullet \langle Q_i\|R', \mathcal{E}(\sigma_i)\rangle.$$

Furthermore, for any $i \in I$, we have

$$(\langle P'\|R', \mathcal{E}(\rho)\rangle, \langle Q_i\|R', \mathcal{E}(\sigma_i)\rangle) \in \mathcal{R}$$

by Eq. (7). That is, $\mu\mathcal{R}\nu$ as required.

The symmetric form when $\langle Q\|R, \mathcal{E}(\sigma)\rangle \xrightarrow{\alpha} \nu$ can be similarly proved. So $\mathcal{R}$ is a weak bisimulation on Con. The result follows by noting that the identity transformation is also a trace-preserving super-operator on $\mathcal{H}_{\overline{qv(P)}}$. □

From Theorem 6.16, the superdense coding protocol and teleportation protocol presented in Section 3 are still valid in any quantum process context which consists only of parallel composition, relabeling, restriction, and conditional.

Similar to classical value-passing CCS, the weak bisimilarity for quantum processes is preserved by all the combinators of qCCS except for summation.

THEOREM 6.17. *If $P \approx Q$ then:*

(1) $a.P \approx a.Q$, $a \in \{\tau, c?x, c!e, \mathsf{c?}q, \mathsf{c!}q, \mathcal{E}[\widetilde{q}], M[\widetilde{q}; x]\}$;
(2) $P\|R \approx Q\|R$;
(3) $P[f] \approx Q[f]$;
(4) $P\backslash L \approx Q\backslash L$;
(5) **if** b **then** $P \approx$ **if** b **then** Q.

PROOF. The proof for (1) is similar to Theorem 38 of Feng et al. [2007], and (2)–(5) are direct from Theorem 6.16. □

6.3. Congruent Equivalence of Quantum Processes

As in classical process algebra, the weak bisimilarity is not preserved by the summation combinator. To deal with this problem, we introduce the notion of equality between quantum processes based on $\approx$.

Definition 6.18. Two configurations $\langle P, \rho\rangle$ and $\langle Q, \sigma\rangle$ are said to be equal, denoted by $\langle P, \rho\rangle \simeq \langle Q, \sigma\rangle$, if $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$, and:

(1) whenever $\langle P, \rho\rangle \xrightarrow{\mathsf{c?}q} \mu$, then $\langle Q, \sigma\rangle \Longrightarrow\!\!\xrightarrow{\mathsf{c?}q} \nu$ for some ν such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu) \approx \mathcal{E}(\nu)$;
(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q, \sigma\rangle \overset{\alpha}{\Longrightarrow} \nu$ and $\mu \approx \nu$;

and the symmetric conditions of (1) and (2).

The only difference between the definitions of $\approx$ and $\simeq$ is that in the latter the $\stackrel{\widehat{\alpha}}{\Longrightarrow}$ transition in clause (2) is replaced by $\stackrel{\alpha}{\Longrightarrow}$; that is, the matching actions for a τ-move have to be at least one τ-move.

Furthermore, we lift the definition of equality to quantum processes as follows. For $P, Q \in qProc$, $P \simeq Q$ if and only if for any quantum state $\rho \in \mathcal{D}(\mathcal{H})$ and any indexed set $\widetilde{v}$ of classical values, $\langle P\{\widetilde{v}/\widetilde{x}\}, \rho\rangle \simeq \langle Q\{\widetilde{v}/\widetilde{x}\}, \rho\rangle$ where $\widetilde{x} = fv(P) \cup fv(Q)$.

It is worth noting that all the weak bisimulation relations proved in the examples of previous sections are also valid when $\approx$ is replaced by $\simeq$. The following properties are easy to show.

THEOREM 6.19.

(1) $\simeq$ is an equivalence relation;
(2) $P \sim Q$ implies $P \simeq Q$, and $P \simeq Q$ implies $P \approx Q$;
(3) if $P \approx Q$ then $a.P \simeq a.Q$ for $a \in \{\tau, c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, \mathcal{E}[\widetilde{q}], M[\widetilde{q}; x]\}$;
(4) $P \simeq Q$ if and only if $P + R \approx Q + R$ for all $R \in qProc$.

Now we prove that the equality relation is preserved by all process constructors of qCCS.

THEOREM 6.20. *If $P \simeq Q$ then:*

(1) $a.P \simeq a.Q$, $a \in \{\tau, c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, \mathcal{E}[\widetilde{q}], M[\widetilde{q}; x]\}$;
(2) $P + R \simeq Q + R$;
(3) $P \| R \simeq Q \| R$;
(4) $P[f] \simeq Q[f]$;
(5) $P \backslash L \simeq Q \backslash L$;
*(6) **if** b **then** $P \simeq$ **if** b **then** Q.*

PROOF. (2) is direct from Theorem 6.19 (4). Others are similar to the proofs of corresponding results for weak bisimilarity. □

We now turn to examine the properties of the congruent equivalence $\simeq$ under recursive definitions.

Definition 6.21. Let E and F be process expressions containing at most process variables $\{X_i(\widetilde{q_i}) : i \in I\}$. Then E and F are equal, denoted by $E \simeq F$, if for all family $\{P_i : i \in I\}$ of quantum processes with $qv(P_i) \subseteq \widetilde{q_i}$, we have

$$E\{P_i/X_i(\widetilde{q_i}) : i \in I\} \simeq F\{P_i/X_i(\widetilde{q_i}) : i \in I\}.$$

The next theorem shows that $\simeq$ is also preserved by recursive definitions.

THEOREM 6.22.

(1) If $A(\widetilde{q}) \stackrel{def}{=} P$, then $A(\widetilde{q}) \simeq P$.
(2) Let $\{E_i : i \in I\}$ and $\{F_i : i \in I\}$ be two families of process expressions containing at most process variables $\{X_i(\widetilde{q_i}) : i \in I\}$, and $E_i \simeq F_i$ for each $i \in I$. If $\{A_i(\widetilde{q_i}) : i \in I\}$ and $\{B_i(\widetilde{q_i}) : i \in I\}$ be two families of process constants such that

$$A_i(\widetilde{q_i}) \stackrel{def}{=} E_i\{A_j(\widetilde{q_j})/X_j(\widetilde{q_j}) : j \in I\}$$
$$B_i(\widetilde{q_i}) \stackrel{def}{=} F_i\{B_j(\widetilde{q_j})/X_j(\widetilde{q_j}) : j \in I\},$$

then $A_i(\widetilde{q_i}) \simeq B_i(\widetilde{q_i})$ for all $i \in I$.

PROOF. (1) is obvious. For (2), we only prove the special case where $|I| = 1$ and for any $i \in I$, $\widetilde{q_i} = \emptyset$. That is, we prove $A \simeq B$ assuming that $qv(A) = qv(B) = \emptyset$, $A \stackrel{def}{=} E(A)$ and $B \stackrel{def}{=} F(B)$ where E and F are process expressions containing process variable X with $qv(X) = \emptyset$, and $E \simeq F$.

Let

$$\mathcal{R} = \{(\langle G(A), \rho\rangle, \langle G(B), \rho\rangle) : \rho \in \mathcal{D}(\mathcal{H}), G \text{ contains at most process variable } X\}.$$

Obviously, for any $\langle G(A), \rho\rangle \mathcal{R} \langle G(B), \rho\rangle$, we have $qv(G(A)) = qv(G(B))$ and $\mathrm{tr}_{qv(G(A))}(\rho) = \mathrm{tr}_{qv(G(B))}(\rho)$. Similar to Propositions 4.12 and 7.8 of Milner [1989], we can prove the following properties by induction on the depth of the inference by which the action $\langle G(A), \rho\rangle \xrightarrow{\alpha} \mu$ is inferred:

(i) whenever $\langle G(A), \rho\rangle \xrightarrow{\mathsf{c}?q} \mu$, then $\langle G(B), \rho\rangle \Longrightarrow\!\!\xrightarrow{\mathsf{c}?q} \nu$ such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu)\mathcal{R}\circ \approx \mathcal{E}(\nu)$;

(ii) whenever $\langle G(A), \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, there exists ν such that $\langle G(B), \rho\rangle \stackrel{\alpha}{\Longrightarrow} \nu$ and $\mu\mathcal{R}\circ \approx \nu$.

Only one case deserves elaboration: when $G = G_1 \| G_2$ and $\langle G(A), \rho\rangle \xrightarrow{\tau} \langle P', \rho\rangle$ is caused by

$$\langle G_1(A), \rho\rangle \xrightarrow{\mathsf{c}?q} \langle P'_1, \rho\rangle \quad \text{and} \quad \langle G_2(A), \rho\rangle \xrightarrow{\mathsf{c}!q} \langle P'_2, \rho\rangle,$$

where $P' = P'_1 \| P'_2$. By induction, we have

$$\langle G_1(B), \rho\rangle \Longrightarrow\!\!\xrightarrow{\mathsf{c}?q} \boxplus_{i\in I} p_i \bullet \langle Q_1^i, \mathcal{F}'_i(\rho)\rangle,$$

where $\mathcal{F}'_i$ is a trace-preserving super-operator acting on $qv(G_1)$ (here Lemma 6.4(2) is used for the $\Longrightarrow$ transition), and for any trace-preserving super-operator $\mathcal{E}$ on $\mathcal{H}_{\overline{qv(P'_1)-\{q\}}}$ and any $i \in I$, it holds

$$\langle P'_1, \mathcal{E}(\rho)\rangle \mathcal{R} \langle Q'_1, \mathcal{E}(\rho)\rangle \approx \langle Q_1^i, \mathcal{E}(\mathcal{F}'_i(\rho)\rangle. \tag{8}$$

Thus $P'_1 = H_1(A)$ and $Q'_1 = H_1(B)$ for some H_1 containing only process variable X.

Also by induction, we have

$$\langle G_2(B), \rho\rangle \stackrel{\mathsf{c}!q}{\Longrightarrow} \boxplus_{j\in J} q_j \bullet \langle Q_2^j, \mathcal{F}_j(\rho)\rangle,$$

where $\mathcal{F}_j$ is a trace-preserving super-operator acting on $qv(G_2)$, and for any $j \in J$,

$$\langle P'_2, \rho\rangle \mathcal{R} \langle Q'_2, \rho\rangle \approx \langle Q_2^j, \mathcal{F}_j(\rho)\rangle. \tag{9}$$

Thus $P'_2 = H_2(A)$ and $Q'_2 = H_2(B)$ for some H_2 containing only process variable X.

Now by inference rule **Q-Com**, and noting that $\mathcal{F}'_i$ and $\mathcal{F}_j$ commute for any $i \in I$ and $j \in J$ since $qv(G_1) \cap qv(G_2) = \emptyset$, we derive that

$$\langle G(B), \rho\rangle \stackrel{\tau}{\Longrightarrow} \boxplus_{i\in I} \boxplus_{j\in J} p_i q_j \bullet \langle Q_1^i \| Q_2^j, \mathcal{F}_j(\mathcal{F}'_i(\rho))\rangle.$$

Now we calculate that for any $i \in I$ and $j \in J$,

$$\begin{array}{lcll}
\langle P'_1 \| P'_2, \rho\rangle & = & \langle (H_1 \| H_2)(A), \rho\rangle & \\
& \mathcal{R} & \langle (H_1 \| H_2)(B), \rho\rangle & \text{By definition} \\
& = & \langle Q'_1 \| Q'_2, \rho\rangle & \\
& \approx & \langle Q'_1 \| Q_2^j, \mathcal{F}_j(\rho)\rangle & \text{By Eq. (9) and Theorem 6.16} \\
& \approx & \langle Q_1^i \| Q_2^j, \mathcal{F}_j(\mathcal{F}'_i(\rho))\rangle & \text{By Eq. (8), Lemma 3.2, and Theorem 6.16.}
\end{array}$$

Similarly, we can prove the symmetric forms of (i) and (ii) for $\langle G(B), \rho\rangle \xrightarrow{\alpha} \nu$. Then $\mathcal{R}$ is a weak bisimulation up to $\approx$, and so $\mathcal{R} \subseteq \approx$ by Lemma 6.15. Now from (i) and (ii) again, we have $\langle G(A), \rho\rangle \simeq \langle G(B), \rho\rangle$. Taking $G = X$ and noting the arbitrariness of ρ, we have $A \simeq B$. □

Finally, the uniqueness of solutions of equations can be proved for process expressions in qCCS, in the sense of $\simeq$.

Definition 6.23. Given a process variable $X(\widetilde{q})$ and a process expression E, we say:

— $X(\widetilde{q})$ is sequential in E if every subexpression of E which contains $X(\widetilde{q})$, excluding $X(\widetilde{q})$ itself, is of the form $a.F$, $\sum_{i\in I} F_i$, or **if** b **then** F;
— $X(\widetilde{q})$ is guarded in E if each occurrence of $X(\widetilde{q})$ is within some subexpression $a.F$ of E where a is a (classical or quantum) input or output.

We also say that E is sequential (respectively guarded) if each process variable is sequential (respectively guarded) in E.

LEMMA 6.24. *Let G be guarded and sequential, and contain at most process variables $\widetilde{X}$. If $\langle G(\widetilde{P}), \rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P'_i, \rho_i\rangle$. Then there exist sequential process expressions $\{H_i : i \in I\}$, containing at most process variables $\widetilde{X}$, such that $P'_i = H_i(\widetilde{P}_\alpha)$ for each i, and for any $\widetilde{Q}$, $\langle G(\widetilde{Q}), \rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle H_i(\widetilde{Q}_\alpha), \rho_i\rangle$. Here*

$$\widetilde{P}_\alpha = \begin{cases} \widetilde{P}\{r/q\} \text{ for some } q \in qv(\widetilde{P}), & \text{if } \alpha = \mathsf{c}?r \\ \widetilde{P}\{v/x\} \text{ for some } x \in fv(\widetilde{P}), & \text{if } \alpha = c?v \text{ or } \alpha = \tau \text{ is caused by a measurement} \\ \widetilde{P}, & \text{otherwise} \end{cases}$$

and $\widetilde{Q}_\alpha$ is defined similarly. Moreover, if $\alpha = \tau$, then H_i is guarded.

PROOF. Similar to Lemma 7.12 of Milner [1989]. □

THEOREM 6.25. *Let $\{E_i : i \in I\}$ be a family of process expressions containing at most process variables $\{X_i(\widetilde{q_i}) : i \in I\}$, and each $X_j(\widetilde{q_j})$ is sequential and guarded in each E_i. Let $\{P_i : i \in I\}$ and $\{Q_i : i \in I\}$ be two families of quantum processes such that $qv(P_i) \cup qv(Q_i) \subseteq \widetilde{q_i}$ for each i, and*

$$P_i \simeq E_i\{P_j/X_j(\widetilde{q_j}) : j \in I\}$$
$$Q_i \simeq E_i\{Q_j/X_j(\widetilde{q_j}) : j \in I\},$$

then $P_i \simeq Q_i$ for all $i \in I$.

PROOF. For simplicity, we only prove the case where $|I| = 1$ and all the processes contain no free classical or quantum variables. That is, we prove $P \simeq Q$ assuming that $qv(P) = qv(Q) = \emptyset$, $fv(P) = fv(Q) = \emptyset$, $P \simeq E(P)$, and $Q \simeq E(Q)$, where E contains at most process variable X.

Let

$$\mathcal{R} = \{(\langle M, \rho\rangle, \langle N, \sigma\rangle) : \langle M, \rho\rangle \approx \langle H(P), \eta\rangle \text{ and } \langle N, \sigma\rangle \approx \langle H(Q), \eta\rangle \text{ for some } \eta \in \mathcal{D}(\mathcal{H}), \text{ and } H \text{ is sequential and contains at most } X\}.$$

We show $\mathcal{R}$ is a weak bisimulation. The proof is somewhat similar to Proposition 7.13 in Milner [1989]. We first claim that for any $\langle M, \rho\rangle \mathcal{R} \langle N, \sigma\rangle$,

$$\text{If } \langle M, \rho\rangle \Longrightarrow \mu, \text{ then } \langle N, \sigma\rangle \Longrightarrow \nu \text{ such that } \mu \mathcal{R} \nu. \tag{10}$$

Suppose $\langle M, \rho\rangle \Longrightarrow \mu$. Then $\langle H(P), \eta\rangle \Longrightarrow \mu_1$, $\mu \approx \mu_1$, from $\langle M, \rho\rangle \approx \langle H(P), \eta\rangle$. By Theorem 6.20, we have $H(E(P)) \simeq H(P)$, so $\langle H(E(P)), \eta\rangle \Longrightarrow \mu_2$ such that $\mu_1 \approx \mu_2$. Note

that X is both sequential and guarded in $H(E(P))$. By repeatedly using Lemma 6.24, we have $\mu_2 = \boxplus_{i\in K} p_i \bullet \langle H_i'(P), \rho_i\rangle$, and

$$\langle H(E(Q)), \eta\rangle \Longrightarrow \nu_2 = \boxplus_{i\in K} p_i \bullet \langle H_i'(Q), \rho_i\rangle,$$

where H_i' is sequential for any $i \in K$. Since $H(E(Q)) \simeq H(Q)$ and $\langle N, \sigma\rangle \approx \langle H(Q), \eta\rangle$, we have $\langle H(Q), \eta\rangle \Longrightarrow \nu_1$, $\nu_2 \approx \nu_1$, and $\langle N, \sigma\rangle \Longrightarrow \nu$, $\nu_1 \approx \nu$. Furthermore, it is obvious that $\mu_2 \mathcal{R} \nu_2$ from Lemma 4.3, and then $\mu \mathcal{R} \nu$ by Lemma 4.2 since $\approx \circ \mathcal{R} \circ \approx \subseteq \mathcal{R}$.

Now let $\langle M, \rho\rangle \xrightarrow{\alpha} \mu$ where $\alpha \neq \tau$. There are two cases to consider.

(1) $\alpha = \mathsf{c}?q$ is a quantum input. Then $\mu = \langle M', \rho\rangle$ for some M'. So $\langle H(P), \eta\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \mu_1$ such that $\mathcal{E}(\mu) \approx \mathcal{E}(\mu_1)$ for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$. By Theorem 6.10 we further have $\langle H(E(P)), \eta\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \mu_2$ such that $\mathcal{F}(\mu_1) \approx \mathcal{F}(\mu_2)$ for any trace-preserving super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(\mu_1)-\{q\}}}$. Note that X is both sequential and guarded in $H(E(P))$. By repeatedly using Lemma 6.24, we have $\mu_2 = \boxplus_{j\in J} q_j \bullet \langle H_j'(P), \rho_j'\rangle$, and

$$\langle H(E(Q)), \eta\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \nu_2 = \boxplus_{j\in J} q_j \bullet \langle H_j'(Q), \rho_j'\rangle,$$

where H_j' is sequential for any $j \in J$. Using Theorem 6.10 again we have $\langle H(Q), \eta\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \nu_1$ such that $\mathcal{F}'(\nu_2) \approx \mathcal{F}'(\nu_1)$ for any trace-preserving super-operator $\mathcal{F}'$ acting on $\mathcal{H}_{\overline{qv(\nu_2)-\{q\}}}$, and $\langle N, \sigma\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \nu$ such that $\mathcal{E}'(\nu_1) \approx \mathcal{E}'(\nu)$ for any trace-preserving super-operator $\mathcal{E}'$ acting on $\mathcal{H}_{\overline{qv(\nu_1)-\{q\}}}$. Finally, since $qv(\mu) = qv(\mu_1) = qv(\nu_1) = qv(\nu_2)$, we have

$$\mathcal{G}(\mu) \approx \mathcal{G}(\mu_1) \approx \mathcal{G}(\mu_2) \text{ and } \mathcal{G}(\nu_2) \approx \mathcal{G}(\nu_1) \approx \mathcal{G}(\nu)$$

for any trace-preserving super-operator $\mathcal{G}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$. Note that by Lemma 4.3, $\mathcal{G}(\mu_2)\mathcal{R}\mathcal{G}(\nu_2)$. Then $\mathcal{G}(\mu)\mathcal{R}\mathcal{G}(\nu)$ from Lemma 4.2 since $\approx \circ \mathcal{R} \circ \approx \subseteq \mathcal{R}$.

(2) α is a quantum output or classical input/output. Then $\langle H(P), \eta\rangle \overset{\alpha}{\Longrightarrow} \mu_1$, $\mu \approx \mu_1$, and $\langle H(E(P)), \eta\rangle \overset{\alpha}{\Longrightarrow} \mu_2$, $\mu_1 \approx \mu_2$. We further break the actions of $\langle H(E(P)), \eta\rangle$ into

$$\langle H(E(P)), \eta\rangle \Longrightarrow\xrightarrow{\alpha} \mu_3 \Longrightarrow \mu_2.$$

Note that X is both sequential and guarded in $H(E(P))$. By repeatedly using Lemma 6.24, we have $\mu_3 = \boxplus_{i\in K} p_i \bullet \langle H_i'(P), \rho_i\rangle$, and

$$\langle H(E(Q)), \eta\rangle \Longrightarrow\xrightarrow{\alpha} \nu_3 = \boxplus_{i\in K} p_i \bullet \langle H_i'(Q), \rho_i\rangle,$$

where H_i' is sequential. For any $i \in K$, it is obvious that $\langle H_i'(P), \rho_i\rangle \mathcal{R} \langle H_i'(Q), \rho_i\rangle$. So by Eq. (10) we have $\nu_3 \Longrightarrow \nu_2$ such that $\mu_2 \mathcal{R} \nu_2$. We further derive $\langle H(Q), \eta\rangle \overset{\alpha}{\Longrightarrow} \nu_1$, $\nu_2 \approx \nu_1$ and $\langle N, \sigma\rangle \overset{\alpha}{\Longrightarrow} \nu$, $\nu_1 \approx \nu$. Finally, we have $\mu \mathcal{R} \nu$ from $\mu_2 \mathcal{R} \nu_2$.

We have proved that $\mathcal{R}$ is a weak bisimulation. In particular, for any sequential H, $H(P) \approx H(Q)$. Since E is guarded and sequential, every occurrence of X is within some subexpression $a.F$ of E where F is also sequential. Then we have $F(P) \approx F(Q)$, and so $a.F(P) \simeq a.F(Q)$. Thus $E(P) \simeq E(Q)$ by Theorem 6.20. Now the result $P \simeq Q$ follows from $P \simeq E(P)$ and $Q \simeq E(Q)$. □

To illustrate the power of the theorems proved in this section, let us reconsider Example 6.9. We will provide another proof for $\mathcal{U}(U) \circ \mathcal{U}(V) \simeq \mathcal{U}(VU)$ using the Expansion

law and the uniqueness of solutions of equations. For simplicity, we only consider the special case where U and V are both 1-qubit unitary operators. Recall the definition of $\mathcal{U}(U) \circ \mathcal{U}(V)$ in Example 3.6

$$\mathcal{U}(U) \circ \mathcal{U}(V) \stackrel{def}{=} (L_s \| \mathcal{U}(U)[\mathsf{e}/\mathsf{c}, \mathsf{f}/\mathsf{d}] \| \mathcal{U}(V)[\mathsf{f}/\mathsf{c}, \mathsf{g}/\mathsf{d}] \| R_s) \backslash L,$$

where $L = \{c, \mathsf{e}, \mathsf{f}, \mathsf{g}\}$. Then from Theorem 6.22 (1), and repeatedly using Theorems 4.11 and 6.20, we have

$$\mathcal{U}(U) \circ \mathcal{U}(V) \simeq \mathsf{c}?q.\tau.U[q].\tau.V[q].\tau.\mathsf{d}!q.\tau.\mathcal{U}(U) \circ \mathcal{U}(V),$$

where the first τ action is caused by interaction between L_s and $\mathcal{U}(U)[\mathsf{e}/\mathsf{c}, \mathsf{f}/\mathsf{d}]$, the second one between $\mathcal{U}(U)[\mathsf{e}/\mathsf{c}, \mathsf{f}/\mathsf{d}]$ and $\mathcal{U}(V)[\mathsf{f}/\mathsf{c}, \mathsf{g}/\mathsf{d}]$, the third one between $\mathcal{U}(V)[\mathsf{f}/\mathsf{c}, \mathsf{g}/\mathsf{d}]$ and R_s, while the last one between R_s and L_s.

On the other hand, by Theorem 6.22 (1) we have

$$\mathcal{U}(VU) \simeq \mathsf{c}?q.VU[q].\mathsf{d}!q.\mathcal{U}(VU).$$

Now let X be a quantum process variable with $qv(X) = \emptyset$, and

$$E = \mathsf{c}?q.\tau.U[q].\tau.V[q].\tau.\mathsf{d}!q.\tau.X, \qquad F = \mathsf{c}?q.VU[q].\mathsf{d}!q.X$$

be two quantum process expressions. Then E and F are both sequential and guarded, and $E \simeq F$. So we have $\mathcal{U}(U) \circ \mathcal{U}(V) \simeq \mathcal{U}(VU)$ from Theorem 6.25.

7. CONCLUSIONS AND FURTHER WORK

In this article, we propose a formal model qCCS, which is a quantum extension of classical value-passing CCS, to model and rigorously analyze the behaviors of quantum distributed computing and quantum communication protocols. We define notions of strong/weak bisimulations for quantum processes in qCCS, and prove that they are preserved by various process constructors, including parallel composition where both classical and quantum communication are present. These are the first congruent equivalences for process algebras proposed so far aiming at modeling quantum communicating systems. We also propose an approximate version of strong bisimulation to characterize the distance between two quantum processes based on strong bisimulation, even when they are not strongly bisimilar. Various examples are fully examined to show the expressiveness of qCCS as well as the proof techniques presented in this article.

Approximate strong bisimulation has been successfully developed in Section 5. A corresponding notion for weak bisimulation seems, however, very difficult to define. A naive trial is to define a relation $\mathcal{R}$ on Con to be a λ-weak bisimulation if for any $\langle P, \rho\rangle, \langle Q, \sigma\rangle \in Con$, $\langle P, \rho\rangle \mathcal{R} \langle Q, \sigma\rangle$ implies that $qv(P) = qv(Q)$, $d[\mathrm{tr}_{qv(P)}(\rho), \mathrm{tr}_{qv(Q)}(\sigma)] \leq \lambda$, and:

(1) whenever $\langle P, \rho\rangle \xrightarrow{\mathsf{c}?q} \mu$, then $\langle Q, \sigma\rangle \Longrightarrow \xrightarrow{\mathsf{c}?q} \nu$ for some ν such that for any trace-preserving super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu) \mathcal{R}_\lambda \mathcal{E}(\nu)$;

(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q, \sigma\rangle \stackrel{\hat{\alpha}}{\Longrightarrow} \nu$ and $\mu \mathcal{R}_\lambda \nu$;

and the symmetric conditions of (1) and (2). To establish a similar result of Lemma 5.7(1), which is the key for the triangle inequality of the derived bisimulation distance, we naturally require that if $\langle P, \rho\rangle \mathcal{R} \langle Q, \sigma\rangle$ for some λ-weak bisimulation $\mathcal{R}$, then whenever $\langle P, \rho\rangle \stackrel{\alpha}{\Longrightarrow} \mu$ for some $\alpha \neq \tau$, there exists ν such that $\langle Q, \sigma\rangle \stackrel{\alpha}{\Longrightarrow} \nu$ and $\mu \mathcal{R}_\lambda \nu$. However, this property does not hold in general. To see this, suppose

$\langle P, \rho\rangle \xrightarrow{\tau} \mu' \xrightarrow{\alpha} \mu$, and $\langle Q, \sigma\rangle \stackrel{\alpha}{\Longrightarrow} \nu'$ is the weak transition $\langle Q, \sigma\rangle$ takes to match the action $\langle P, \rho\rangle \xrightarrow{\tau} \mu'$, and $\mu' \mathcal{R}_\lambda \nu'$. However, the conditions that $\mu' \mathcal{R}_\lambda \nu'$ and $\mu' \xrightarrow{\alpha} \mu$ do not necessarily imply that $\nu' \stackrel{\alpha}{\Longrightarrow} \nu$ for some ν; they only guarantee that a portion of ν with the probability weight not less than $1 - \lambda$ can perform a weak α-action. Furthermore, even such a ν exists, we can only infer $\mu \mathcal{R}_{2\lambda} \nu$ from $\mu' \mathcal{R}_\lambda \nu'$ but not $\mu \mathcal{R}_\lambda \nu$ as expected. That is, the imperfection, or error, which is allowed by approximate bisimulation will accumulate during the execution of weak transitions.

Another interesting direction worth researching is to expand the application scope of qCCS to model and analyze the security properties of quantum cryptographic systems. By introducing cryptographic primitives, such as constructors for encryption and decryption, into pi-calculus, the Spi calculus [Abadi and Gordon 1997] has been very successful in cryptographic protocol analysis. We believe that a similar extension of our qCCS will provide tools for analyzing quantum cryptographic protocols such as BB84 quantum key distribution protocol.

ACKNOWLEDGMENTS

The authors thank Professor Prakash Panangaden and Dr. Yuxin Deng for their generous comments and suggestions. In particular, Yuxin pointed out a flaw in the definition of weak transitions in our POPL paper and suggested to us that we adopt the combined version as in Definition 6.1 of the current article. The reviewers of POPL'11 are also acknowledged for their comments which have improved the presentation and the quality of the article.

REFERENCES

ABADI, M. AND GORDON, A. D. 1997. A calculus for cryptographic protocols: The spi calculus. In *Proceedings of the 4th ACM Conference on Computer and Communications Security*. ACM, 36–47.

BAIER, C. AND HERMANNS, H. 1997. Weak bisimulation for fully probabilistic processes. In *Proceedings of the International Conference on Computer Aided Verification (CAV'97)*. Lecture Notes in Computer Science, vol. 1254, Springer, 119–130.

BAIER, C. AND KWIATKOWSKA, M. 2000. Domain equations for probabilistic processes. *Math. Struct. Comput. Sci. 10*, 665–717.

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

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

DENG, Y. AND DU, W. 2011. Logical, metric, and algorithmic characterisations of probabilistic bisimulation. arxiv:1103.4577v1 [cs.lo].

DENG, Y., PALAMIDESSI, C., AND PANG, J. 2005. Compositional reasoning for probabilistic finite-state behaviors. In *Processes, Terms and Cycles: Steps on the Road to Infinity*. 309–337.

DENG, Y., CHOTHIA, T., PALAMIDESSI, C., AND PANG, J. 2006. Metrics for action-labelled quantitative transition systems1. *Electron. Not. Theor. Comput. Sci. 153,* 2, 79–96.

DENG, Y., VAN GLABBEEK, R., HENNESSY, M., MORGAN, C., AND ZHANG, C. 2007. Remarks on testing probabilistic processes. *Electron. Not. Theor. Comput. Sci. 172*, 359–397.

DESHARNAIS, J., GUPTA, V., JAGADEESAN, R., AND PANANGADEN, P. 2002. Weak bisimulation is sound and complete for PCTL*. In *Proceedings of the International Conference on Concurrency Theory (CONCUR)*. 355–370.

DESHARNAIS, J., GUPTA, V., JAGADEESAN, R., AND PANANGADEN, P. 2004. Metrics for labelled markov processes. *Theor. Comput. Sci. 318,* 3, 323–354.

DESHARNAIS, J., GUPTA, V., JAGADEESAN, R., AND PANANGADEN, P. 2010. Weak bisimulation is sound and complete for PCTL*. *Inf. Comput. 208,* 2, 203–219.

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

FENG, Y., DUAN, R., AND YING, M. 2011. Bisimulations for quantum processes. In *Proceedings of the 38th ACM Symposium on Principles of Programming Languages (POPL'11)*, M. Sagiv Ed., 523–534.

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

GIACALONE, A., JOU, C., AND SMOLKA, S. 1990. Algebraic reasoning for probabilistic concurrent systems. In *Proceedings of the IFIP WG 2.2/2.3 Working Conference on Programming Concepts and Methods*. North-Holland, Amsterdam, 443–458.

GROVER, L. K. 1997. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett. 78,* 2, 325.

HENNESSY, M. 1991. A proof system for communicating processes with value-passing. *Formal Aspects of Comput. Sci. 3*, 346–366.

HENNESSY, M. AND INGÓLFSDÓTTIR, A. 1993. A theory of communicating processes with value-passing. *Inf. Comput. 107,* 2, 202–236.

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

KITAEV, A. 1997. Quantum computations: Algorithms and error correction. *Russ. Math. Surv. 52,* 6, 1191–1249.

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

LALIRE, M. 2006. Relations among quantum processes: Bisimilarity and congruence. *Math. Struct. Comput. Sci. 16*, 3, 407–428.

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

MILNER, R., PARROW, J., AND WALKER, D. 1992. A calculus of mobile processes, parts I and II. *Inf. Comput. 100*, 1–77.

NIELSEN, M. AND CHUANG, I. 2000. *Quantum Computation and Quantum Information*. Cambridge University Press.

SHOR, P. W. 1994. Algorithms for quantum computation: Discrete log and factoring. In *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science (FOCS'94)*. 124–134.

VAN BREUGEL, F. 2010. http://www.sti.uniurb.it/events/sfm10qapl/slides/franck-part1.pdf.

VON NEUMANN, J. 1955. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Princeton, NJ.

YING, M., FENG, Y., DUAN, R., AND JI, Z. 2009. An algebra of quantum processes. *ACM Trans. Comput. Logic 10,* 3, 1–36.

YING, M. S. 2001. *Topology in Process Calculus: Approximate Correctness and Infinite Evolution of Concurrent Programs*. Springer New York.

YING, M. S. 2002. Bisimulation indexes and their applications. *Theor. Comput. Sci. 275*, 1–68.

Received April 2011; revised March 2012; accepted November 2012