An Algebra of Quantum Processes

MINGSHENG YING

Tsinghua University and University of Technology, Sydney

and

YUAN FENG and RUNYAO DUAN

Tsinghua University

and

ZHENGFENG JI

Institute of Software, Chinese Academy of Sciences

We introduce an algebra qCCS of pure quantum processes in which communications by moving quantum states physically are allowed and computations are modeled by super-operators, but no classical data is explicitly involved. An operational semantics of qCCS is presented in terms of (non-probabilistic) labeled transition systems. Strong bisimulation between processes modeled in qCCS is defined, and its fundamental algebraic properties are established, including uniqueness of the solutions of recursive equations. To model sequential computation in qCCS, a reduction relation between processes is defined. By combining reduction relation and strong bisimulation we introduce the notion of strong reduction-bisimulation, which is a device for observing interaction of computation and communication in quantum systems. Finally, a notion of strong approximate bisimulation (equivalently, strong bisimulation distance) and its reduction counterpart are introduced. It is proved that both approximate bisimilarity and approximate reduction-bisimilarity are preserved by various constructors of quantum processes. This provides us with a formal tool for observing robustness of quantum processes against inaccuracy in the implementation of its elementary gates.

---

1. INTRODUCTION

Quantum information science is usually divided into two subareas: quantum computation and quantum communication. Quantum computation offers the possibility of considerable speedup over classical computation by exploring the power of superposition of quantum states. Two striking examples of quantum algorithms are Shor's quantum factoring and Grover's quantum searching. On the other hand, some communication protocols are proposed by employing quantum mechanical principles (in particular, the no-cloning property and entanglement), for example BB84 and B92, which are provably secure. Quantum communication systems using these protocols are already commercially available from Id Quantique, MagiQ Technologies and NEC.

The studies of quantum process algebras allow us to glue the two subareas of quantum information science. To provide formal techniques for modeling, analysis and verification of quantum communication protocols, Gay and Nagarajan [5], [6] defined a language CQP (Communicating Quantum Processes), which is obtained from the pi-calculus by adding primitives for measurements and transformations of quantum states and allowing transmission of qubits. They gave an operational semantics and presented a type system for CQP, and in particular proved that the semantics preserves typing and that typing guarantees that each qubit is owned by a unique process within a system. To model concurrent quantum computation, Jorrand and Lalire [7], [8], [11], [12] defined a language QPAlg (Quantum Process Algebra). It is obtained by adding primitives expressing unitary transformations and quantum measurements, as well as communications of quantum states, to a classical process algebra, which is similar to CCS. An operational semantics of QPAlg is given, and further a probabilistic branching bisimulation between quantum processes modeled in QPAlg is defined.

In this paper, we introduce a new algebra of quantum processes, qCCS, which is a quantum generalization of CCS. The design decision of qCCS differs from that of the previous quantum process algebras in the following two aspects: (1) The driving idea of the design of CQP is to provide formal model for analyzing quantum communication protocols. Almost all of the existing quantum protocols involve transmission of both classical and quantum data. The purpose of designing QPAlg is to model cooperation between quantum and classical computations. Thus, these quantum process algebras have to accommodate quantum communication as well as classical communication. The aim of the present paper is different, and we mainly want to provide a suitable framework in which we can understand the mechanism of quantum concurrent computation and observe interaction and conjugation of computation and communication in quantum systems. At the first step, it is reasonable to isolate quantum data from classical data so that we have a much simpler model in which a clearer understanding of quantum concurrent computation may be achieved. So, we decide to focus our attention on an algebra of purely quantum processes, not involving any classical information. Of course, in the future, after we have a thorough understanding of purely quantum processes, qCCS can be extended by adding classical ingredients. (2) The mathematical tools used to describe transformations of quantum states in the previous quantum process algebras are unitary operators. According the basic postulates of quantum mechanics, unitary operators are suited to depict the dynamics of closed

quantum systems, but a more suitable mathematical formalism for evolution of open quantum systems is given in terms of super-operators. Since quantum process algebras are mainly applied in modeling quantum concurrent systems in which interactions between their subsystems happen frequently, and it seems more reasonable to treat the involved systems as open systems, we choose to use super-operators in describing transformations of quantum states. Indeed, the usage of super-operators in qCCS was influenced by Selinger's denotational semantics for his quantum functional programming language QPL [16].

There are still some technical differences between qCCS and the previous quantum process algebras. First, the treatment of quantum variables and their substitutions is a key ingredient in defining the operational and bisimulation semantics of qCCS. This was not addressed in the previous works. It was already realized in [4], [5], [6], [7], [8], [11], [12] that one should consider passing of the quantum systems used to express certain quantum information instead of passing of the quantum information itself, due to the no-cloning property of quantum information [18]. Hence, quantum variables must be explicitly introduced to denote the quantum systems under consideration. In treating quantum variables in qCCS, we follow the way of manipulating names in the pi-calculus [14]. But a serious difference is that distinct quantum variables cannot be substituted by the same quantum variable, complying with, again, the no-cloning theorem of quantum information. Second, as in classical process algebras, operational semantics of quantum processes is presented in terms of transitions between configurations. However, a quantum variable and its current state have to be separated in order to avoid abuse of quantum information which may violate the no-cloning theorem. Thus, a quantum configuration defined in [4], [5], [6], [7], [8], [11], [12] consists of a quantum process together with state information of the involved quantum variables. In this paper, a configuration is required to record state information of all quantum variables (not only those occurring in the process under consideration). Although a configuration defined in this way includes some unnecessary information, it allows us to simplify considerably our presentation. (Note that such a simple idea is widely used in mathematical logic; for example, it simplifies the presentation of propositional logic in the following way: in evaluating a given propositional formula we only need to know the truth values assigned to the propositional variables occurring in this formula, but a truth valuation is generally defined to be an assignment of truth values to all propositional variables.) Third, in the previous works [4], [5], [6], [7], [8], [11], [12], the operational semantics of a quantum process algebra is always defined to be a probabilistic transition system, but this paper presents a non-probabilistic operational semantics of qCCS. This is realized by treating quantum measurements as super-operators (see Example 2.5(2) and (3)), and it considerably simplifies the bisimulation semantics of qCCS. Nevertheless, probabilistic information still can be retrieved from such a non-probabilistic semantics via Eq. (1) below. Fourth, only the notion of exact bisimulation is generalized to quantum processes in [4], [11]. Recall that a set of classical gates is universal if it can be used to compute exactly an arbitrary boolean function. However, exact universality does not make sense in quantum computation because all quantum gates form a continuum which cannot be generated by a finite set of quantum gates. Instead, a set of quantum gates is said to be universal provided any quantum gate can be approximated to arbitrary accuracy by a circuit constructed from the gates in this set. To describe approximation between quantum processes and, in particular, implementation of a quantum process by some (usually finitely many) special quantum gates, an approximate version of bisimulation (or

equivalently, bisimulation distance) is still missing. Recently, the first author [19], [20], [21] and van Breugel [17] among others introduced the notion of approximate bisimulation for classical processes in which a distance between actions is presumed. In the present paper, both exact and approximate bisimulations are defined in qCCS, the latter using a distance between super-operators induced naturally from the trace distance of quantum states. We believe that approximate bisimulations are appropriate formal tools for analyzing robustness of quantum processes against inaccuracy in the implementation of its elementary gates.

This paper is organized as follows: Section 2 reviews some basic notions, needed in the subsequent sections, from quantum theory. In Section 3 we define the syntax and an operational semantics of qCCS and give some simple examples to illustrate the expressive power of qCCS. The notion of strong bisimulation between quantum processes is introduced, monoid and expansion laws as well as congruence and recursive properties of strong bisimilarity are established, and uniqueness of solutions of equations with respect to strong bisimilarity is presented in Section 4. In Section 5, we first define a reduction relation between strings of quantum operations and then extend it to a reduction between quantum processes. The notion of strong reduction-bisimilarity is defined by combining reduction relation and strong bisimilarity, and it is shown to be congruent under the process constructors in qCCS. In Section 6, the notions of approximate strong bisimilarity and reduction-bisimilarity are proposed and their corresponding metrics are defined. It is proved that all process constructors are non-expansive with respect to both strong bisimulation metric and reduction-bisimulation metric. Section 7 is the concluding section where we draw a brief conclusion and mention some topics for further studies. For readability, we put the detailed proofs of some propositions in the Appendix.

2. PRELIMINARIES

For convenience of the reader we briefly recall some basic notions from quantum theory and fix the notations needed in the sequel. We refer to [15] for more details.

2.1 Hilbert spaces

An isolated physical system is associated with a Hilbert space which is called the state space of the system. In this paper, we mainly consider finite-dimensional and countably infinite-dimensional Hilbert spaces. A finite-dimensional Hilbert space is a complex vector space $\mathcal{H}$ together with an inner product which is a mapping $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbf{C}$ satisfying the following properties:

(1) $\langle \varphi | \varphi \rangle \geq 0$ with equality if and only if $|\varphi\rangle = 0$;

(2) $\langle \varphi | \psi \rangle = \langle \psi | \varphi \rangle^*$;

(3) $\langle \varphi | \lambda_1 \psi_1 + \lambda_2 \psi_2 \rangle = \lambda_1 \langle \varphi | \psi_1 \rangle + \lambda_2 \langle \varphi | \psi_2 \rangle$,

where $\mathbf{C}$ is the set of complex numbers, and λ^* stands for the conjugate of λ for each complex number $\lambda \in \mathbf{C}$. All countably infinite-dimensional Hilbert spaces considered in this paper will be simply treated as tensor products of countably infinitely many finite-dimensional Hilbert spaces (see Subsection 2.4 below).

EXAMPLE 2.1. *Let $n \geq 1$. For any $|\varphi\rangle = (x_1, ..., x_n)^T, |\psi\rangle = (y_1, ..., y_n)^T \in \mathbf{C}^n$ and $\lambda \in \mathbf{C}$, we define:*

$$|\varphi\rangle + |\psi\rangle = (x_1 + y_1, ..., x_n + y_n)^T,$$

$$\lambda|\varphi\rangle = (\lambda x_1, ..., \lambda x_n)^T,$$

where ^{T} stands for transpose. Then $\mathbf{C}^n$ is a vector space. We often write $\langle\varphi|$ for the adjoint $|\varphi\rangle^\dagger$ of $|\varphi\rangle$. Furthermore, we define $\langle\cdot|\cdot\rangle$ in $\mathbf{C}^n$ as follows:

$$\langle\varphi|\psi\rangle = \sum_{i=1}^{n} x_i^* y_i.$$

Then $(\mathbf{C}^n, \langle\cdot|\cdot\rangle)$ is an $n-$dimensional Hilbert space. Indeed, each $n-$dimensional Hilbert space is isometric to $\mathbf{C}^n$. In particular, a qubit is a physical system whose state space is $\mathcal{H}_2 = \mathbf{C}^2$. If we write $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, corresponding to one-bit classical values and called the computational basis, then a qubit has state $\alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbf{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. The Hadamard basis consists of the following two states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

For any vector $|\psi\rangle$ in $\mathcal{H}$, its length $||\psi||$ is defined to be $\sqrt{\langle\psi|\psi\rangle}$. A pure state of a quantum system is a unit vector in its state space; that is, a vector $|\psi\rangle$ with $||\psi|| = 1$. An orthonormal basis of a Hilbert space $\mathcal{H}$ is a basis $\{|i\rangle\}$ with

$$\langle i|j\rangle = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$$

Then the trace of a linear operator A on $\mathcal{H}$ is defined to be

$$tr(A) = \sum_i \langle i|A|i\rangle.$$

A mixed state of quantum system is represented by a density operator. A density operator in a Hilbert space $\mathcal{H}$ is a linear operator ρ on it fulfilling the following conditions:

(1) ρ is positive in the sense that $\langle\psi|\rho|\psi\rangle \geq 0$ for all $|\psi\rangle$;
(2) $tr(\rho) = 1$.

An equivalent concept of density operator is an ensemble of pure states. An ensemble is a set of the form $\{(p_i, |\psi_i\rangle)\}$ such that $p_i \geq 0$ and $|\psi_i\rangle$ is a pure state for each i, and $\sum_i p_i = 1$. Then

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$$

is a density operator, and conversely each density operator can be generated by an ensemble of pure states in this way. A positive operator ρ is called a partial density operator if $tr(\rho) \leq 1$. We write $\mathcal{D}(\mathcal{H})$ for the set of partial density operators on $\mathcal{H}$.

2.2 Unitary operators

The evolution of a closed quantum system is described by a unitary operator on its state space. A linear operator U on a Hilbert space $\mathcal{H}$ is said to be unitary if $U^\dagger U = I_\mathcal{H}$, where $I_\mathcal{H}$ is the identity operator on $\mathcal{H}$, and $U^\dagger$ is the adjoint of U. If the states of the system at times t_1 and t_2 are ρ_1 and ρ_2, respectively, then

$$\rho_2 = U\rho_1 U^\dagger$$

for some unitary operator U which depends only on t_1 and t_2. In particular, if ρ_1 and ρ_2 are pure states $|\psi_1\rangle$ and $|\psi_2\rangle$, respectively; that is, $\rho_1 = |\psi_1\rangle\langle\psi_1|$ and $\rho_2 = |\psi_2\rangle\langle\psi_2|$, then we have $|\psi_2\rangle = U|\psi_1\rangle$.

EXAMPLE 2.2. *The most frequently used unitary operators on qubits are the Hadamard transformation:*

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

and the Pauli matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

2.3 Quantum measurement

A quantum measurement is described by a collection $\{M_m\}$ of measurement operators, where the indexes 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

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

and the state of the system after the measurement is

$$\frac{M_m \rho M_m^\dagger}{p(m)}.$$

For the case that ρ is a pure state $|\psi\rangle$, we have $p(m) = ||M_m|\psi\rangle||^2$, and the post-measurement state is

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}.$$

EXAMPLE 2.3. *The measurement on qubits in the computational basis consists of $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$. If we perform it on a qubit which is in state $\alpha|0\rangle + \beta|1\rangle$, then either the result 0 will be obtained, with probability $|\alpha|^2$, or the result 1, with probability $|\beta|^2$.*

2.4 Tensor products

The state space of a composite system is the tensor product of the state spaces of its components. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces. Then their tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ consists of linear combinations of vectors $|\psi_1\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$.

For any linear operator A_1 on $\mathcal{H}_1$ and A_2 on $\mathcal{H}_2$, $A_1 \otimes A_2$ is an operator on $\mathcal{H}_1 \otimes \mathcal{H}_2$ and it is defined by

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

for each $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$.

Let $|\varphi\rangle = \sum_i \alpha_i |\varphi_{1i}\varphi_{2i}\rangle$ and $|\psi\rangle = \sum_j \beta_j |\psi_{1j}\psi_{2j}\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Then their inner product is defined as follows:

$$\langle\varphi|\psi\rangle = \sum_{i,j} \alpha_i^* \beta_j \langle\varphi_{1i}|\psi_{1j}\rangle \langle\varphi_{2i}|\psi_{2j}\rangle.$$

EXAMPLE 2.4. *A composite quantum system can exhibit the phenomenon of entanglement. A state of a composite system is an entangled state if it cannot be written as a product of states of its component systems. The following are maximally entangled states of two-qubits, called Bell states:*

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

The notion of tensor product may be easily generalized to the case of any finite number of Hilbert spaces. The tensor product of countably infinitely many finite-dimensional Hilbert spaces is a countably infinite-dimensional Hilbert space isometric to l^2 of sequences $\{x_n\}_{n=0}^{\infty}$ of complex numbers such that $\sum_{n=0}^{\infty} |x_n|^2$ converges. The vector addition, scalar multiplication and inner product are defined as follows:

$$|\varphi\rangle + |\psi\rangle = \{x_n + y_n\}_{n=0}^{\infty},$$

$$\lambda|\varphi\rangle = \{\lambda x_n\}_{n=0}^{\infty},$$

$$\langle\varphi|\psi\rangle = \sum_{n=0}^{\infty} x_n^* y_n$$

for any $|\varphi\rangle = \{x_n\}_{n=0}^{\infty}, |\psi\rangle = \{y_n\}_{n=0}^{\infty} \in l^2$ and $\lambda \in \mathbf{C}$. It is easy to see that l^2 enjoys the following completeness: if $\{|\varphi_n\rangle\}_{n=0}^{\infty}$ is a Cauchy sequence in l^2, i.e. for any $\epsilon > 0$, there exists positive integer N such that $||\varphi_m - \varphi_n|| < \epsilon$ for all $m, n \geq N$, then exists $|\varphi\rangle \in l^2$ with $\lim_{n\to\infty} |\varphi_n\rangle = |\varphi\rangle$, i.e. for any $\epsilon > 0$, there exists positive integer N such that $||\varphi_n - \varphi|| < \epsilon$ for all $n \geq N$.

The notion of tensor product of two linear operators can be generalized to the case of more than two operators and the case of countably infinitely many operators in a natural way. Since density operators are special linear operators, their tensor product is then well-defined. A basic postulate of quantum mechanics asserts that if component system i is in state ρ_i for each i, then the state of the composite system is $\bigotimes_i \rho_i$.

2.5 Super-operators

The dynamics of open quantum systems cannot be described by unitary operators, and one of its mathematical formalisms is the notion of super-operator. A super-operator on a Hilbert space $\mathcal{H}$ is a linear operator $\mathcal{E}$ from the space of linear operators on $\mathcal{H}$ into itself which satisfies the following two conditions:

(1) $tr[\mathcal{E}(\rho)] \leq tr(\rho)$ for each $\rho \in \mathcal{D}(\mathcal{H})$;
(2) Complete positivity: for any extra Hilbert space $\mathcal{H}_R$, $(\mathcal{I}_R \otimes \mathcal{E})(A)$ is positive provided A is a positive operator on $\mathcal{H}_R \otimes \mathcal{H}$, where $\mathcal{I}_R$ is the identity operation on $\mathcal{H}_R$.

If (1) is strengthened to $tr[\mathcal{E}(\rho)] = tr(\rho)$ for all $\rho \in \mathcal{D}(\mathcal{H})$, then $\mathcal{E}$ is said to be trace-preserving.

EXAMPLE 2.5. (*1*) *Let U be a unitary operator on Hilbert space $\mathcal{H}$, and $\mathcal{E}(\rho) = U\rho U^\dagger$ for any $\rho \in \mathcal{D}(\mathcal{H})$. Then $\mathcal{E}$ is a trace-preserving super-operator.*

(2) *Let $\{M_m\}$ be a quantum measurement on $\mathcal{H}$. For each m, we define $\mathcal{E}_m(\rho) = M_m \rho M_m^\dagger$ for any $\rho \in \mathcal{D}(\mathcal{H})$. Then $\mathcal{E}_m$ is a super-operator, which is not necessarily trace-preserving. If the state of the system immediately before the measurement is ρ, then the probability of obtaining measurement result m is*

$$p(m) = tr(\mathcal{E}_m(\rho)), \tag{1}$$

and the state of the system immediately after the measurement is

$$\mathcal{E}_m(\rho)/tr(\mathcal{E}_m(\rho)).$$

(3) *As in (2), let $\{M_m\}$ be a quantum measurement on $\mathcal{H}$. If $\mathcal{E}$ is given by this measurement, with the result of the measurement unknown, i.e.,*

$$\mathcal{E}(\rho) = \sum_m M_m \rho M_m^\dagger$$

for each $\rho \in \mathcal{D}(\mathcal{H})$, then $\mathcal{E}$ is a trace-preserving super-operator.

The following theorem gives two elegant representations of super-operators.

LEMMA 2.1. *([15], Section 8.2.3; Theorem 8.1) The following three statements are equivalent:*

(*1*) *$\mathcal{E}$ is a super-operator on Hilbert space $\mathcal{H}$;*

(2) *(System-environment model) There are an environment system E with state space $\mathcal{H}_E$, and a unitary transformation U and a projector P on $\mathcal{H} \otimes \mathcal{H}_E$ such that*

$$\mathcal{E}(\rho) = tr_E[PU(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P]$$

for any $\rho \in \mathcal{D}(\mathcal{H})$, where $\{|e_k\rangle\}$ is an orthonormal basis of $\mathcal{H}_E$, and $tr_E(\cdot)$ is defined by

$$tr_E(\sigma) = \sum_k \langle e_k|\sigma|e_k\rangle$$

for any $\sigma \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H}_E)$;

(3) *(Kraus operator-sum representation) There exists a set of operators $\{E_i\}$ on $\mathcal{H}$ such that $\sum_i E_i^\dagger E_i \sqsubseteq I$ and*

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

for all density operators $\rho \in \mathcal{D}(\mathcal{H})$, where $\sqsubseteq$ stands for the Löwner order; that is, $A \sqsubseteq B$ if and only if $B - A$ is a positive operator. We often say that $\mathcal{E}$ is represented by the set $\{E_i\}$ of operators, or $\{E_i\}$ are operation elements giving rise to $\mathcal{E}$ when $\mathcal{E}$ is given by the above equation.

2.6 Diamond distance between super-operators

We shall need a distance between super-operators in defining approximate bisimulation between quantum processes. We choose to use a natural extension of trace distance between mixed quantum states. For any positive operator A, if $A = \sum_i \lambda_i |i\rangle\langle i|$, $\lambda_i \geq 0$ for all i, is a spectral decomposition of A, then we define

$$\sqrt{A} = \sum_i \sqrt{\lambda_i} |i\rangle\langle i|.$$

Furthermore, for any operator A, we define $|A| = \sqrt{A^\dagger A}$. One of the most popular metrics measuring how close two quantum states are, used by the quantum information community, is trace distance. For any $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, their trace distance is defined to be

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

$D(\rho, \sigma)$ quantifies the distinguishability between mixed states ρ and σ. The following property of trace distance is needed in the sequel.

LEMMA 2.2. *([15], Theorem 9.2) If $\mathcal{E}$ is a trace-preserving super-operator on $\mathcal{H}$, then*

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D(\rho, \sigma)$$

for any $\rho, \sigma \in \mathcal{D}(\mathcal{H})$.

The notion of trace distance can be extended to the case of super-operators in a natural way [10]. For any super-operators $\mathcal{E}_1$, $\mathcal{E}_2$ on $\mathcal{H}$, their diamond trace distance is defined to be

$$D_\diamond(\mathcal{E}_1, \mathcal{E}_2) = \sup\{D((\mathcal{E}_1 \otimes \mathcal{I}_{\mathcal{H}'})(\rho), (\mathcal{E}_2 \otimes \mathcal{I}_{\mathcal{H}'})(\rho)) : \rho \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H}')\}$$

where $\mathcal{H}'$ ranges over all finite-dimensional Hilbert spaces. $D_\diamond(\mathcal{E}_1, \mathcal{E}_2)$ 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. SYNTAX AND OPERATIONAL SEMANTICS

3.1 Syntax

Let $Chan$ be the set of names for quantum channels, and let Var be the set of quantum variables. It is assumed that Var is a countably infinite set. We shall use meta-variables $c, d, ...$ to range over $Chan$ and $x, y, z, ...$ to range over Var. Let τ be the name of silent action.

For each quantum variable $x \in Var$, imagine that we have a quantum system named by x. Let $\mathcal{H}_x$ be a finite-dimensional complex Hilbert space, which is the state space of the $x-$system. For any $x, y \in Var$, if $\mathcal{H}_x = \mathcal{H}_y$, then it is said that x and y have the same type. Imagine further that there is a big quantum system composed of all $x-$systems, $x \in Var$, in which all of our quantum processes live. We call this composed system the environment of our calculus. Put

$$\mathcal{H}_X = \bigotimes_{x \in X} \mathcal{H}_x$$

for any $X \subseteq Var$. Then $\mathcal{H} = \mathcal{H}_{Var}$ is the state space of the environment. Note that $\mathcal{H}$ is a countably infinite-dimensional Hilbert space.

We assume a set of process constant schemes, ranged over by meta-variables $A, B, ...$ For each process constant A, a nonnegative arity $ar(A)$ is assigned to it. Let $\widetilde{x} = x_1, ..., x_{ar(A)}$ be a tuple of distinct quantum variables. Then $A(\widetilde{x})$ is called a process constant.

We write $\mathcal{P}$ for the set of quantum processes, and we write $fv(P)$ for the set of free quantum variables in P for each quantum process $P \in \mathcal{P}$. Now we are ready to present the syntax of qCCS.

DEFINITION 3.1. *Quantum processes are defined inductively by the following formation rules:*

(1) *each process constant $A(\widetilde{x})$ is in $\mathcal{P}$ and $fv(A(\widetilde{x})) = \{\widetilde{x}\}$;*

(2) $\mathbf{nil} \in \mathcal{P}$ *and* $fv(\mathbf{nil}) = \emptyset$;

(3) *if $P \in \mathcal{P}$, then $\tau.P \in \mathcal{P}$ and $fv(\tau.P) = fv(P)$;*

(4) *if $P \in \mathcal{P}$, X is a finite subset of Var, and $\mathcal{E}$ is a super-operator on $\mathcal{H}_X$, then $\mathcal{E}[X].P \in \mathcal{P}$ and $fv(\mathcal{E}[X].P) = fv(P) \cup X$;*

(5) *if $P \in \mathcal{P}$, then $c?x.P \in \mathcal{P}$, and $fv(c?x.P) = fv(P) - \{x\}$;*

(6) *if $P \in \mathcal{P}$ and $x \notin fv(P)$, then $c!x.P \in \mathcal{P}$, and $fv(c!x.P) = fv(P) \cup \{x\}$;*

(7) *if $P, Q \in \mathcal{P}$, then $P + Q \in \mathcal{P}$ and $fv(P + Q) = fv(P) \cup fv(Q)$;*

(8) *if $P, Q \in \mathcal{P}$ and $fv(P) \cap fv(Q) = \emptyset$, then $P\|Q \in \mathcal{P}$ and $fv(P\|Q) = fv(P) \cup fv(Q)$;*

(9) *if $P \in \mathcal{P}$ and $L \subseteq Chan$, then $P\backslash L \in \mathcal{P}$ and $fv(P\backslash L) = fv(P)$.*

Using the standard BNF grammar the syntax of qCCS can be summarized as follows:

$$P ::= A(\widetilde{x}) \mid \mathbf{nil} \mid \tau.P \mid \mathcal{E}[X].P \mid c?x.P \mid c!x.P \mid P + P \mid P\|P \mid P\backslash L.$$

It is similar to the syntax of classical CCS, and the only differences between them are:

— Clause 4 in the above definition allows us to perform quantum operations on some involved systems;

— Condition $x \notin fv(P)$ in clause 6 and condition $fv(P) \cap fv(Q) = \emptyset$ in clause 8 are required due to the well-known fact that unknown quantum information cannot be perfectly cloned [18].

It is worth noting that these conditions force us to assign a set of free quantum variables to each process constant in advance. Quantum operations described in clause 4 may be thought of as constructs for sequential quantum computation. There are also constructs for sequential computation in the value-passing CCS, but they are not explicitly given. There such constructs are implicitly assumed in value expressions (see [13], page 55) so that one can focus his attention on examining communication behaviors between processes. However, we explicitly present the constructs for sequential quantum computation in the syntax of qCCS, and it is one of our main purposes to observe interaction between sequential quantum computation and communication of quantum information.

There are two kinds of binding in our language for quantum processes: the restriction $\backslash L$ binds all channel names in L, and the input prefix $c?x$ binds quantum variable x. The symbol $\equiv_\alpha$ will be used to denote alpha-convertibility on processes defined by replacing bound quantum variables in the standard way.

For each process constant scheme A, a defining equation of the form

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

is assumed, where P is a process with $fv(P) \subseteq \{\widetilde{x}\}$. Recursive definition in qCCS is different from that in classical CCS in some intricate way. For example, in qCCS,

$$A(x) \stackrel{def}{=} c!x.A(x)$$

is not allowed to be the defining equation of process constant scheme A. In fact, if $x \in fv(A(x))$ then $c!x.A(x)$ is not a process, and if $x \notin fv(A(x))$ then $fv(c!x.A(x)) \not\subseteq fv(A(x))$. However,

$$A(y) \stackrel{def}{=} c?x.c!x.A(y)$$

is a legitimate defining equation of A.

It is well-known that in the pi-calculus one has to treat substitution of names very carefully. However, we need to treat substitution of quantum variables in an even more careful way due to the fact that arbitrary cloning of quantum information is prohibited [18], [2]. In particular, we have:

DEFINITION 3.2. *A substitution of quantum variables is a one-to-one mapping f from Var into itself satisfying*

(1) *x and $f(x)$ have the same type for all $x \in Var$; and*
(2) *$f|_{Var-X} = Id_{Var-X}$ for some finite subset X of Var, where Id_Y stands for the identity function on Y.*

It is common that two different classical variables can be substituted by the same variable. But it is not the case in qCCS because a substitution is required to be a bijection. Such a requirement comes reasonably from our intention that different variables are references to different quantum systems. Since quantum variable $f(x)$ will be used to substitute quantum variable x, it is reasonable to require that the $x-$system and the $f(x)-$system have the same state space. This is exactly condition (1) in the above definition.

Let $P \in \mathcal{P}$ and f be a substitution. Then Pf denotes the process obtained from P by simultaneously substituting $f(x)$ for each free occurrence of x in P for all x. To give a precise definition of Pf, we need to introduce the notion of application of a substitution on a super-operator. If f is a one-to-one mapping from Var into itself, then f induces naturally an isomorphism from $\mathcal{H}$ onto $\mathcal{H}_{f(Var)}$, which is a subspace of $\mathcal{H}$. For simplicity, it is also denoted by f. Precisely, the isomorphism $f : \mathcal{H} \to \mathcal{H}_{f(Var)}$ is defined as follows:

$$f(\bigotimes_{x \in Var} |\varphi_x\rangle_x) = \bigotimes_{x \in Var} |\varphi_x\rangle_{f(x)}$$

for any $|\varphi_x\rangle \in \mathcal{H}_x$, $x \in Var$. Applying f to a state which is not a tensor product of states in $\mathcal{H}_x$ ($x \in Var$) may be carried out simply by linearity. Furthermore, it induces a bijection $f : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H}_{f(Var)})$. For any $\rho = \sum_i p_i|\varphi_i\rangle\langle\varphi_i| \in \mathcal{D}(\mathcal{H})$, where $|\varphi_i\rangle \in \mathcal{H}$ for all i, we have:

$$f(\rho) = \sum_i p_i|f(\varphi_i)\rangle\langle f(\varphi_i)|.$$

In particular, if $f(x) = y$, $f(y) = x$ and $f(z) = z$ for all $z \neq x, y$, then $f(\rho)$ is often written as $\rho\{y/x\}$.

For any super-operator $\mathcal{E}$ on $\mathcal{H}_X$, we define super-operator $\mathcal{E}f$ on $\mathcal{H}_{f(X)}$ by

$$\mathcal{E}f = f|_X \circ \mathcal{E} \circ (f|_X)^{-1},$$

where $f|_X$ is the restriction of f on X, which is obviously a bijection from X onto $f(X)$.

$$
\begin{array}{ccc}
\mathcal{D}(\mathcal{H}_X) & \xrightarrow{\mathcal{E}} & \mathcal{D}(\mathcal{H}_X) \\[2mm]
f \downarrow & & \downarrow f \\[2mm]
\mathcal{D}(\mathcal{H}_{f(X)}) & \xrightarrow[\mathcal{E}f]{} & \mathcal{D}(\mathcal{H}_{f(X)})
\end{array}
$$

With the above preliminaries, now we are able to define substitution of quantum variables in a quantum process.

DEFINITION 3.3. *For any $P \in \mathcal{P}$ and substitution f, Pf is defined recursively as follows:*

(1) *if P is a process constant $A(x_1, ..., x_n)$ then*

$$Pf = A(f(x_1), ..., f(x_n));$$

(2) *if $P = $ **nil** then $Pf = $ **nil**;*

(3) *if $P = \tau.P'$ then $Pf = \tau.P'f$;*

(4) *if $P = \mathcal{E}[X].P'$ then $Pf = (\mathcal{E}f)[f(X)].P'f$;*

(5) *if $P = c?x.P'$ then $Pf = c?y.P'\{y/x\}f_y$, where $y \notin fv(c?x.P') \cup fv(P'f)$, and f_y is the substitution with $f_y(y) = y$, $f_y(f^{-1}(y)) = f(y)$ and $f_y(z) = f(z)$ for all $z \neq y, f^{-1}(y)$;*

(6) *if $P = c!x.P'$ then $Pf = c!f(x).P'f$;*

(7) *if $P = P_1 + P_2$ then $Pf = P_1f + P_2f$;*

(8) *if $P = P_1\|P_2$ then $Pf = P_1f\|P_2f$;*

(9) *if $P = P'\backslash L$ then $Pf = P'f\backslash L$.*

Note that in clause 4 a corresponding modification on super-operator $\mathcal{E}$ is made when substituting quantum variables in X. In addition, the requirement that f is one-to-one becomes vital when we consider substitution of output prefix in clauses 6 and of parallel composition in clause 8; for example, if $f(x) = f(y) = x$, and

$$P_1 = c!x.d!y.\mathbf{nil}, \quad P_2 = c!x.\mathbf{nil}\|d!y.\mathbf{nil},$$

then the following two expressions

$$P_1f = c!x.d!x.\mathbf{nil}, \quad P_2f = c!x.\mathbf{nil}\|d!x.\mathbf{nil}$$

are not processes.

If $(Pf)f^{-1} \equiv_\alpha P$; that is, there is no variable conflict where $f(x) \in fv(P) - \{x\}$ for some $x \in fv(P)$, then Pf is said to be well-defined. In what follows we always assume that Pf is well-defined whenever it occurs.

Let $\widetilde{x} = x_1, ..., x_n$ and $\widetilde{y} = y_1, ..., y_n$. If $f(x_i) = y_i$ $(1 \leq i \leq n)$, we write $P\{\widetilde{y}/\widetilde{x}\}$ or $P\{y_1/x_1, ..., y_n/x_n\}$ for Pf.

3.2 Operational Semantics

The operational semantics of qCCS will be given by transitions between configurations, labeled by actions. A configuration is defined to be a pair $\langle P, \rho \rangle$ where $P \in \mathcal{P}$ is a process, and $\rho \in \mathcal{D}(\mathcal{H})$ specifies the current state of the environment. Intuitively, ρ is an instantiation (or valuation) of quantum variables. Instantiations of classical variables can be made independently from each other, but quantum systems represented by different variables may be correlated because ρ is allowed to be an entangled state. The set of configurations is written Con.

We set

$$Act = \{\tau\} \cup Act_{op} \cup Act_{com}$$

for the set of actions, where

$$Act_{op} = \{\mathcal{E}[X] : X \text{ is a finite subset of } Var \text{ and } \mathcal{E} \text{ is a super} - \text{operator on } \mathcal{H}_X\}$$

is the set of quantum operations, and

$$Act_{com} = \{c?x, c!x : c \in Chan \text{ and } x \in Var\}$$

is the set of communication actions, including inputs and outputs. The set Act will be ranged over by meta-variables $\alpha, \beta, \ldots$. We need the following notations for actions:

— For each $\alpha \in Act$, we use $cn(\alpha)$ to stand for the channel name in action α; that is, $cn(c?x) = cn(c!x) = c$, and $cn(\tau)$ and $cn(\mathcal{E}[X])$ are not defined.

— We write $fv(\alpha)$ for the set of free variables in α; that is, $fv(c!x) = \{x\}$, $fv(\mathcal{E}[X]) = X$, $fv(\tau) = fv(c?x) = \emptyset$.

— We define $bv(\alpha)$ to be the bound variable in α; that is, $bv(c?x) = x$, and $bv(\tau)$, $bv(\mathcal{E}[X])$ and $bv(c!x)$ are not defined.

To present the operational semantics of qCCS, we need one more auxiliary notation. For any $X \subseteq Var$ and super-operator $\mathcal{E}$ on $\mathcal{H}_X$, the cylindric extension of $\mathcal{E}$ on $\mathcal{H}$ is defined to be

$$\mathcal{E}_X \stackrel{def}{=} \mathcal{E} \otimes \mathcal{I}_{\mathcal{H}_{Var-X}} \tag{2}$$

where $\mathcal{I}_{\mathcal{H}_{Var-X}}$ is the identity operator on $\mathcal{H}_{Var-X}$. In what follows we always assume that X is a finite subset of Var and $\mathcal{E}$ is a super-operator on $\mathcal{H}_X$ whenever $\mathcal{E}_X$ is encountered.

Then the operational semantics of qCCS is given as a transition system $(Con, Act, \rightarrow)$, where the transition relation $\rightarrow$ is defined by the following rules:

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

$$\textbf{Oper} : \frac{}{\langle \mathcal{E}[X].P, \rho \rangle \xrightarrow{\mathcal{E}[X]} \langle P, \mathcal{E}_X(\rho) \rangle}$$

$$\textbf{Input} : \frac{}{\langle c?x.P, \rho \rangle \xrightarrow{c?y} \langle P\{y/x\}, \rho \rangle} \quad y \notin fv(c?x.P)$$

$$\textbf{Output} : \frac{}{\langle c!x.P, \rho \rangle \xrightarrow{c!x} \langle P, \rho \rangle}$$

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

$$\textbf{Intl1} : \frac{\langle P, \rho \rangle \xrightarrow{c?x} \langle P', \rho' \rangle}{\langle P \| Q, \rho \rangle \xrightarrow{c?x} \langle P' \| Q, \rho' \rangle} \quad x \notin fv(Q)$$

$$\textbf{Intl2} : \frac{\langle P, \rho \rangle \xrightarrow{\alpha} \langle P', \rho' \rangle}{\langle P \| Q, \rho \rangle \xrightarrow{\alpha} \langle P' \| Q, \rho' \rangle} \quad \alpha \text{ is not an input}$$

$$\textbf{Comm} : \frac{\langle P, \rho \rangle \xrightarrow{c?x} \langle P', \rho \rangle \quad \langle Q, \rho \rangle \xrightarrow{c!x} \langle Q', \rho \rangle}{\langle P \| Q, \rho \rangle \xrightarrow{\tau} \langle P' \| Q', \rho \rangle}$$

$$\textbf{Res} : \frac{\langle P, \rho \rangle \xrightarrow{\alpha} \langle P', \rho' \rangle}{\langle P \backslash L, \rho \rangle \xrightarrow{\alpha} \langle P' \backslash L, \rho' \rangle} \quad cn(\alpha) \notin L$$

$$\textbf{Def} : \frac{\langle P\{\widetilde{y}/\widetilde{x}\}, \rho \rangle \xrightarrow{\alpha} \langle P', \rho' \rangle}{\langle A(\widetilde{y}), \rho \rangle \xrightarrow{\alpha} \langle P', \rho' \rangle} \quad A(\widetilde{x}) \overset{def}{=} P$$

The symmetric forms of the **Choice**, **Intl1**, **Intl2** and **Comm** rules are omitted in the above table.

The operator $\mathcal{E}_X(\cdot)$ in the **Oper** rule was defined by Eq. (2). In the output transition $\langle c!x.P, \rho \rangle \xrightarrow{c!x} \langle P, \rho \rangle$, the $x-$system is sent out through channel c. Note that the current state of the $x-$system is specified in ρ. But ρ is not necessary to be a separable state, and it is possible that the $x-$system is entangled with the $y-$system for some $y \in Var - \{x\}$. Moreover, the entanglement between the $x-$system and the $y-$systems ($y \notin Var - \{x\}$) is preserved after the action $c!x$. The input transition $\langle c?x.P, \rho \rangle \xrightarrow{c?y} \langle P\{y/x\}, \rho \rangle$ means that the $y-$system is received from channel c and then it is put into the (free) occurrences of x in P (There may be more than one free occurrences of a single variable x in P because it is not required that $fv(P) \cap fv(Q) = \emptyset$ in sum $P + Q$). It should be noted that in $c?x.P$ the variable x is bound and it does not represent concretely the $x-$system. Instead it is merely a reference to the place where the received system will go. Thus, $c?x.P$ can perform action $c?y$ with $y \neq x$. The side condition $y \notin fv(c?x.P)$ for the input transition is obviously

to avoid variable name conflict, and it also makes that $P\{y/x\}$ is well-defined. During performing both the input and output actions, the state of the environment is not changed. Passing quantum systems happens in a communication described by the **Comm** rule, but it is realized in a "call-by-name" scheme and does not change the state of the environment.

From Definition 3.1(8) we note that it is required that $fv(P') \cap fv(Q') = \emptyset$ to guarantee that the **Comm** rule is reasonable. However, we do not need to impose this condition into the **Comm** rule because it is a consequence of the other rules. The verification of this condition is postponed to the end of Lemma 3.2. The same happens to the **Intl1** and **Intl2** rules.

3.3 Examples

To illustrate the transition rules introduced in the last subsection, we give some simple examples.

In the first example, we shall use the language of qCCS to describe how quantum systems are passed between processes and how a unitary transformation or a quantum measurement is performed on some quantum systems. The most interesting thing is to observe how entangled systems behave during computation and communication.

EXAMPLE 3.1. *Let*

$$P_1 = c?y.P_1', \quad P_2 = c!x.P_2'$$

and $P = (P_1 \| P_2) \backslash c$, where $x \notin fv(P_1)$. Then for any ρ, the only possible transition of P is

$$\langle P, \rho \rangle \xrightarrow{\tau} \langle (P_1'\{x/y\} \| P_2') \backslash c, \rho \rangle.$$

Note that in this transition the $x-$system is passed from P_2 to P_1 but the state ρ of the environment is not changed. This is reasonable because ρ does not contain any position information of the quantum systems under consideration; more precisely, in a configuration $\langle Q, \rho \rangle$, for all quantum variables x, ρ only describes the state of the $x-$system, but it does not indicate any subprocess of Q by which the $x-$system is possessed.

If

$$Q_1 = c?y.H[y].Q_1', \quad Q = (Q_1 \| P_2) \backslash c,$$

and $\rho = |0\rangle_x \langle 0| \otimes \rho'$ where $\rho' \in \mathcal{D}(\mathcal{H}_{Var-\{x\}})$ and $x \notin fv(Q_1)$, then

$$\langle Q, \rho \rangle \xrightarrow{\tau} \langle (H[x].Q_1'\{x/y\} \| P_2') \backslash c, \rho \rangle$$
$$\xrightarrow{H[x]} \langle (Q_1'\{x/y\} \| P_2') \backslash c, |+\rangle_x \langle +| \otimes \rho' \rangle.$$

At the beginning of the transition the state of the $x-$system is $|0\rangle$. Then the $x-$system is passed from P_2 to Q_1 and the Hadamard transformation is performed on it at Q_1. The state of the $x-$system becomes $|+\rangle$ after the transition.

Suppose that

$$R_1 = c?y.CNOT[y, z].R_1'$$

and $R = (R_1 \| P_2) \backslash c$ and $\sigma = |+\rangle_x \langle +| \otimes |0\rangle_z \langle 0| \otimes \sigma'$ where $\sigma' \in \mathcal{D}(\mathcal{H}_{Var-\{x,z\}})$ and $x \notin fv(R_1)$. Then

$$\langle R, \sigma \rangle \xrightarrow{\tau} \langle (CNOT[x, z].R_1'\{x/y\} \| P_2') \backslash c, \sigma \rangle$$
$$\xrightarrow{CNOT[x,z]} \langle (R_1'\{x/y\} \| P_2') \backslash c, |\beta_{00}\rangle_{xz} \langle \beta_{00}| \otimes \sigma' \rangle.$$

The $x-$system is passed from P_2 to R_1, and then the $CNOT$ operator is applied to it and the $z-$system together. It is worth noting that the state of the $xz-$system is separable before the transition, but an entanglement between the $x-$system and the $z-$system is created at the end of the transition.

Let

$$S_1 = c?y.CNOT[y, z].\mathcal{M}_{0,1}[z].S_1'$$

and $S = (S_1 \| P_2) \backslash c$, where $\mathcal{M}_{0,1}$ is the operation generated by the measurement of single qubit in the computational basis $|0\rangle$, $|1\rangle$, with the measurement result unknown; that is, $\mathcal{M}_{0,1}(\rho) = P_0 \rho P_0 + P_1 \rho P_1$ for each $\rho \in \mathcal{D}(\mathcal{H}_2)$, where $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$. Then

$$\langle S, \sigma \rangle \xrightarrow{\tau} \langle (CNOT[x, z].\mathcal{M}_{0,1}[z].S_1'\{x/y\} \| P_2') \backslash c, \sigma \rangle$$

$$\xrightarrow{CNOT[x,z]} \langle (\mathcal{M}_{0,1}[z].S_1'\{x/y\} \| P_2') \backslash c, |\beta_{00}\rangle_{xz}\langle \beta_{00}| \otimes \sigma' \rangle$$

$$\xrightarrow{\mathcal{M}_{0,1}[z]} \langle (S_1'\{x/y\} \| P_2') \backslash c, \frac{1}{2}(|00\rangle_{xz}\langle 00| + |11\rangle_{xz}\langle 11|) \otimes \sigma' \rangle.$$

In the last transition the measurement in computational basis $|0\rangle$, $|1\rangle$ is performed on the $z-$system. We can see that the $x-$system and the $z-$system are always in the same state in the last configuration. This is because they are entangled before the measurement.

The communication channels in qCCS (named by elements of $Chan$) are implicitly assumed to be noiseless. However, the major part of quantum information theory is devoted to solve the problem of transmitting reliably information through noisy quantum channels (see [15], Chapter 12). The next example shows how we can formally describe noisy quantum channels in qCCS by combining noiseless communications and quantum operations on the passed systems.

EXAMPLE 3.2. *Quantum noisy channel. We imagine a simple scenario where Alice sends quantum information to Bob through a quantum noisy channel. Usually, a quantum noisy channel is represented by a super-operator $\mathcal{E}$ (see Chapters 8 and 12 of [15]). Thus, Alice and Bob may be described as processes:*

$$P = c_1!x.P', \quad Q = c_2?z.Q'$$

respectively, and the channel is described as a nullary process constant scheme C whose defining equation is

$$C \stackrel{def}{=} c_1?y.\mathcal{E}[y].c_2!y.C.$$

Put $S = (P \| C \| Q) \backslash \{c_1, c_2\}$. If information that Alice wants to send is expressed by a quantum state ρ of the $x-$system, then for any $\rho' \in \mathcal{D}(\mathcal{H}_{Var-\{x\}})$, we have:

$$\langle S, \rho \otimes \rho' \rangle \xrightarrow{\tau} \langle (P' \| \mathcal{E}[x].c_2!x.C \| Q) \backslash \{c_1, c_2\}, \rho \otimes \rho' \rangle$$

$$\xrightarrow{\mathcal{E}[x]} \langle (P' \| c_2!x.C \| Q) \backslash \{c_1, c_2\}, \mathcal{E}(\rho) \otimes \rho' \rangle$$

$$\xrightarrow{\tau} \langle (P' \| C \| Q'\{x/z\}) \backslash \{c_1, c_2\}, \mathcal{E}(\rho) \otimes \rho' \rangle.$$

Note that $fv(C)$ does not contain y; otherwise C is not a process. Thus, $C\{x/y\} = C$.

Moreover, suppose that a system-environment model of $\mathcal{E}$ is given as in Lemma 2.1(2). Let $\mathcal{E}_U$, $\mathcal{E}_P$ and $\mathcal{E}_{tr_E}$ be super-operators on $\mathcal{H}_x \otimes \mathcal{H}_E$ and be defined as follows: $\mathcal{E}_U(\sigma) =$

$$\langle S', \rho \otimes |e_0\rangle\langle e_0| \otimes \rho''\rangle \xrightarrow{\tau} \langle (P'\|\mathcal{E}_U[\{x,E\}].\mathcal{E}_P[\{x,E\}].\mathcal{E}_{tr_E}[\{x,E\}].c_2!x.C'(E)$$
$$\|Q)\backslash\{c_1, c_2\}, \rho \otimes |e_0\rangle\langle e_0| \otimes \rho''\rangle$$
$$\xrightarrow{\mathcal{E}_U[\{x,E\}]} \langle (P'\|\mathcal{E}_P[\{x,E\}].\mathcal{E}_{tr_E}[\{x,E\}].c_2!x.C'(E)\|Q)\backslash\{c_1, c_2\},$$
$$U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger \otimes \rho''\rangle \qquad (3)$$
$$\xrightarrow{\mathcal{E}_P[\{x,E\}]} \langle (P'\|\mathcal{E}_{tr_E}[\{x,E\}].c_2!x.C'(E)\|Q)\backslash\{c_1, c_2\}, PU(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P \otimes \rho''\rangle$$
$$\xrightarrow{\mathcal{E}_{tr_E}[\{x,E\}]} \langle (P'\|c_2!x.C'(E)\|Q)\backslash\{c_1, c_2\}, \mathcal{E}(\rho) \otimes |e_0\rangle\langle e_0| \otimes \rho''\rangle$$
$$\xrightarrow{\tau} \langle (P'\|C'(E)\|Q'\{x/z\})\backslash\{c_1, c_2\}, \mathcal{E}(\rho) \otimes |e_0\rangle\langle e_0| \otimes \rho''\rangle.$$

$U\sigma U^\dagger$, $\mathcal{E}_P(\sigma) = P\sigma P$, and

$$\mathcal{E}_{tr_E}(\sigma) = \sum_k \langle e_k|\sigma|e_k\rangle \otimes |e_0\rangle\langle e_0|,$$

respectively, for all $\sigma \in \mathcal{D}(\mathcal{H}_x \otimes \mathcal{H}_E)$. *We define process constant scheme* C' *by*

$$C'(E) \stackrel{def}{=} c_1?y.\mathcal{E}_U[\{y,E\}].\mathcal{E}_P[\{y,E\}].\mathcal{E}_{tr_E}[\{y,E\}].c_2!y.C'(E),$$

and put $S' = (P\|C'(E)\|Q)\backslash\{c_1, c_2\}$. *Then for all* $\rho \in \mathcal{D}(\mathcal{H}_x)$ *and* $\rho'' \in \mathcal{D}(\mathcal{H}_{Var-\{x,E\}})$, *the transitions of* S' *are displayed in Eq. (3).*

Quantum copying has attracted considerably much interest in the community of quantum information. The aim is to find some physical devices, called quantum-copying machines, which can produce two copies of a unknown input quantum state at their output. However, Wootters and Zurek [18] and Dieks [2] proved the no-cloning theorem which asserts that such an ideal quantum-copying machine does not exist. Now the no-cloning is widely recognized as one of the essential differences between classical and quantum information. Although there is not a perfect cloning machine, the no-cloning theorem does not forbid imperfect copying of arbitrary quantum states. Indeed, an approximate quantum copier was first designed by Buzek and Hillery [1]. The following example gives a formal description of it in the language of qCCS.

EXAMPLE 3.3. *Approximate quantum copier. Suppose that an agent* Q *wants to copy a (unknown) quantum state,* Q *sends the state to a copier* P *through channel* c, *and* P *receives it and puts it at place* y *(the original mode). First,* P *has to ask for a new place from another agent* R *as the copy mode. Then* P *performs a copying operation on the original and copy modes together, which is represented by a unitary transformation* U, *independent of the input state. Finally,* P *will send two (approximate) copies of the original state back to* Q *through channel* c. *So,* P, Q, R *and the whole system* S *may be described as follows:*

$$P = c?y.d?z.U[y,z].c!y.c!z.P, \quad Q = c!x.c?u.c?v.Q', \quad R = d!x_0.\mathbf{nil},$$

and $S = (P\|Q\|R)\backslash\{c,d\}$. *Note that* P *is a nullary process constant scheme and* $y, z \notin fv(P)$.

Let $\rho = |\varphi\rangle_x\langle\varphi| \otimes |0\rangle_{x_0}\langle 0| \otimes \sigma$, *where* $\sigma \in \mathcal{D}(\mathcal{H}_{Var-\{x,x_0\}})$, $|\varphi\rangle$ *is the state to be copied, and the initial state of the copy mode is assumed to be* $|0\rangle$. *Then the copying*

process is described by the following transitions:

$$\langle S, \rho \rangle \overset{\tau}{\to} \langle (d?z.U[x,z].c!x.c!z.P \| c?u.c?v.Q' \| R) \backslash \{c,d\}, \rho \rangle$$

$$\overset{\tau}{\to} \langle (U[x,x_0].c!x.c!x_0.P \| c?u.c?v.Q' \| \mathbf{nil}) \backslash \{c,d\}, \rho \rangle$$

$$\overset{U[x,x_0]}{\to} \langle (c!x.c!x_0.P \| c?u.c?v.Q' \| \mathbf{nil}) \backslash \{c,d\}, \rho' \rangle$$

$$\overset{\tau}{\to} \langle (c!x_0.P \| c?v.Q'\{x/u\} \| \mathbf{nil}) \backslash \{c,d\}, \rho' \rangle$$

$$\overset{\tau}{\to} \langle P \| Q'\{x/u\}\{x_0/v\} \| \mathbf{nil}) \backslash \{c,d\}, \rho' \rangle,$$

where it is supposed that $U|\varphi\rangle_x |0\rangle_{x_0} = |\varphi'\rangle_x |\varphi'\rangle_{x_0}$, and $\rho' = |\varphi'\rangle_x \langle\varphi'| \otimes |\varphi'\rangle_{x_0} \langle\varphi'| \otimes \sigma$. The Wootters-Zurek-Dieks no-cloning theorem [18], [2] excludes the possibility that for all $|\varphi\rangle \in \mathcal{H}_x$, $|\varphi'\rangle = |\varphi\rangle$. But it is shown by Buzek and Hillery [1] that there exists a (universal) copier P which approximately copies the input state $|\varphi\rangle$ such that the quality of the output state $|\varphi'\rangle$, measured by the Hilbert-Schmidt norm of the difference between $|\varphi\rangle$ and $|\varphi'\rangle$, does not depend on $|\varphi\rangle$.

3.4 Properties of Transitions

We now present some basic properties of the transition relation defined in Section 3.2. Their proofs can be carried out by induction on the depth of inference. Some of them need very careful analysis, we put them into the Appendix to improve readability of the paper.

First, we observe how does the environment of a configuration change in a transition.

LEMMA 3.1. (*1*) *If $\langle P, \rho \rangle \overset{\mathcal{E}[X]}{\to} \langle P', \rho' \rangle$, then*
  (*a*) $\rho' = \mathcal{E}_X(\rho)$; *and*
  (*b*) $\langle P, \sigma \rangle \overset{\mathcal{E}[X]}{\to} \langle P', \mathcal{E}_X(\sigma) \rangle$ *holds for all $\sigma \in \mathcal{D}(\mathcal{H})$.*

(*2*) *If $\langle P, \rho \rangle \overset{\alpha}{\to} \langle P', \rho' \rangle$ and α is not of the form $\mathcal{E}[X]$, then*
  (*a*) $\rho = \rho'$; *and*
  (*b*) $\langle P, \sigma \rangle \overset{\alpha}{\to} \langle P', \sigma \rangle$ *holds for all $\sigma \in \mathcal{D}(\mathcal{H})$. Thus, we can simply write $P \overset{\alpha}{\to} P'$.*

Next we see how are the variables in an action related to the free variables of a process performing this action and those of the process immediately after it.

LEMMA 3.2. *If $\langle P, \rho \rangle \overset{\alpha}{\to} \langle P', \rho' \rangle$, then*

(*1*) $fv(\alpha) \subseteq fv(P) - fv(P')$; *and*

(*2*) $fv(P') \subseteq fv(P) \cup \{bv(\alpha)\}$.

This lemma enables us to verify that the **Intl1, Intl2** and **Comm** rules are well-defined. We only consider **Comm** for instance: if $\langle P, \rho \rangle \overset{c?x}{\to} \langle P', \rho \rangle$ and $\langle Q, \rho \rangle \overset{c!x}{\to} \langle Q', \rho \rangle$, then using the above lemma we obtain $fv(P') \subseteq fv(P) \cup \{x\}$, $fv(Q') \subseteq fv(Q)$ and $x \notin fv(Q')$. If $P \| Q \in \mathcal{P}$, this obviously leads to $fv(P') \cap fv(Q') = \emptyset$ because $fv(P) \cap fv(Q) = \emptyset$. The other two rules can be dealt with in a similar way.

The next lemma shows that the variable in an input can be changed in a transition provided a corresponding modification of the process after the transition is made.

LEMMA 3.3. *If $\langle P, \rho \rangle \overset{c?x}{\to} \langle P', \rho \rangle$ and $y \notin fv(P)$, then $\langle P, \rho \rangle \overset{c?y}{\to} \langle P'', \rho \rangle$ for some $P'' \equiv_\alpha P'\{y/x\}$.*

The following two lemmas carefully examine interference of substitution and transition. Let f be a substitution. Then we define its extension on actions by $f(\tau) = \tau$, $f(\mathcal{E}[X]) = \mathcal{E}f[f(X)]$, $f(c?x) = c?x$, and $f(c!x) = c!f(x)$.

LEMMA 3.4. *If* $\langle P, \rho \rangle \xrightarrow{\alpha} \langle P', \rho' \rangle$ *and* $f(bv(\alpha)) = bv(\alpha)$, *then* $\langle Pf, f(\rho) \rangle \xrightarrow{f(\alpha)} \langle P'', f(\rho') \rangle$ *for some* $P'' \equiv_\alpha P'f$.

LEMMA 3.5. *If* $\langle Pf, f(\rho) \rangle \xrightarrow{\alpha} \langle Q, \sigma \rangle$ *and* $f(bv(\alpha)) = bv(\alpha)$, *then for some* β, P' *and* ρ', $\langle P, \rho \rangle \xrightarrow{\beta} \langle P', \rho' \rangle$, $Q \equiv_\alpha P'f$, $\sigma = f(\rho')$ *and* $\alpha = f(\beta)$.

Finally, we exhibit a certain invariance of transitions under $\alpha-$conversion.

LEMMA 3.6. *Let* $P_1 \equiv_\alpha P_2$. *Then*

(1) *if* $\langle P_1, \rho \rangle \xrightarrow{\alpha} \langle P_1', \rho' \rangle$ *and* α *is not an input, then* $\langle P_2, \rho \rangle \xrightarrow{\alpha} \langle P_2', \rho' \rangle$ *for some* $P_2' \equiv_\alpha P_1'$;

(2) *if* $\langle P_1, \rho \rangle \xrightarrow{c?x} \langle P_1', \rho \rangle$, *then for any* $y \notin fv(P_2)$, $\langle P_2, \rho \rangle \xrightarrow{c?y} \langle P_2', \rho \rangle$ *for some* $P_2' \equiv_\alpha P_1'\{y/x\}$.

4. STRONG BISIMULATIONS

4.1 Basic Definitions

We first introduce the notion of strong bisimulation on configurations.

DEFINITION 4.1. *A symmetric relation* $\mathcal{R} \subseteq Con \times Con$ *is called a 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,*

(1) *whenever* $\langle P, \rho \rangle \xrightarrow{\alpha} \langle P', \rho' \rangle$ *and* α *is not an input, then for some* Q' *and* σ', $\langle Q, \sigma \rangle \xrightarrow{\alpha} \langle Q', \sigma' \rangle$ *and* $\langle P', \rho' \rangle \mathcal{R} \langle Q', \sigma' \rangle$;

(2) *whenever* $\langle P, \rho \rangle \xrightarrow{c?x} \langle P', \rho \rangle$ *and* $x \notin fv(P) \cup fv(Q)$, *then for some* Q', $\langle Q, \sigma \rangle \xrightarrow{c?x} \langle Q', \sigma \rangle$ *and for all* $y \notin fv(P') \cup fv(Q') - \{x\}$, $\langle P'\{y/x\}, \rho \rangle \mathcal{R} \langle Q'\{y/x\}, \sigma \rangle$.

It should be noted that in Clause 2 we require $y \notin fv(P') \cup fv(Q') - \{x\}$. If we would not put this requirement, then two previously different quantum states may become the same state after substitution $\{y/x\}$. This is forbidden by the no-cloning theorem of quantum information.

Then we are able to define strong bisimilarity between configurations in a familiar way.

DEFINITION 4.2. *For any* $\langle P, \rho \rangle, \langle Q, \sigma \rangle \in Con$, *we say that* $\langle P, \rho \rangle$ *and* $\langle Q, \sigma \rangle$ *are strongly bisimilar, written* $\langle P, \rho \rangle \sim \langle Q, \sigma \rangle$, *if* $\langle P, \rho \rangle \mathcal{R} \langle Q, \sigma \rangle$ *for some strong bisimulation* $\mathcal{R}$; *that is, strong bisimilarity on* Con *is the greatest strong bisimulation:*

$$\sim = \bigcup \{\mathcal{R} : \mathcal{R} \text{ is a strong bisimulation}\}.$$

Now strong bisimilarity between processes may be defined by comparing two processes in the same environment.

DEFINITION 4.3. *For any quantum processes* $P, Q \in \mathcal{P}$, *we say that* P *and* Q *are strongly bisimilar, written* $P \sim Q$, *if* $\langle P, \rho \rangle \sim \langle Q, \rho \rangle$ *for all* $\rho \in \mathcal{D}(\mathcal{H})$.

The following lemma gives a recursive characterization of strong bisimilarity between configurations, and it is useful in establishing strong bisimilarity between some processes.

LEMMA 4.1. *For any $\langle P, \rho \rangle, \langle Q, \sigma \rangle \in Con$, $\langle P, \rho \rangle \sim \langle Q, \sigma \rangle$ if and only if,*

(1) *whenever $\langle P, \rho \rangle \xrightarrow{\alpha} \langle P', \rho' \rangle$ and α is not an input, then for some Q' and σ', $\langle Q, \sigma \rangle \xrightarrow{\alpha} \langle Q', \sigma' \rangle$ and $\langle P', \rho' \rangle \sim \langle Q', \sigma' \rangle$;*

(2) *whenever $\langle P, \rho \rangle \xrightarrow{c?x} \langle P', \rho \rangle$ and $x \notin fv(P) \cup fv(Q)$, then for some Q', $\langle Q, \sigma \rangle \xrightarrow{c?x} \langle Q', \sigma \rangle$ and for all $y \notin fv(P') \cup fv(Q') - \{x\}$, $\langle P'\{y/x\}, \rho \rangle \sim \langle Q'\{y/x\}, \sigma \rangle$,*

and the symmetric forms of 1 and 2.

Proof. Similar to the proof of Proposition 4.4 in [13]. □

In the remainder of this section we are going to present some fundamental properties of strong bisimilarity. First, we show that strong bisimilarity is preserved by $\alpha-$conversion.

PROPOSITION 4.1. *If $P_1 \equiv_\alpha P_2$, then $P_1 \sim P_2$.*

Proof. It is easy to show that

$$\mathcal{R} = \{(\langle P_1, \rho \rangle, \langle P_2, \rho \rangle) : P_1 \equiv_\alpha P_2\}$$

is a strong bisimulation by using Lemma 3.6. □

4.2   Monoid Laws, Expansion Law and Congruence

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

PROPOSITION 4.2. *For any $P, Q, R \in \mathcal{P}$, and $K, L \subseteq Chan$, we have:*

(1) $P + Q \sim Q + P$;

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

(3) $P + P \sim P$;

(4) $P + \mathbf{nil} \sim P$;

(5) $P \| Q \sim Q \| P$;

(6) $P \| (Q \| R) \sim (P \| Q) \| R$;

(7) $P \| \mathbf{nil} \sim P$;

(8) $P \backslash L \sim P$ if $cn(P) \cap L = \emptyset$, where $cn(P)$ is the set of free channel names in P;

(9) $(P \backslash K) \backslash L \sim P \backslash (K \cup L)$.

Proof. The items (1)-(4) may be proved by using Lemma 4.1, and the items (5)-(9) may be proved by constructing appropriate strong bisimulation. Here, we only prove (6) as an example. Put

$$\mathcal{R} = \{(\langle P \| (Q \| R), \rho \rangle, \langle (P \| Q) \| R, \rho \rangle) : P, Q, R \in \mathcal{P} \text{ and } \rho \in \mathcal{D}(\mathcal{H})\}$$

It suffices to show that $\mathcal{R}$ is a strong bisimulation. Suppose that

$$\langle P \| (Q \| R), \rho \rangle \xrightarrow{\alpha} \langle S, \rho' \rangle. \tag{4}$$

We only consider the following two cases, and the others are easy or similar.

Case 1. The transition Eq. (4) is derived from $\langle Q, \rho \rangle \xrightarrow{c?x} \langle Q', \rho \rangle$ and $\langle R, \rho \rangle \xrightarrow{c!x} \langle R', \rho \rangle$ by **Comm**. Then $\alpha = \tau$, $\rho' = \rho$ and $S = P \| (Q' \| R')$. It follows from Lemma 3.2 that $x \in fv(R)$. This leads to $x \notin fv(P \| Q) = fv(P) \cup fv(Q)$ because $(P \| Q) \| R \in \mathcal{P}$.

Consequently, we may apply the **Intl1** rule to assert that $\langle P \| Q, \rho \rangle \xrightarrow{c?x} \langle P \| Q', \rho \rangle$, and furthermore by the **Comm** rule we obtain

$$\langle (P \| Q) \| R, \rho \rangle \xrightarrow{\tau} \langle (P \| Q') \| R', \rho \rangle.$$

Now it suffices to note that $\langle S, \rho \rangle \mathcal{R} \langle (P \| Q') \| R', \rho \rangle$.

Case 2. $\alpha = c?x$,

$$x \notin fv(P \| (Q \| R)) \cup fv((P \| Q) \| R) = fv(P) \cup fv(Q) \cup fv(R)$$

and the transition Eq. (4) is derived from $\langle P, \rho \rangle \xrightarrow{c?x} \langle P', \rho \rangle$ by **Intl1**. Then $\rho' = \rho$ and $S = P' \| (Q \| R)$. Since $x \notin fv(Q)$, it follows from the **Intl1** rule that $\langle P \| Q, \rho \rangle \xrightarrow{c?x} \langle P' \| Q, \rho \rangle$. We also have $x \notin fv(R)$. Then using the **Intl1** rule once again we obtain

$$\langle (P \| Q) \| R, \rho \rangle \xrightarrow{c?x} \langle (P' \| Q) \| R, \rho \rangle.$$

Finally, we note that for each

$$y \notin fv(P' \| (Q \| R)) \cup fv((P' \| Q) \| R) - \{x\},$$

$$S\{y/x\} = P'\{y/x\} \| (Q \| R),$$

$$((P' \| Q) \| R)\{y/x\} = (P'\{y/x\} \| Q) \| R,$$

and it follows that

$$\langle S\{y/x\}, \rho \rangle \mathcal{R} \langle ((P' \| Q) \| R)\{y/x\}, \rho \rangle. \ \square$$

PROPOSITION 4.3. *(Expansion law) For any $P, Q \in \mathcal{P}$, we have:*

$$(P \| Q) \backslash L \sim \sum \{\alpha.(P' \| Q) \backslash L : P \xrightarrow{\alpha} P' \text{ and } cn(\alpha) \notin L\}$$

$$+ \sum \{\alpha.(P \| Q') \backslash L : Q \xrightarrow{\alpha} Q' \text{ and } cn(\alpha) \notin L\}$$

$$+ \sum \{\tau.(P' \| Q') \backslash L : P \xrightarrow{c?x} P' \text{ and } Q \xrightarrow{c!x} Q',$$

$$\text{or } P \xrightarrow{c!x} P' \text{ and } Q \xrightarrow{c?x} Q'\}.$$

Proof. Write S for the process in the right-hand side. Then we can show that $\langle (P \| Q) \backslash L, \rho \rangle \sim \langle S, \rho \rangle$ for all $\rho \in \mathcal{D}(\mathcal{H})$ in a way similar to that in classical CCS (see [13], Proposition 4.9). $\square$

The following lemma indicates that strong bisimilarity is preserved by substitution. Its proof requires careful manipulation of variables, and it is put into the Appendix for readability of the paper.

LEMMA 4.2. *For any $P, Q \in \mathcal{P}$ and for any substitution f, $P \sim Q$ if and only if $Pf \sim Qf$.*

Now we are ready to show one of the major results in this paper that strong bisimilarity is a congruence relation with respect to all combinators in qCCS. It is well-known that congruence is a key property in all classical process algebras. However, to our best

knowledge, full congruence has not been established for quantum processes in the previous works. For example, Lalire [11] introduced probabilistic rooted branching bisimilarity between quantum processes in QPAlg and proved that it is an equivalence relation and preserved by variable declaration, action prefix, nondeterministic choice, probabilistic choice, conditional choice and restriction. But she also gave a counterexample to show that probabilistic rooted branching (strong) bisimilarity is not preserved by parallel composition. In [4], a notion of probabilistic (strong/weak) bisimilarity between processes in a quantum extension of classical value-passing CCS was proposed by the authors of this paper. Again, there are some evidences showing that in general such a probabilistic bisimilarity might not be preserved by parallel composition. If we write $\sim_p$ for this probabilistic bisimilarity, then what was achieved in [4] is that $P \sim_p Q$ implies $P\|R \sim_p Q\|R$ when P and Q are free of quantum input, or R is free of unitary transformation and measurement; and the condition on P, Q and R is very restrictive. These facts seems to hint that parallel composition cannot live well in the quantum world where entanglement is present and cloning is forbidden. Parallel composition is definitely the most important combinator in any process algebra. Thus, understanding the behavior of parallel composition of quantum processes should be one of the key issues in designing a quantum process algebra. As pointed out in the Introduction, in order to have a clear understanding of quantum parallel composition, we decide to make a sharp cleanup in this paper, excluding classical computation and communication from the previous quantum process algebras and focusing our attention on pure quantum processes. This enables us to define a bisimilarity between quantum processes which is preserved by parallel composition and thus enjoys full congruence.

THEOREM 4.1. *(1) If $A \overset{def}{=} P$ then $A \sim P$.*

(2) If $P \sim Q$, then we have:

  (a) $\tau.P \sim \tau.Q$;
  (b) $\mathcal{E}[X].P \sim \mathcal{E}[X].Q$;
  (c) $c!x.P \sim c!x.Q$;
  (d) $c?x.P \sim c?x.Q$;
  (e) $P + R \sim Q + R$;
  (f) $P\|R \sim Q\|R$;
  (g) $P\backslash L \sim Q\backslash L$.

Proof. The proofs of (1), (2.a)-(2.c) and (2.e) are routine applications of Lemma 4.1, and (2.d) may be proved by using Lemmas 4.1 and 4.2. For (2.g), we only need to show that

$$\mathcal{R} = \{(\langle P\backslash L, \rho\rangle, \langle Q\backslash L, \sigma\rangle) : \langle P, \rho\rangle \sim \langle Q, \sigma\rangle\}$$

is a strong bisimulation, and the routine details are omitted.

The proof of (2.f) is not a straightforward generalization of the proof for classical processes, and it requires a new idea in constructing a strong bisimulation equating $P\|R$ and $Q\|R$. The major difficulty arises from interference between sequential quantum computation and communicating quantum systems. The key technique is inserting a properly chosen quantum operation into an existing sequence of quantum operations. Furthermore, the proof requires a very careful analysis of interplay between quantum variables, sequential applications of super-operators, and communication of quantum systems as well as subtle treatment of substitution of quantum variables. We define $\mathcal{R}$ to be a binary relation

between configurations, consisting of the pairs:

$$(\langle P\|R, \mathcal{F}_{Y_n}^{(n)}\mathcal{E}_{X_n}^{(n)}\mathcal{F}_{Y_{n-1}}^{(n-1)}\mathcal{E}_{X_{n-1}}^{(n-1)}...\mathcal{F}_{Y_1}^{(1)}\mathcal{E}_{X_1}^{(1)}\mathcal{F}_{Y_0}^{(0)}(\rho)\rangle,$$

$$\langle Q\|R, \mathcal{F}_{Y_n}^{(n)}\mathcal{E}_{X_n}^{(n)}\mathcal{F}_{Y_{n-1}}^{(n-1)}\mathcal{E}_{X_{n-1}}^{(n-1)}...\mathcal{F}_{Y_1}^{(1)}\mathcal{E}_{X_1}^{(1)}\mathcal{F}_{Y_0}^{(0)}(\sigma)\rangle),$$

where $n \geq 0$, $R \in \mathcal{P}$, X_i $(1 \leq i \leq n)$ and Y_i $(0 \leq i \leq n)$ are finite subsets of Var, $\mathcal{E}_{X_i}^{(i)}$ is a super-operator on $\mathcal{H}_{X_i}$ for each $1 \leq i \leq n$, and $\mathcal{F}_{Y_i}^{(i)}$ is a super-operator on $\mathcal{H}_{Y_i}$ for each $0 \leq i \leq n$, and

$$\langle P, \mathcal{E}_{X_n}^{(n)}\mathcal{E}_{X_{n-1}}^{(n-1)}...\mathcal{E}_{X_1}^{(1)}(\rho)\rangle \sim \langle Q, \mathcal{E}_{X_n}^{(n)}\mathcal{E}_{X_{n-1}}^{(n-1)}...\mathcal{E}_{X_1}^{(1)}(\sigma)\rangle.$$

The idea behind the definition of $\mathcal{R}$ is that we can insert an arbitrary quantum operation $\mathcal{F}_{Y_i}^{(i)}$ between two existing previously quantum operation $\mathcal{E}_{X_i}^{(i)}$ and $\mathcal{E}_{X_{i+1}}^{(i+1)}$ for any $1 \leq i \leq n-1$, and we can also insert an arbitrary quantum operation $\mathcal{F}_{Y_n}^{(n)}$ after the last operation $\mathcal{E}_{X_n}^{(n)}$ and insert $\mathcal{F}_{Y_0}^{(0)}$ before the first operation $\mathcal{E}_{X_1}^{(1)}$. The technique of insertion is unnecessary in the classical value-passing CCS from which sequential computation is abstracted by assuming value expressions (see [13], page 55). However, it is indispensable in qCCS where one has to consider interference between sequential quantum computation and communicating quantum systems.

For simplicity, we write $\mathcal{A} = \mathcal{E}_{X_n}^{(n)}\mathcal{E}_{X_{n-1}}^{(n-1)}...\mathcal{E}_{X_1}^{(1)}$ and

$$\mathcal{B} = \mathcal{F}_{Y_n}^{(n)}\mathcal{E}_{X_n}^{(n)}\mathcal{F}_{Y_{n-1}}^{(n-1)}\mathcal{E}_{X_{n-1}}^{(n-1)}...\mathcal{F}_{Y_1}^{(1)}\mathcal{E}_{X_1}^{(1)}\mathcal{F}_{Y_0}^{(0)}.$$

If $P \sim Q$, then for each ρ, $\langle P, \rho\rangle \sim \langle Q, \rho\rangle$, and it implies $\langle P\|R, \rho\rangle \mathcal{R} \langle Q\|R, \rho\rangle$ by taking $n = 0$ and $\mathcal{F}_{Y_0}^{(0)} = \mathcal{I}_{\mathcal{H}_{Y_0}}$ in $\mathcal{B}$. Therefore, it suffices to show that $\mathcal{R}$ is a strong bisimulation. To this end, suppose that $\langle P, \mathcal{A}(\rho)\rangle \sim \langle Q, \mathcal{A}(\sigma)\rangle$ and

$$\langle P\|R, \mathcal{B}(\rho)\rangle \xrightarrow{\alpha} \langle S, \rho'\rangle. \tag{5}$$

Our aim is to find a transition of $\langle Q\|R, \mathcal{B}(\rho)\rangle$ which matches transition Eq. (5) according to Definition 4.1. We consider the following four cases:

Case 1. $\alpha = \tau$. We have $\rho' = \mathcal{B}(\rho)$, and this case is divided into the following four subcases:

Subcase 1.1. The transition (5) is derived by **Intl2** from $\langle P, \mathcal{B}(\rho)\rangle \xrightarrow{\tau} \langle P', \mathcal{B}(\rho)\rangle$. Then $S = P'\|R$. By Lemma 3.1 we obtain $\langle P, \mathcal{A}(\rho)\rangle \xrightarrow{\tau} \langle P', \mathcal{A}(\rho)\rangle$. Since $\langle P, \mathcal{A}(\rho)\rangle \sim \langle Q, \mathcal{A}(\sigma)\rangle$, it holds that $\langle Q, \mathcal{A}(\sigma)\rangle \xrightarrow{\tau} \langle Q', \mathcal{A}(\sigma)\rangle$ for some Q' with $\langle P', \mathcal{A}(\rho)\rangle \sim \langle Q', \mathcal{A}(\sigma)\rangle$. Applying Lemma 3.1 once again we have $\langle Q, \mathcal{B}(\sigma)\rangle \xrightarrow{\tau} \langle Q', \mathcal{B}(\sigma)\rangle$, and the **Intl2** rule allows us to assert that $\langle Q\|R, \mathcal{B}(\sigma)\rangle \xrightarrow{\tau} \langle Q'\|R, \mathcal{B}(\sigma)\rangle$. It is easy to see that $\langle S, \rho'\rangle \mathcal{R} \langle Q'\|R, \mathcal{B}(\sigma)\rangle$ from the definition of $\mathcal{R}$.

Subcase 1.2. The transition (5) is derived by **Intl2** from $\langle R, \mathcal{B}(\rho)\rangle \xrightarrow{\tau} \langle R', \mathcal{B}(\rho)\rangle$. Then $S = P\|R'$, and from Lemma 3.1 and the **Intl2** rule it follows that $\langle R, \mathcal{B}(\sigma)\rangle \xrightarrow{\tau} \langle R', \mathcal{B}(\sigma)\rangle$ and $\langle Q\|R, \mathcal{B}(\sigma)\rangle \xrightarrow{\tau} \langle Q\|R', \mathcal{B}(\sigma)\rangle$. In addition, we have $\langle S, \rho'\rangle \mathcal{R} \langle Q\| R', \mathcal{B}(\sigma)\rangle$ because $\langle P, \mathcal{A}(\rho)\rangle \sim \langle Q, \mathcal{A}(\sigma)\rangle$.

Subcase 1.3. The transition (5) is derived by **Comm** from $\langle P, \mathcal{B}(\rho)\rangle \xrightarrow{c?x} \langle P', \mathcal{B}(\rho)\rangle$ and $\langle R, \mathcal{B}(\rho)\rangle \xrightarrow{c!x} \langle R', \mathcal{B}(\rho)\rangle$. First, we have $\langle P, \mathcal{A}(\rho)\rangle \xrightarrow{c?x} \langle P', \mathcal{A}(\rho)\rangle$ and $\langle R, \mathcal{B}(\sigma)\rangle \xrightarrow{c!x} \langle R', \mathcal{B}(\sigma)\rangle$ by using Lemma 3.1. With Lemma 3.2 we see $x \in fv(R)$. Note that $fv(P) \cap fv(R) = fv(Q) \cap fv(R) = \emptyset$. Thus, $x \notin fv(P) \cup fv(Q)$. Since $\langle P, \mathcal{A}(\rho)\rangle \sim \langle Q, \mathcal{A}(\sigma)\rangle$,

it follows that $\langle Q, \mathcal{A}(\sigma)\rangle \overset{c?x}{\rightarrow} \langle Q', \mathcal{A}(\sigma)\rangle$ for some Q' with $\langle P', \mathcal{A}(\rho)\rangle \sim \langle Q', \mathcal{A}(\sigma)\rangle$. By Lemma 3.1 and the **Comm** rule we obtain $\langle Q, \mathcal{B}(\sigma)\rangle \overset{c?x}{\rightarrow} \langle Q', \mathcal{B}(\sigma)\rangle$ and $\langle Q\|R, \mathcal{B}(\sigma)\rangle \overset{\tau}{\rightarrow} \langle Q'\|R', \mathcal{B}(\sigma)\rangle$. Moreover, it holds that $\langle S, \rho'\rangle \mathcal{R} \langle Q'\|R', \mathcal{B}(\sigma)\rangle$.

Subcase 1.4. The transition (5) is derived by **Comm** from $\langle P, \mathcal{B}(\rho)\rangle \overset{c!x}{\rightarrow} \langle P', \mathcal{B}(\rho)\rangle$ and $\langle R, \mathcal{B}(\rho)\rangle \overset{c?x}{\rightarrow} \langle R', \mathcal{B}(\rho)\rangle$. Similar to Subcase 1.3.

Case 2. $\alpha = \mathcal{G}[Z]$, where Z is a finite subset of Var, and $\mathcal{G}$ is a super-operator on $\mathcal{H}_Z$. We have $\rho' = \mathcal{G}_Z \mathcal{B}(\rho)$, and this case is divided into the following two subcases:

Subcase 2.1. The transition (5) is derived by **Intl2** from $\langle P, \mathcal{B}(\rho)\rangle \overset{\mathcal{G}[Z]}{\rightarrow} \langle P', \mathcal{G}_Z \mathcal{B}(\rho)\rangle$. Then $S = P'\|R$. It follows from Lemma 3.1 that $\langle P, \mathcal{A}(\rho)\rangle \overset{\mathcal{G}[Z]}{\rightarrow} \langle P', \mathcal{G}_Z \mathcal{A}(\rho)\rangle$, and $\langle Q, \mathcal{A}(\sigma)\rangle \overset{\mathcal{G}[Z]}{\rightarrow} \langle Q', \mathcal{G}_Z \mathcal{A}(\sigma)\rangle$ for some Q' with $\langle P', \mathcal{G}_Z \mathcal{A}(\rho)\rangle \sim \langle Q', \mathcal{G}_Z \mathcal{A}(\sigma)\rangle$ because $\langle P, \mathcal{A}(\rho)\rangle \sim \langle Q, \mathcal{A}(\sigma)\rangle$. Hence, using Lemma 3.1 once again we obtain $\langle Q, \mathcal{B}(\sigma)\rangle \overset{\mathcal{G}[Z]}{\rightarrow} \langle Q', \mathcal{G}_Z \mathcal{B}(\sigma)\rangle$. Consequently, using the **Intl2** rule leads to

$$\langle Q\|R, \mathcal{B}(\sigma)\rangle \overset{\mathcal{G}[Z]}{\rightarrow} \langle Q'\|R, \mathcal{G}_Z \mathcal{B}(\sigma)\rangle.$$

Comparing carefully $\mathcal{G}_Z \mathcal{A}$ and $\mathcal{G}_Z \mathcal{B}$, we see that $\mathcal{G}_Z \mathcal{B}$ results from inserting

$$\mathcal{F}_{Y_{n+1}}^{(n+1)} = \mathcal{I}_{\mathcal{H}_{Y_{n+1}}} = \mathcal{I}_{\mathcal{H}}, \mathcal{F}_{Y_n}^{(n)}, \mathcal{F}_{Y_{n-1}}^{(n-1)}, ..., \mathcal{F}_{Y_1}^{(1)}, \mathcal{F}_{Y_0}^{(0)}$$

at appropriate positions in $\mathcal{G}_Z \mathcal{A}$, where Y_{n+1} is an arbitrary finite subset of Var. This implies $\langle S, \rho'\rangle \mathcal{R} \langle Q'\|R, \mathcal{G}_Z \mathcal{B}(\sigma)\rangle$.

Subcase 2.2. The transition (5) is derived by **Intl2** from $\langle R, \mathcal{B}(\rho)\rangle \overset{\mathcal{G}[Z]}{\rightarrow} \langle R', \mathcal{G}_Z \mathcal{B}(\rho)\rangle$. Then $S = P\|R'$, and $\langle R, \mathcal{B}(\sigma)\rangle \overset{\mathcal{G}[Z]}{\rightarrow} \langle R', \mathcal{G}_Z \mathcal{B}(\sigma)\rangle$ follows immediately by using Lemma 3.1. Hence, it holds that

$$\langle Q\|R, \mathcal{B}(\sigma)\rangle \overset{\mathcal{G}[Z]}{\rightarrow} \langle Q\|R', \mathcal{G}_Z \mathcal{B}(\sigma)\rangle.$$

Let

$$\mathcal{K}_{Y_n \cup Z}^{(n)} = (\mathcal{F}_{Y_n}^{(n)} \otimes \mathcal{I}_{\mathcal{H}_{Z-Y_n}}) \circ (\mathcal{G}_Z \otimes \mathcal{I}_{\mathcal{H}_{Y_n - Z}}).$$

Then $\mathcal{K}_{Y_n \cup Z}^{(n)}$ is a super-operator on $\mathcal{H}_{Y_n \cup Z}$, and $\mathcal{G}_Z \mathcal{B}$ is obtained by inserting appropriately

$$\mathcal{K}_{Y_n \cup Z}^{(n)}, \mathcal{F}_{Y_{n-1}}^{(n-1)}, ..., \mathcal{F}_{Y_1}^{(1)}, \mathcal{F}_{Y_0}^{(0)}$$

in $\mathcal{A}$. Now it follows that $\langle S, \rho'\rangle \mathcal{R} \langle Q\|R, \mathcal{G}_Z \mathcal{B}(\sigma)\rangle$ from $\langle P, \mathcal{A}(\rho)\rangle \sim \langle Q, \mathcal{A}(\sigma)\rangle$.

At the first glance, one may think that the full generality of $\mathcal{A}$ is not necessary because in the above two subcases we only add a quantum operation at the beginning of a sequence of quantum operations. However, this is not the case. It should be noted that our proof is carried by induction on the depth of inference (5), and quantum operation inserted at the beginning of a sequence will be moved to the middle of a lager sequence in the later steps.

Case 3. $\alpha = c!x$. We need to consider the following two subcases:

Subcase 3.1. The transition (5) is derived by **Intl2** from $\langle P, \mathcal{B}(\rho)\rangle \overset{c!x}{\rightarrow} \langle P', \mathcal{B}(\rho)\rangle$. Similar to Subcase 1.1.

Subcase 3.2. The transition (5) is derived by **Intl2** from $\langle R, \mathcal{B}(\rho)\rangle \overset{c!x}{\rightarrow} \langle R', \mathcal{B}(\rho)\rangle$. Similar to Subcase 1.2.

Case 4. $\alpha = c?x$ and

$$x \notin fv(P\|R) \cup fv(Q\|R) = fv(P) \cup fv(Q) \cup fv(R).$$

We have $\rho' = \mathcal{B}(\rho)$, and this case is divided into the following two subcases:

Subcase 4.1. The transition (5) is derived by **Intl1** from $\langle P, \mathcal{B}(\rho)\rangle \overset{c?x}{\to} \langle P', \mathcal{B}(\rho)\rangle$. Then $S = P' \| R$, and using Lemma 3.1 we obtain $\langle P, \mathcal{A}(\rho)\rangle \overset{c?x}{\to} \langle P', \mathcal{A}(\rho)\rangle$. From $\langle P, \mathcal{A}(\rho)\rangle \sim \langle Q, \mathcal{A}(\sigma)\rangle$ and $x \notin fv(P) \cup fv(Q)$, it follows that $\langle Q, \mathcal{A}(\sigma)\rangle \overset{c?x}{\to} \langle Q', \mathcal{A}(\sigma)\rangle$ for some Q' with for all $y \notin fv(P') \cup fv(Q') - \{x\}$, and

$$\langle P'\{y/x\}, \mathcal{A}(\rho)\rangle \sim \langle Q'\{y/x\}, \mathcal{A}(\sigma)\rangle.$$

Furthermore, we have $\langle Q, \mathcal{B}(\sigma)\rangle \overset{c?x}{\to} \langle Q', \mathcal{B}(\sigma)\rangle$ by using Lemma 3.1 once again. Note that $x \notin fv(R)$. Thus, applying the **Intl1** rule yields $\langle Q\|R, \mathcal{B}(\sigma)\rangle \overset{c?x}{\to} \langle Q'\|R, \mathcal{B}(\sigma)\rangle$. What remains is to verify that

$$\langle (P'\|R)\{z/x\}, \mathcal{B}(\rho)\rangle \mathcal{R} \langle (Q'\|R)\{z/x\}, \mathcal{B}(\sigma)\rangle$$

for all $z \notin fv(P'\|R) \cup fv(Q'\|R) - \{x\}$. To this end, we only need to note that

$$(P'\|R)\{z/x\} = P'\{z/x\}\|R\{z/x\},$$

$$(Q'\|R)\{z/x\} = Q'\{z/x\}\|R\{z/x\},$$

and $z \notin fv(P'\|R) \cup fv(Q'\|R) - \{x\}$ implies $z \notin fv(P') \cup fv(Q') - \{x\}$.

Subcase 4.2. The transition (5) is derived by **Intl1** from $\langle R, \mathcal{B}(\rho)\rangle \overset{c?x}{\to} \langle R', \mathcal{B}(\rho)\rangle$. Then $S = P\|R'$, and $\langle R, \mathcal{B}(\sigma)\rangle \overset{c?x}{\to} \langle R', \mathcal{B}(\sigma)\rangle$ follows from Lemma 3.1. Consequently, we may obtain $\langle Q\|R, \mathcal{B}(\sigma)\rangle \overset{c?x}{\to} \langle Q\|R', \mathcal{B}(\sigma)\rangle$ by using the **Intl1** rule, because $x \notin fv(Q)$. So, we only need to show that

$$\langle (P\|R')\{y/x\}, \mathcal{B}(\rho)\rangle \mathcal{R} \langle (Q\|R')\{y/x\}, \mathcal{B}(\sigma)\rangle$$

for all $y \notin fv(P\|R') \cup fv(Q\|R') - \{x\}$. Note that $x \notin fv(P) \cup fv(Q)$. Thus, it holds that $(P\|R')\{y/x\} = P\|R'\{y/x\}$ and $(Q\|R')\{y/x\} = Q\|R'\{y/x\}$, and the conclusion follows immediately from the definition of $\mathcal{R}$. $\square$

4.3 Recursion

We now assume a set of process variable schemes, ranged over by $\mathbf{X}, \mathbf{Y}, \dots$. For each process variable scheme $\mathbf{X}$, a nonnegative arity $ar(\mathbf{X})$ is assigned to it. If $\widetilde{x} = x_1, \dots, x_{ar(\mathbf{X})}$ is a tuple of distinct quantum variables, $\mathbf{X}(\widetilde{x})$ 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"):

— *each process variable* $\mathbf{X}(\widetilde{x})$ *is a process expression and* $fv(\mathbf{X}(\widetilde{x})) = \{\widetilde{x}\}$.

We use meta-variables $\mathbf{E}, \mathbf{F}, \dots$ to range over process expressions.

Suppose that $\mathbf{E}$ is a process expression, and $\{\mathbf{X}_i(\widetilde{x}_i) : i \leq m\}$ is a family of process variables. If $\{P_i : i \leq m\}$ is a family of processes such that $fv(P_i) \subseteq \{\widetilde{x}_i\}$ for all $i \leq m$, then we write

$$\mathbf{E}\{\mathbf{X}_i(\widetilde{x}_i) := P_i, i \leq m\}$$

for the process obtained by replacing simultaneously $\mathbf{X}_i\{\widetilde{y}_i\}$ in $\mathbf{E}$ with $P_i\{\widetilde{y}/\widetilde{x}\}$ for all $i \leq m$.

DEFINITION 4.4. *Let* **E** *and* **F** *be process expressions containing at most process variable schemes* $\mathbf{X}_i$ ($i \leq m$). *If for all families* $\{P_i\}$ *of processes with* $fv(P_i) \subseteq \{\widetilde{x}_i\}$, $i \leq m$,

$$\mathbf{E}\{\mathbf{X}_i(\widetilde{x}_i) := P_i, i \leq m\} \sim \mathbf{F}\{\mathbf{X}_i(\widetilde{x}_i) := P_i, i \leq m\},$$

then we say that **E** *and* **F** *are strongly bisimilar and write* $\mathbf{E} \sim \mathbf{F}$.

We now present the main results of this subsection, but their proofs are put into the Appendix to increase readability of the paper. The next proposition indicates that recursive definition preserves strong bisimilarity.

PROPOSITION 4.4. *Let* $\{A_i : i \leq m\}$ *and* $\{B_i : i \leq m\}$ *be two families of process constant schemes, and let* $\{\mathbf{E}_i : i \leq m\}$ *and* $\{\mathbf{F}_i : i \leq m\}$ *contain at most process variable schemes* $\mathbf{X}_i$ ($i \leq m$). *If for all* $i \leq m$, *we have:* $\mathbf{E}_i \sim \mathbf{F}_i$, *and*

$$A_i(\widetilde{x}_i) \stackrel{def}{=} \mathbf{E}_i\{\mathbf{X}_j(\widetilde{x}_j) := A_j(\widetilde{x}_j), j \leq m\},$$

$$B_i(\widetilde{x}_i) \stackrel{def}{=} \mathbf{F}_i\{\mathbf{X}_j(\widetilde{x}_j) := B_j(\widetilde{x}_j), j \leq m\},$$

then $A_i(\widetilde{x}_i) \sim B_i(\widetilde{x}_i)$ *for all* $i \leq m$.

A process variable scheme **X** is said to be weakly guarded in a process expression **E** if every occurrence of **X** in **E** is within a subexpression of the form $\alpha.\mathbf{F}$.

The following proposition shows uniqueness of solutions of equations.

PROPOSITION 4.5. *Suppose that process expressions* $\mathbf{E}_i$ ($i \leq m$) *contain at most process variable schemes* $\mathbf{X}_i$ ($i \leq m$), *and each* $\mathbf{X}_i$ *is weakly guarded in each* $\mathbf{E}_j$ ($i, j \leq m$). *If processes* P_i *and* Q_i ($i \leq m$) *satisfy that, for all* $i \leq m$, $fv(P_i), fv(Q_i) \subseteq \{\widetilde{x}_i\}$, *and*

$$P_i \sim \mathbf{E}_i\{\mathbf{X_j}(\widetilde{x}_j) := P_j, j \leq m\},$$

$$Q_i \sim \mathbf{E}_i\{\mathbf{X_j}(\widetilde{x}_j) := Q_j, j \leq m\},$$

then $P_i \sim Q_i$ *for all* $i \leq m$.

5. STRONG REDUCTION-BISIMILARITY

Quantum operations describe sequential computation in quantum processes. It is obvious that two different sequences of quantum operations may have the same effect, but they are distinguished from each other in defining strong bisimulation (Definition 4.1). To overcome this objection, we need to introduce the notion of operation reduction. Operation reduction between strings of actions is defined by the following two rules: if X_i is a finite subset of Var, $\mathcal{E}^{(i)}$ is a super-operator on $\mathcal{H}_{X_i}$ for all $1 \leq i \leq n$, $X = \bigcup_{i=1}^{n} X_i$, and

$$\mathcal{E} = (\mathcal{E}^{(n)} \otimes \mathcal{I}_{X-X_n}) \circ ... \circ (\mathcal{E}^{(2)} \otimes \mathcal{I}_{X-X_2}) \circ (\mathcal{E}^{(1)} \otimes \mathcal{I}_{X-X_1}),$$

then we have

$$\textbf{Oper-Red} : \frac{}{\mathcal{E}^{(1)}[X_1]\mathcal{E}^{(2)}[X_2]...\mathcal{E}^{(n)}[X_n] \rightarrow \mathcal{E}[X]}$$

$$\textbf{String-Struct} : \frac{t \rightarrow t'}{t_1 t t_2 \rightarrow t_1 t' t_2}$$

where $t, t', t_1, t_2 \in Act^*$ are any strings of actions.

Operation reduction between processes is a natural extension of reduction between strings of actions, and it is defined by the following structural rules:

$$\textbf{Act-Red} : \frac{\alpha_1...\alpha_m \to \beta_1...\beta_n}{\alpha_1....\alpha_m.P \to \beta_1....\beta_n.P}$$

$$\textbf{Pre-Struct} : \frac{P \to P'}{\alpha.P \to \alpha.P'}$$

$$\textbf{Sum-Struct} : \frac{P \to P'}{P + Q \to P' + Q}$$

$$\textbf{Par-Struct} : \frac{P \to P'}{P\|Q \to P'\|Q}$$

$$\textbf{Res-Struct} : \frac{P \to P'}{P\backslash L \to P'\backslash L}$$

$$\textbf{Ref} : \frac{}{P \to P}$$

$$\textbf{Trans} : \frac{P \to Q \quad Q \to R}{P \to R}$$

The symmetric forms of the **Sum-Struct** and **Par-Struct** rules are omitted in the above table.

LEMMA 5.1. (*1*) *For any $P \in \mathcal{P}$, there exists a unique process, written $\lceil P \rceil$, such that $P \to \lceil P \rceil$, and $\lceil P \rceil \to Q$ does not hold for all $Q \in \mathcal{P}$ except $\lceil P \rceil$ itself.*
(2) *If $P \to P'$, then $P' \to \lceil P \rceil$.*

Proof. Induction on the structure of P. □

By ignoring different decompositions of a quantum operation, we have:

DEFINITION 5.1. *Strong reduction-bisimilarity $\overset{*}{\sim}$ is defined to be the transitive closure of $\simeq$, i.e.,*

$$\overset{*}{\sim} = \bigcup_{n=1}^{\infty} \simeq^n,$$

where for any $P, Q \in \mathcal{P}$, $P \simeq Q$ if there are P_1, P_2, Q_1 and Q_2 such that $P \sim P_1 \to P_2$, $Q \sim Q_1 \to Q_2$ and $P_2 \sim Q_2$.

$$P \ \sim \ P_1 \ \to \ P_2$$

$$\simeq \qquad\qquad\quad \sim$$

$$Q \ \sim \ Q_1 \ \to \ Q_2$$

Strong reduction-bisimilarity provides us with a framework in which we can observe interaction between sequential quantum computation and communication of quantum systems. Some basic properties of strong reduction-bisimilarity are presented in the following:

THEOREM 5.1. *(1) If $P \sim Q$ then $P \overset{*}{\sim} Q$.*

(2) If $P \to P'$ then $P \overset{*}{\sim} P'$. In particular, if $X = \bigcup_{i=1}^{n} X_n$ and

$$\mathcal{E} = (\mathcal{E}^{(n)} \otimes \mathcal{I}_{X-X_n}) \circ ... \circ (\mathcal{E}^{(2)} \otimes \mathcal{I}_{X-X_2}) \circ (\mathcal{E}^{(1)} \otimes \mathcal{I}_{X-X_1}),$$

then we have:

(a) $\mathcal{E}^{(1)}[X_1].\mathcal{E}^{(2)}[X_2]....\mathcal{E}^{(n)}[X_n].P \overset{*}{\sim} \mathcal{E}[X].P$;

(b) $A(\widetilde{x}) \overset{*}{\sim} \mathcal{E}[X].A(\widetilde{x})$ when process constant scheme A is defined by

$$A(\widetilde{x}) \overset{def}{=} \mathcal{E}^{(1)}[X_1].\mathcal{E}^{(2)}[X_2]....\mathcal{E}^{(n)}[X_n].A(\widetilde{x}),$$

where $\{\widetilde{x}\} = \bigcup_{i=1}^{n} X_i$.

(3) $\overset{*}{\sim}$ is an equivalence relation.

(4) If $P \overset{*}{\sim} Q$ then

(a) $\alpha.P \overset{*}{\sim} \alpha.Q$;

(b) $P + R \overset{*}{\sim} Q + R$;

(c) $P\|R \overset{*}{\sim} Q\|R$; and

(d) $P\backslash L \overset{*}{\sim} Q\backslash L$.

Proof. (1), (2) and (3) are immediately from Definition 5.1, and (4) may be easily proved by using Theorem 4.1. □

6. APPROXIMATE STRONG BISIMULATIONS

It is required in the definition of strong bisimulation that two bisimilar processes must perform exactly the same sequences of quantum operations. This condition is obviously over-discriminative because two different sequences of quantum operations may have the same effect. Such an observation motivated us to introduce the notion of strong reduction-bisimilarity in the last section. In many cases, however, strong reduction-bisimilarity still may not make sense because quantum operations form a continuum and their minor changes can violate strong reduction-bisimilarity between two quantum processes. Thus, an approximate variant of bisimilarity should be vital in a quantum process algebra. Let λ be a nonnegative real number, and let $\mathcal{R}$ be a binary relation between quantum processes. If for any $P \in \mathcal{P}$ and $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, $D(\rho, \sigma) \leq \lambda$ implies $\langle P, \rho \rangle \mathcal{R} \langle P, \sigma \rangle$, where $D(\cdot, \cdot)$ stands for trace distance, then $\mathcal{R}$ is said to be $\lambda-$closed. Now we are able to define approximate strong bisimulation.

DEFINITION 6.1. *A symmetric, $\lambda-$closed relation $\mathcal{R} \subseteq Con \times Con$ is called a strong $\lambda-$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,*

(1) whenever α is τ or an output and $\langle P, \rho \rangle \overset{\alpha}{\to} \langle P', \rho \rangle$, then for some Q', $\langle Q, \sigma \rangle \overset{\alpha}{\to} \langle Q', \sigma \rangle$ and $\langle P', \rho \rangle \mathcal{R} \langle Q', \sigma \rangle$;

(2) whenever $\langle P, \rho \rangle \overset{\mathcal{E}[X]}{\to} \langle P', \rho' \rangle$, then for some $\mathcal{F}$, Q' and σ', $\langle Q, \sigma \rangle \overset{\mathcal{F}[X]}{\to} \langle Q', \sigma' \rangle$, $\langle P', \rho' \rangle \mathcal{R} \langle Q', \sigma' \rangle$, and $D_\diamond(\mathcal{E}, \mathcal{F}) \leq \lambda$, where diamond distance $D_\diamond(\cdot, \cdot)$ between super-operators is defined as in Subsection 2.6;

(3) *whenever $\langle P, \rho \rangle \overset{c?x}{\to} \langle P', \rho \rangle$ and $x \notin fv(P) \cup fv(Q)$, then for some Q', $\langle Q, \sigma \rangle \overset{c?x}{\to}$ $\langle Q', \sigma \rangle$ and for all $y \notin fv(P') \cup fv(Q') - \{x\}$, $\langle P'\{y/x\}, \rho \rangle \mathcal{R} \langle Q'\{y/x\}, \sigma \rangle$.*

DEFINITION 6.2. *For any $\langle P, \rho \rangle, \langle Q, \sigma \rangle \in Con$, we say that $\langle P, \rho \rangle$ and $\langle Q, \sigma \rangle$ are strongly $\lambda-$bisimilar, written $\langle P, \rho \rangle \sim_\lambda \langle Q, \sigma \rangle$, if $\langle P, \rho \rangle \mathcal{R} \langle Q, \sigma \rangle$ for some strong $\lambda-$bisimulation $\mathcal{R}$. In other words, strong $\lambda-$bisimilarity on Con is defined by*

$$\sim_\lambda = \bigcup \{\mathcal{R} : \mathcal{R} \text{ is a strong } \lambda - \text{bisimulation}\}.$$

DEFINITION 6.3. *Let $P, Q \in \mathcal{P}$. Then:*

(1) *We say that P and Q are strongly $\lambda-$bisimilar, written $P \sim_\lambda Q$, if $\langle P, \rho \rangle \sim_\lambda \langle Q, \rho \rangle$ for all $\rho \in \mathcal{D}(\mathcal{H})$.*

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

$$D_{sb}(P, Q) = \inf\{\lambda \geq 0 : P \sim_\lambda Q\}.$$

The following characterization of $\lambda-$bisimilarity between configurations is useful, and its proof is easy.

LEMMA 6.1. *For any $\langle P, \rho \rangle, \langle Q, \sigma \rangle \in Con$, $\langle P, \rho \rangle \sim_\lambda \langle Q, \sigma \rangle$ if and only if,*

(1) *whenever α is τ or an output and $\langle P, \rho \rangle \overset{\alpha}{\to} \langle P', \rho \rangle$, then for some Q', $\langle Q, \sigma \rangle \overset{\alpha}{\to} \langle Q', \sigma \rangle$ and $\langle P', \rho \rangle \sim_\lambda \langle Q', \sigma \rangle$;*

(2) *whenever $\langle P, \rho \rangle \overset{\mathcal{E}[X]}{\to} \langle P', \rho' \rangle$, then for some $\mathcal{F}$ and Q' and σ', $\langle Q, \sigma \rangle \overset{\mathcal{F}[X]}{\to} \langle Q', \sigma' \rangle$, $\langle P', \rho' \rangle \sim_\lambda \langle Q', \sigma' \rangle$, and $D_\diamond(\mathcal{E}, \mathcal{F}) \leq \lambda$;*

(3) *whenever $\langle P, \rho \rangle \overset{c?x}{\to} \langle P', \rho \rangle$ and $x \notin fv(P) \cup fv(Q)$, then for some Q', $\langle Q, \sigma \rangle \overset{c?x}{\to}$ $\langle Q', \sigma \rangle$ and for all $y \notin fv(P') \cup fv(Q') - \{x\}$, $\langle P'\{y/x\}, \rho \rangle \sim_\lambda \langle Q'\{y/x\}, \sigma \rangle$,*

and the symmetric forms of 1, 2 and 3.

We shall need the following simple lemma in the proof of Theorem 6.1(1) below.

LEMMA 6.2. *If R_i is a strong λ_i-bisimulation $(i = 1, 2)$, then $\mathcal{R}_1 \circ \mathcal{R}_2$ is a strong $(\lambda_1 + \lambda_2)-$bisimulation.*

Proof. We first show that $\mathcal{R}_1 \circ \mathcal{R}_2$ is $(\lambda_1 + \lambda_2)-$closed. If $D(\rho, \sigma) \leq \lambda_1 + \lambda_2$, then there must be δ such that $D(\rho, \delta) \leq \lambda_1$ and $D(\delta, \sigma) \leq \lambda_2$. Since $\mathcal{R}_i$ is λ_i-closed for $i = 1, 2$, it holds that $\langle P, \rho \rangle \mathcal{R}_1 \langle P, \delta \rangle$ and $\langle P, \delta \rangle \mathcal{R}_2 \langle P, \sigma \rangle$. This implies $\langle P, \rho \rangle \mathcal{R}_1 \circ \mathcal{R}_2 \langle P, \sigma \rangle$.

Now suppose that $\langle P, \rho \rangle \mathcal{R}_1 \circ \mathcal{R}_2 \langle Q, \sigma \rangle$. Then $\langle P, \rho \rangle \mathcal{R}_1 \langle R, \delta \rangle \mathcal{R}_2 \langle Q, \sigma \rangle$ for some R and δ. We only need to consider the following case: if $\langle P, \rho \rangle \overset{\mathcal{E}[X]}{\to} \langle P', \rho' \rangle$, then for some $\mathcal{G}$, R' and δ', $\langle R, \delta \rangle \overset{\mathcal{G}[X]}{\to} \langle R', \delta' \rangle$, $\langle P', \rho' \rangle \mathcal{R}_1 \langle R', \delta' \rangle$ and $D_\diamond(\mathcal{E}, \mathcal{G}) \leq \lambda_1$, and furthermore, for some $\mathcal{F}, Q'$ and σ', $\langle Q, \sigma \rangle \overset{\mathcal{F}[X]}{\to} \langle Q', \sigma' \rangle$, $\langle R', \delta' \rangle \mathcal{R}_2 \langle Q', \sigma' \rangle$ and $D_\diamond(\mathcal{G}, \mathcal{F}) \leq \lambda_2$. Then $\langle P', \rho' \rangle \mathcal{R}_1 \circ \mathcal{R}_2 \langle Q', \sigma' \rangle$ and

$$D_\diamond(\mathcal{E}, \mathcal{F}) \leq D_\diamond(\mathcal{E}, \mathcal{G}) + D_\diamond(\mathcal{G}, \mathcal{F}) \leq \lambda_1 + \lambda_2. \ \square$$

The next proposition shows that the process constructors introduced in qCCS are all non-expansive according to pseudo-metric D_{sb}.

THEOREM 6.1. *(1) Strong bisimulation distance D_{sb} is a pseudo-metric on $\mathcal{P}$.*

(2) *For any quantum processes P, Q, we have:*

   (a) $D_{sb}(\alpha.P, \alpha.Q) \leq D_{sb}(P, Q)$ *if α is τ, an output or an input;*

   (b) $D_{sb}(\mathcal{E}[X].P, \mathcal{F}[Y].Q) \leq \max\{\eta_{X,Y}, D_\diamond(\mathcal{E}, \mathcal{F}) + D_{sb}(P, Q)\}$, *where*

$$\eta_{X,Y} = \begin{cases} 0, & \text{if } X = Y, \\ \infty, & \text{otherwise}; \end{cases}$$

   (c) $D_{sb}(P + R, Q + R) \leq D_{sb}(P, Q)$;

   (d) $D_{sb}(P\|R, Q\|R) \leq D_{sb}(P, Q)$ *if all super-operators occurring in P, Q and R are trace-preserving;*

   (e) $D_{sb}(P\backslash L, Q\backslash L) \leq D_{sb}(P, Q)$.

Proof. To prove (1), we only need to check the triangle inequality

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

for any quantum processes P, Q and R. It suffices to show that for any $\lambda_1, \lambda_2 > 0$, if $D_{sb}(P, Q) < \lambda_1$ and $D_{sb}(Q, R) < \lambda_2$, then $D_{sb}(P, R) < \lambda_1 + \lambda_2$. In fact, it follows from $D_{sb}(P, Q) < \lambda_1$ and $D_{sb}(Q, R) < \lambda_2$ that for some $\mu_1 < \lambda_1$ and $\mu_2 < \lambda_2$, we have $P \sim_{\mu_1} Q \sim_{\mu_2} R$. Thus, for all ρ, $\langle P, \rho \rangle \sim_{\mu_1} \langle Q, \rho \rangle \sim_{\mu_2} \langle R, \rho \rangle$, and there are strong μ_1-bisimulation $\mathcal{R}_1$ and strong μ_2-bisimulation $\mathcal{R}_2$ such that $\langle P, \rho \rangle \mathcal{R}_1 \langle Q, \rho \rangle \mathcal{R}_2 \langle R, \rho \rangle$. This leads to $\langle P, \rho \rangle \mathcal{R}_1 \circ \mathcal{R}_2 \langle R, \rho \rangle$. The above lemma asserts that $\mathcal{R}_1 \circ \mathcal{R}_2$ is a strong $(\mu_1 + \mu_2)-$bisimulation, and thus $\langle P, \rho \rangle \sim_{\mu_1 + \mu_2} \langle R, \rho \rangle$. Hence, $P \sim_{\mu_1 + \mu_2} R$, and $D_{sb}(P, R) \leq \mu_1 + \mu_2 < \lambda_1 + \lambda_2$.

(2.a) is immediate from Lemma 6.1. The proofs of (2.c) and (2.e) are easy.

(2.b) It is obvious for the case of $X \neq Y$. Now assume $X = Y$. If $D_\diamond(\mathcal{E}, \mathcal{F}) < \lambda$ and $D_{sb}(P, Q) < \mu$, then there is $\mu' < \mu$ such that $P \sim_{\mu'} Q$; that is, $\langle P, \sigma \rangle \sim_{\mu'} \langle Q, \sigma \rangle$ for all σ. For each ρ, we have $\langle \mathcal{E}[X].P, \rho \rangle \overset{\mathcal{E}[X]}{\to} \langle P, \mathcal{E}_X(\rho) \rangle$ and $\langle \mathcal{F}[Y].Q, \rho \rangle \overset{\mathcal{F}[X]}{\to} \langle Q, \mathcal{F}_X(\rho) \rangle$. Note that

$$D(\mathcal{E}_X(\rho), \mathcal{F}_X(\rho)) = D(\mathcal{E}(\rho), \mathcal{F}(\rho)) \leq D_\diamond(\mathcal{E}, \mathcal{F}) < \lambda$$

and $\sim_\lambda$ is $\lambda-$closed. Then

$$\langle P, \mathcal{E}_X(\rho) \rangle \sim_{\mu'} \langle Q, \mathcal{E}_X(\rho) \rangle \sim_\lambda \langle Q, \mathcal{F}_X(\rho) \rangle,$$

and $\langle P, \mathcal{E}_X(\rho) \rangle \sim_{\lambda + \mu'} \langle Q, \mathcal{F}_X(\rho) \rangle$. From Lemma 6.1 we see that $\langle \mathcal{E}[X].P, \rho \rangle \sim_{\lambda + \mu'} \langle \mathcal{F}[Y].Q, \rho \rangle$. Hence

$$D_{sb}(\mathcal{E}[X].P, \mathcal{F}[X].Q) \leq \lambda + \mu' < \lambda + \mu.$$

This completes the proof by noting that λ and μ are arbitrary.

(2.d) For arbitrary $\lambda > 0$, if $D_{sb}(P, Q) < \lambda$, then there is $\mu < \lambda$ such that $P \sim_\mu Q$; that is, $\langle P, \rho \rangle \sim_\mu \langle Q, \rho \rangle$ for all ρ. Our purpose is to show that $D_{sb}(P\|R, Q\|R) \leq \lambda$. To do this, we only need to find a strong $\mu-$bisimulation $\mathcal{R}_\mu$ containing $(\langle P\|R, \rho \rangle, \langle Q\|R, \rho \rangle)$ for all ρ. This can be carried out by a modification of the technique used in the proof of Theorem 4.1(2.f). We put the technical details into the Appendix. □

An approximate version of strong reduction-bisimilarity can be defined in a natural way:

DEFINITION 6.4. *Let $P, Q \in \mathcal{P}$. Then:*

(1) *We say that P and Q are strongly $\lambda-$reduction-bisimilar, written $P \overset{*}{\sim}_\lambda Q$, if there are $n \geq 0$, $\lambda_1, ..., \lambda_n \geq 0$ and $R_1, R'_1, ..., R_n, R'_n \in \mathcal{P}$ such that $\sum_{i=1}^{n} \lambda_i \leq \lambda$ and*

$$P \overset{*}{\sim} R_1 \sim_{\lambda_1} R'_1 \overset{*}{\sim} ... \overset{*}{\sim} R_n \sim_{\lambda_n} R'_n \overset{*}{\sim} Q.$$

(2) *The strong reduction-bisimulation distance between P and Q is defined by*

$$D_{srb}(P, Q) = \inf\{\lambda \geq 0 : P \overset{*}{\sim}_\lambda Q\}$$

Similar to Theorem 6.1, we have:

THEOREM 6.2. (1) *Strong reduction-bisimulation distance D_{srb} is a pseudo-metric on $\mathcal{P}$.*

(2) *For any quantum processes P, Q, we have:*
   (a) $D_{srb}(\alpha.P, \alpha.Q) \leq D_{srb}(P, Q)$ *if α is τ, an output or an input;*
   (b) $D_{srb}(\mathcal{E}[X].P, \mathcal{F}[Y].Q) \leq \max\{\eta_{X,Y}, D_\diamond(\mathcal{E}, \mathcal{F}) + D_{srb}(P, Q)\}$, *where $\eta_{X,Y}$ is as in Proposition 6.1(2.b);*
   (c) $D_{srb}(P + R, Q + R) \leq D_{srb}(P, Q)$;
   (d) $D_{srb}(P \| R, Q \| R) \leq D_{srb}(P, Q)$ *if all super-operators occurring in P, Q and R are trace-preserving;*
   (e) $D_{srb}(P \backslash L, Q \backslash L) \leq D_{srb}(P, Q)$.

Proof. (1) To show the triangle inequality:

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

it suffices to note that for any $\lambda, \mu \geq 0$, $P \overset{*}{\sim}_\lambda Q$ and $Q \overset{*}{\sim}_\mu R$ implies $P \overset{*}{\sim}_{\lambda+\mu} R$. This is immediate from the definition of strong $\lambda-$reduction-bisimilarity.

(2) We choose to prove (2.b), and the proofs of the other items are similar. Assume that $X = Y$. For any $\lambda \geq 0$, if $P \overset{*}{\sim}_\lambda Q$, then we have

$$P \overset{*}{\sim} R_1 \sim_{\lambda_1} R'_1 \overset{*}{\sim} ... \overset{*}{\sim} R_n \sim_{\lambda_n} R'_n \overset{*}{\sim} Q$$

for some $R_1, R'_1, ..., R_n, R'_n$ and $\lambda_1, ..., \lambda_n$ with $\sum_{i=1}^{n} \lambda_i \leq \lambda$. Then it follows from Theorems 5.1(4) and 6.1(2) that

$$\mathcal{E}[X].P \overset{*}{\sim} \mathcal{E}[X].R_1 \sim_{D(\mathcal{E},\mathcal{F})+\lambda_1} \mathcal{F}[X].R'_1 \overset{*}{\sim} ...$$
$$\overset{*}{\sim} \mathcal{F}[X].R_n \sim_{\lambda_n} \mathcal{F}[X].R'_n \overset{*}{\sim} \mathcal{F}[X].Q$$

On the other hand, we have

$$(D_\diamond(\mathcal{E}, \mathcal{F}) + \lambda_1) + \lambda_2 + ... + \lambda_n \leq D_\diamond(\mathcal{E}, \mathcal{F}) + \lambda.$$

Thus, $\mathcal{E}[X].P \overset{*}{\sim}_{D(\mathcal{E},\mathcal{F})+\lambda} \mathcal{F}[X].Q$. Therefore,

$$D_{srb}(\mathcal{E}[X].P, \mathcal{F}[X].Q) \leq \inf\{D_\diamond(\mathcal{E}, \mathcal{F}) + \lambda : P \overset{*}{\sim}_\lambda Q\}$$
$$= D_\diamond(\mathcal{E}, \mathcal{F}) + D_{srb}(P, Q). \ \square$$

A quantum process $P \in \mathcal{P}$ is said to be finite if it contains no process constants. We write $\mathcal{P}_{fin}$ for the set of finite quantum processes. For any set Ω of quantum gates, we write $\mathcal{P}_{fin}[\Omega]$ for the set of finite quantum processes in which only gates from Ω and measurements in computational bases are used as quantum operations (see Clause 4 in Definition 3.1 and Example 2.5). By combining Theorems 5.1(2.a) and 6.2(2) we obtain:

COROLLARY 6.1. *If Ω is an approximately universal set of quantum gates (e.g., the Hadamard gate, phase gate, CNOT, and $\pi/8$ gate (or the Toffoli gate)) ([15], Chapter 4), then $\mathcal{P}_{fin}[\Omega]$ is dense in $\mathcal{P}_{fin}$ according to pseudo-metric D_{srb}.*

7. CONCLUSION

This paper defines an algebra qCCS of quantum processes and presents its transitional semantics. The strong bisimulation semantics of qCCS is established, and its modification by reduction of quantum operations is given. Furthermore, approximate versions of strong bisimulation and reduction bisimulation are introduced.

We conclude this paper by mentioning some topics for further studies. Only the strong bisimulation semantics of qCCS has been established in the present paper, and a weak bisimulation semantics is still to be exploited for qCCS. However, it is more interesting to consider some problems about quantum processes that are irrelevant in classical quantum process algebras. Several authors started to examine the role of entanglement in quantum sequential computation (see for example [9], [3]). It seems that entanglement is much more essential in quantum concurrent computation. So, an interesting topic is to understand the role of entanglement in computation within the framework of qCCS. The most spectacular result in fault-tolerant quantum computation is the threshold theorem that it is possible to efficiently perform an arbitrarily large quantum computation provided the noise in individual quantum gates is below a certain constant (cf. [15], Section 10.6). This theorem considers only the case of quantum sequential computation. Its generalization in quantum concurrent computation would be a great challenge. The bisimulation distances D_{sb} and D_{srb} introduced in this paper can be used to express certain fault-tolerance criteria.

It is should be pointed out that qCCS is a purely quantum process algebra in the sense that no classical information is explicitly involved in it. The motivation for striping out classical computation and communication is that the combination of classical and quantum information gives rise to major difficulties when attempting to define a bisimilarity which is a congruence with respect to parallel composition. The main purpose and relevance of designing a quantum process algebra is to provide a formal model for distributed quantum computations and quantum communication protocols, typical instances of which are teleportation, super-dense coding and BB84. These paradigmatic protocols rely on both quantum and classical computation and communication. So, one of the most important topics for further studies would be to find a suitable extension of qCCS in which both quantum and classical information can be accommodated well.

ELECTRONIC APPENDIX

The electronic appendix for this article can be accessed in the ACM Digital Library by visiting the following URL: `http://www.acm.org/pubs/citations/journals/tocl/2008-V-N/p1-UF`

REFERENCES

[1] V. Buzek and M. Hillery, Quantum copying: beyond the no-cloning theorem, *Physical Review A,* 54(1996)1844-1852.

[2] D. Dieks, Communication by EPR devices, *Physics Letters A,* 92(1982)271-272.

[3] E. D'Hondt, *Distributed Quantum Computation: A Measurement-Based Approach*, Ph.D Thesis, Vrije Universiteit Brussel, 2005.

[4] Y. Feng, R. Y. Duan, Z. F. Ji and M. S. Ying, Probabilistic bisimulations for quantum processes, *Information and Computation*, 205(2007)1608-1639.

[5] S. J. Gay and R. Nagarajan, Communicating quantum processes, in: *Proceedings of the 32nd ACM Symposium on Principles of Programming Languages, Long Beach, California, USA*, ACM Press, 2005, pp. 145 - 157.

[6] S. J. Gay and R. Nagarajan, Typechecking communicating quantum processes, *Mathematical Structures in Computer Science*, 16(2006)375-406.

[7] P. Jorrand and M. Lalire, Toward a quantum process algebra, in: *Proceedings of the 1st ACM Conference on Computing Frontiers, Ischia, Italy*, ACM Press, 2005, pp. 111 - 119.

[8] P. Jorrand and M. Lalire, From quantum physics to programming languages: a process algebraic approach, in: J. -P. Banatre, P. Fradet, J. -L. Giavitto and O. Michel (eds.), *Unconventional Programming Paradigms, International Workshop UPP 2004, Le Mont Saint Michel, France, September 15-17, 2004, Revised Selected and Invited Papers*, Lecture Notes in Computer Science 3566, Springer, 2005, pp. 1-16.

[9] R. Josza and N. Linden, On the role of entanglement in quantum computational speed-up, *Proc. Roy. Soc. Lond.*, A459(2003)2011-2032.

[10] A. Kitaev, Quantum computations: algorithms and error-correction, *Russian Mathematical Surveys*, 52(1997)1191-1249.

[11] M. Lalire, Relations among quantum processes: Bisimilarity and congruence, *Mathematical Structures in Computer Science*, 16(2006)407-428.

[12] M. Lalire and P. Jorrand, A process algebraic approach to concurrent and distributed quantum computation: operational semantics, in: P. Selinger (ed.), *Proceedings of the 2nd International Workshop on Quantum Programming Languages*, TUCS General Publications 33, Turku Centre for Computer Science, Finland, 2004, pp. 109-126.

[13] R. Milner, *Communication and Concurrency*, Prentice Hall, New York, 1989.

[14] R. Milner, J. Parrow and D. Walker, A calculus of mobile processes, Parts I and II, *Information and Computation,* 100(1992)1-77.

[15] Nielsen, M. A. and Chuang, I. L. *Quantum Computation and Quantum Information,* Cambridge University Press, Cambridge, 2000.

[16] P. Selinger, Towards a quantum programming language, *Mathematical Structures in Computer Science,* 14(2004)527-586.

[17] F. van Breugel, A behavioural pseudometric for metric labelled transition systems, in: *CONCUR 2005 - Concurrency Theory, Proceedings*, LNCS 3653, Springer-Verlag, Heidelberg, pp. 141-155.

[18] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature,* 299(1982)802-803.

[19] M. S. Ying, *Topology in Process Calculus: Approximate Correctness and Infinite Evolution of Concurrent Programs,* Springer-Verlag, New York, 2001.

[20] M. S. Ying, Bisimulation indexes and their applications, *Theoretical Computer Science,* 275(2002)1-68.

[21] M. S. Ying and M. Wirsing, Approximate bisimilarity, in: T. Rus (Ed.), *Algebraic Methodology and Software Technology, 8th International Conference, AMAST 2000, Proceedings*, LNCS 1816, Springer-Verlag, Heidelberg, pp. 309-322.