An Algebraic Language for Distributed Quantum Computing

Mingsheng Ying and Yuan Feng

***Abstract*— A classical circuit can be represented by a circuit graph or equivalently by a Boolean expression. The advantage of a circuit graph is that it can help us to obtain an intuitive understanding of the circuit under consideration, whereas the advantage of a Boolean expression is that it is suited to various algebraic manipulations. In the literature, however, quantum circuits are mainly drawn as circuit graphs, and a formal language for quantum circuits that has a function similar to that of Boolean expressions for classical circuits is still missing. Certainly, quantum circuit graphs will become unmanageable when complicated quantum computing problems are encountered, and in particular when they have to be solved by employing the distributed paradigm where complex quantum communication networks are involved. In this paper, we design an algebraic language for formally specifying quantum circuits in distributed quantum computing. Using this language, quantum circuits can be represented in a convenient and compact way, similar to the way that we use Boolean expressions in dealing with classical circuits. Moreover, some fundamental algebraic laws for quantum circuits expressed in this language are established. These laws form a basis of rigorously reasoning about distributed quantum computing and quantum communication protocols.**

***Index Terms*— Quantum computing, circuits, distributed systems**

I. Introduction

The studies of distributed quantum computing have a history of more than ten years, with the earliest suggestions traced back to Grover [12] and Cleve and Buhrman [3] among others. Various experiments toward physical implementation of distributed quantum computing have been frequently reported in recent years [19]. Also, some computer scientists begun to design architecture of distributed quantum hardware systems; for example [21]. The current theoretical research on distributed quantum computing can be roughly classified into two categories:

- find quantum algorithms for solving paradigmatic problems from classical distributed computing. For example, it was shown that no classical algorithms can solve exactly the leader election problem in anonymous networks [18], but Tani, Kobayashi and Matsumoto [20] and D'Hondt and Panangaden [5] found a quantum algorithm that can solve it for any network topology in polynomial communication/time complexity provided the involved parties are connected by quantum communication links (more precisely, entanglements).
- use the physical resources of two or more small capacity quantum computers to simulate a large capacity quantum computer. For example, Yimsiriwattana and Lomonaco Jr. [26] presented a distributed implementation of Shor's quantum factoring algorithm; Cirac, Ekert, Huelga and Macchiavello [2] examined the performance of distributed quantum computing when quantum communication links between the parties are noisy, using the phase estimation problem as an illustrative example; van Meter, Nemoto and Munro [22] analyzed the effect of various quantum error correction codes and the influence of teleportation failure in designing distributed quantum computing systems.

Up to now, most efforts have been devoted to the second topic because practical quantum computers with large qubit capacity are very difficult to build, and one possible way to overcome this difficulty is to use the distributed paradigm in quantum computing.

Quantum algorithms and protocols are usually expressed in the form of quantum circuits, which are often drawn as circuit graphs in the literature. Obviously, if a quantum algorithm or protocol is very complicated, then its circuit graph would be too big to be drawn and manipulated. The situation becomes even worse in the case of distributed quantum computing where a large number of parties are involved and many communication links among them are present. Recall that in classical computing a circuit can not only be drawn as a circuit graph but also be written as a Boolean expression. Boolean expressions are much more suitable for algebraic manipulations than circuit graphs. In particular, simplification of circuits can be carried out conveniently in the form of Boolean expressions. However, a language which has a function in quantum computing analogous to that of Boolean expressions in classical computing is still missing.

The purpose of this paper is to provide an algebraic language which can express distributed (and sequential) quantum algorithms and quantum communication protocols in a convenient and compact way. We shall carefully define formal semantics of this language. Some fundamental algebraic laws for quantum circuits expressed in this language will be established. This will provide us with convenient and solid mathematical techniques for rigorous reasoning about distributed quantum computing.

This paper is organized as follows: For convenience of the reader, we review some basic notions from quantum mechanics and quantum computing in Section 2, where we also fix some notation needed in the following sections. A single scheme of primitive actions in quantum circuits is isolated and its computational behavior is carefully examined in Section 3. In Section 4, formal definitions of a quantum circuit and its domain and codomain are presented. Then we define the notions of quantum

This work was partly supported by the National Foundation of Natural Sciences of China (Grant No: 60736011, 60621062) and the National Key Project for Fundamental Research of China (Grant No: 2007CB807901).

Corresponding author

Manuscript received February 11, 2008; revised xxxx, 2008.

The authors are with the Center of Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology, Sydney, NSW 2007, Australia, and the State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China (email: yingmsh@tsinghua.edu.cn)

resource and classical communication in a quantum circuit. In particular, we introduce the notion of partition of subsystems in order to describe distributed quantum computing. Section 5 is devoted to establishing various useful algebraic laws for quantum circuits. A normal form of quantum circuits with quantum resources explicitly displayed before primitive actions is then obtained by using these laws. In Section 6, we present some examples to illustrate the expressive power of the formal language developed in the present paper. We draw a brief conclusion and point out some topics for further studies in Section 7. The proofs of the main results are put into the appendix.

II. Preliminaries and Notation

A. Qubits

The basic data unit in a quantum computer is a qubit, which can be physically realized by a two-level quantum-mechanical system, e.g., the horizontal and vertical polarizations of a photon, or the up and down spins of a single electron. Formally, the state space of qubits is the $2-$dimensional Hilbert space $\mathcal{H}_2$. A qubit is represented by a unit vector in $\mathcal{H}_2$ of the form $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, where $|0\rangle$ and $|1\rangle$ are two basis states, and α_0 and α_1 are complex numbers with $|\alpha_0|^2 + |\alpha_1|^2 = 1$. More generally, we can introduce the notion of multi-qubit which is used in quantum computing as a register. To do this, we need to fix a notation. In set theory, an ordinal number is defined to be the set of all ordinal numbers smaller than it. We adopt this idea in this paper; that is, we shall use n to denote the set of the first n nonnegative integers, $n = \{0, 1, ..., n-1\}$. In particular, $2 = \{0, 1\}$. For any finite set I, a $|I|-$qubit may be indexed by I, where $|I|$ stands for the cardinality of I. An $I-$indexed $|I|-$qubit will be simply called an $I-$qubit. The state space of $I-$qubits is the tensor product $\mathcal{H}_2^{\otimes I}$ of $I-$indexed copies of $\mathcal{H}_2$ according to a basic postulate of quantum mechanics. Thus, an $I-$qubit is represented by a unit vector in $\mathcal{H}_2^{\otimes I}$, which can be written as $|\psi\rangle = \sum_{t\in 2^I} \alpha_t|t\rangle$, where 2^I is the power set of I, i.e. the set of mappings from I into 2, and all α_t are complex numbers and they are called amplitudes. It is required that α_t's satisfy the normalization condition $\sum_{t\in 2^I} |\alpha_t|^2 = 1$. We often use the subscript I in $|\psi\rangle_I$ to indicate that $|\psi\rangle$ is in $\mathcal{H}_2^{\otimes I}$. More precisely, if $|I| = n$ and $I = \{A_0, A_1, ..., A_{n-1}\}$, then for each $t \in 2^I$, $|t\rangle_I$ stands for $|t_0\rangle_{A_0}|t_1\rangle_{A_1}...|t_{n-1}\rangle_{A_{n-1}}$, where $t_i = t(A_i) = 0$ or 1 and the subscript A_i is used to indicate the fact that the bit $|t_i\rangle$ belongs to the A_i-systems for all $i = 0, 1, ..., n-1$. For any $|\psi\rangle \in \mathcal{H}_2^{\otimes I}$, we define the domain of $|\psi\rangle$ to be $dom(|\psi\rangle) = I$. The reason for introducing an abstract index set I is that one may use other symbols rather than nonnegative integers to name qubits in applications. We now turn to consider the special case where I is an initial segment of nonnegative integers. First, we shall identify $\mathcal{H}_2$ with $\mathcal{H}_2^{\otimes 1}$. More generally, for any positive integer n, each $t \in 2^n$ can be written as an n-bit string $t(0)t(1)...t(n-1)$. So, an $n-$qubit is a superposition of $n-$bits, and it can be written in the following way:

$$|\psi\rangle = \sum_{t_0,t_1,...,t_{n-1}\in\{0,1\}} \alpha_{t_0t_1...t_{n-1}}|t_0t_1...t_{n-1}\rangle,$$

where $\{|t_0t_1...t_{n-1}\rangle : t_0, t_1, ..., t_{n-1} = 0 \text{ or } 1\}$ is the standard orthonormal basis, called the computational basis, of $\mathcal{H}_2^{\otimes n}$. Furthermore, $|\psi\rangle$ can be conveniently represented by the complex column vector $(\alpha_{t_0t_1...t_{n-1}} : t_0, t_1, ..., t_{n-1} \in \{0, 1\})^T$ of length 2^n, where components $\alpha_{t_0t_1...t_{n-1}}$ are arranged according to the lexical ordering of $t_0t_1...t_{n-1}$, and T stands for transpose. We can also write $|\psi\rangle = (\alpha_0, \alpha_1, ..., \alpha_{2^n-1})^T$ if we identify the integer $t_0 2^{n-1} + t_1 2^{n-2} + ... + t_{n-1}2^0$ with its binary representation $t_0t_1...t_{n-1}$. (Here you see that treating n as the set of the first n nonnegative integers enables a smooth transition between $\mathcal{H}_2^{\otimes n}$ and $\mathcal{H}_2^{\otimes I}$). The GHZ (Greenberger-Horne-Zeilinger) state $|E_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$ in $\mathcal{H}_2^{\otimes n}$ is frequently used in distributed quantum computation, where we use $|t\rangle^{\otimes n}$ to denote $|tt...t\rangle$ (n t's) for $t = 0, 1$. In particular, $|E_2\rangle = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle$ is called the EPR (Einstein-Podolsky-Rosen) state. We shall simply write $|E\rangle$ for $|E_2\rangle$. Using the vector notation of qubits, $|E_n\rangle$ can be written as $\frac{1}{\sqrt{2}}(1, \overbrace{0, ..., 0}^{2^n-2}, 1)^T$, and $|E\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$.

A convenient way of describing quantum systems whose states are not completely known is to introduce the notion of ensemble. We use the term ensemble when, roughly speaking, we are holding some classical information that tells us which of several possible quantum states the system is in. For example, this approach is used for quantum error correction, where the (classical) syndrome is paired with a quantum state, and the goal is to choose repair operations based on the syndrome that will coalesce the various ensemble members back to the desired quantum state. In Subsection II-C, ensembles will be used to describe outcomes of quantum measurements. An easy way of formally manipulating ensembles is to treat them as multi-sets which are generalizations of a set. A member of a multi-set can have more than one membership, while each member of a set has only one membership. We shall use $\{.\}$ to denote sets and use $\{|.|\}$ to denote multi-sets. A multi-set $\mathcal{E} = \{|(p_i, |\psi_i\rangle) : i = 1, ..., n|\}$ is called an ensemble in $\mathcal{H}_2^{\otimes I}$ if $0 \leq p_i$ and $|\psi_i\rangle$ is a quantum state in $\mathcal{H}_2^{\otimes I}$ for each i, and $\sum_{i=1}^n p_i = 1$, where p_i stands for the probability that the system is in state $|\psi_i\rangle$. We write $s(\mathcal{E}) = \{|\psi_i\rangle : i = 1, ..., n\}$ for the set of quantum states occurring in $\mathcal{E}$. For each $|\psi\rangle \in s(\mathcal{E})$, put $p(|\psi\rangle) = \sum\{|p_i : |\psi_i\rangle = |\psi\rangle, 1 \leq i \leq n|\}$. Then we shall not distinguish the ensemble $\mathcal{E}$ from its reduction ensemble $\{(p(|\psi\rangle), |\psi\rangle) : |\psi\rangle \in s(\mathcal{E})\}$, which is a set. Furthermore, we shall not distinguish a pure state $|\psi\rangle$ from the singleton ensemble $\{(1, |\psi\rangle)\}$ in which the system is in state $|\psi\rangle$ with probability 1. We say that the domain of $\mathcal{E}$ is I and write $dom(\mathcal{E}) = I$ if $\mathcal{E}$ is an ensemble in $\mathcal{H}_2^{\otimes I}$. We introduce the empty ensemble in $\mathcal{H}_2^{\otimes I}$, written $\emptyset_I$, which is not really an ensemble. This will allow us to define a so-called inactive circuit in a convenient way. It is reasonable to identify $\emptyset_I$ with $\emptyset_J$ for any two finite sets I and J. Thus, the subscript I of $\emptyset_I$ will always be dropped.

B. Quantum Gates

A quantum gate acting on a quantum register consisting n qubits is described by a $2^n \times 2^n$ unitary matrix, that is, a complex matrix such that $UU^\dagger$ is the identity matrix, where $U^\dagger$ stands for the Hermitian conjugate (or conjugate transpose) of U; that is, the $(i, j)-$entry of $U^\dagger$ is the complex conjugate of $(j, i)-$entry of U.

The evolution of quantum states is described by a quantum gate. If $|\psi\rangle = (\alpha_0, \alpha_1, ..., \alpha_{2^n-1})^T$ is a quantum state in $\mathcal{H}_2^{\otimes n}$, and U is an $n-$qubit gate, then the outcome of performing U on $|\psi\rangle$ is defined to be the quantum state in $\mathcal{H}_2^{\otimes n}$ represented by the

vector $U|\psi\rangle$, where $U|\psi\rangle$ is given according to the usual matrix multiplication.

We now give some examples of quantum gate. The Pauli gates are single-qubit gates: $X = NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Another useful single-qubit gate is the Hadamard gate: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Thus,

$$NOT|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle,$$

$NOT|1\rangle = |0\rangle$, $Y|0\rangle = i|1\rangle$, $Y|1\rangle = -i|0\rangle$, $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$. Also, we have:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. We shall need controlled gates in the following sections. Let U be a $k-$qubit gate. Then $C^n(U)$ is defined to be an $(n+k)-$qubit gate, and with linearity it is uniquely determined by its action on the computational basis of the $n-$qubit subsystem and its action on the remaining $k-$qubit subsystem, i.e. the following equation: $C^{(n)}(U)|t_0t_1...t_{n-1}\rangle|\psi\rangle = |t_0t_1...t_{n-1}\rangle U^{t_0t_1...t_{n-1}}|\psi\rangle$ for any $t_0, t_1, ..., t_{n-1} \in \{0,1\}$ and $|\psi\rangle \in \mathcal{H}_2^{\otimes k}$. In the right-hand side of the above equation the exponential $t_0t_1...t_{n-1}$ of U means the product of $t_0, t_1, ..., t_{n-1}$. We shall simply write $CNOT$ for $C^{(1)}(NOT)$. For example,

$$CNOT|E\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle).$$

Note that in the above example the input $|E\rangle$ is an entangled state in the sense that it cannot be factored in the way of $|E\rangle = |\psi_1\rangle|\psi_2\rangle$ with $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_2$. On the other hand, the output is a product state because it can be written as $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$. So, $CNOT$ transforms an entangled state $|E\rangle$ to a product state. Conversely, it also transforms the product state $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ to the entangled state $|E\rangle$.

To define unitary transformation on $\mathcal{H}_2^{\otimes I}$, we need to introduce some notation. If $h : I \to J$ is a bijection, then it defines a linear operator $h : \mathcal{H}_2^{\otimes I} \to \mathcal{H}_2^{\otimes J}$ by $h(\otimes_{i\in I}|\psi_i\rangle_i) \stackrel{def}{=} \otimes_{i\in I}|\psi_i\rangle_{h(i)}$ for all $|\psi_i\rangle \in \mathcal{H}_2$, $i \in I$. Intuitively, h is a renaming function; that is, it changes a qubit indexed by i to a qubit indexed by $h(i)$. Moreover, if $\mathcal{E}$ is an ensemble, then we write $h(\mathcal{E}) = \{|(p, h(|\psi\rangle)) : (p, |\psi\rangle) \in \mathcal{E}|\}$. In particular, we have $h(\emptyset) = \emptyset$. For any mapping $f : X \to Y$, we write $dom(f)$ and $ran(f)$ for the domain and range of h, respectively; that is, $dom(f) = X$ and $ran(f) = \{f(x) : x \in X\}$. Suppose that U is an $n-$qubit gate and h is a one-to-one mapping with $dom(h) = n$ and $ran(h) = I$. Then we can use U and h to define a unitary transformation U_h on $\mathcal{H}_2^{\otimes I}$. Intuitively, U_h acts on the $I-$qubits according to the ordering of members in I given by h; i.e. the $h(k)-$qubit is the $(k+1)$th qubit to which U is applied for all $k \leq n-1$. Formally, for any quantum state $|\psi\rangle \in \mathcal{H}_2^{\otimes I}$, $U_h(|\psi\rangle) \stackrel{def}{=} h(U(h^{-1}(|\psi\rangle)))$. The intuition behind the above equation is as follows: U is a unitary operator on $\mathcal{H}_2^{\otimes n}$ and we wish to apply it to a state $|\psi\rangle$ in $\mathcal{H}_2^{\otimes I}$. So, we first map $|\psi\rangle$ to a canonical form in $\mathcal{H}_2^{\otimes n}$ that allows us to apply U, and then undo the mapping to restore the obtained state to the original qubit locations. Alternatively, if $U = \bigotimes_{k=0}^{n-1} U_k$, where each U_k is a single-qubit gate on the $(k+1)$th qubit and $\bigotimes$ stands for tensor product of matrices, and $t_i \in \{0,1\}$ for all $i \in I$, then $U_h(\bigotimes_{i\in I}|t_i\rangle_i) \stackrel{def}{=} \bigotimes_{i\in I}(U_{h^{-1}(i)}|t_i\rangle)_i$. In general, since the set of product unitary operators forms a basis of the space of matrices, U can be written in the following way:

$$U = \sum_l \alpha_l (\bigotimes_{k=0}^{n-1} U_{lk}) \quad (1)$$

where U_{lk} is a single-qubit gate acting on the $(k+1)$th qubit for all l, k, and the above defining equation can be easily extended to the general case by linearity.

C. Quantum Measurements

One of the most significant differences between classical and quantum information comes from quantum measurement. In this paper we only consider quantum measurement in the computational basis. Let $|\psi\rangle$ be a quantum state in $\mathcal{H}_2^{\otimes I}$, and let $J \subseteq I$. Then $|\psi\rangle$ can be written in the following way: $|\psi\rangle = \sum_{t\in 2^J} \alpha_t|t\rangle_J|\psi_t\rangle$ where $|\psi_t\rangle$ is in $\mathcal{H}_2^{\otimes(I\setminus J)}$ for each $t \in 2^J$. Obviously, $\{|t\rangle : t \in 2^J\}$ is the computational basis of the state space $\mathcal{H}_2^{\otimes J}$ of $J-$qubits, which forms a subsystem of $I-$qubits. If the quantum measurement in the computational basis is performed on the $J-$qubits, then we obtain the ensemble $\{|(|\alpha_t|^2, |\psi_t\rangle)|\}$. This means that the probability that the measurement outcome is t is $|\alpha_t|^2$, and the state of the remaining subsystem, the $(J \setminus I)-$qubits, becomes $|\psi_t\rangle$ (and the whole system is in state $|t\rangle|\psi_t\rangle$) immediately after the measurement if the measurement outcome is t for any $t \in 2^J$. As an example, we consider a state of two qubits $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. If we perform a measurement in the computational basis on the first qubit, then for $i = 0, 1$, the probability that we get i is $p_i = |\alpha_{i0}|^2 + |\alpha_{i1}|^2$, and the state of the second qubit after the measurement is $\frac{1}{\sqrt{p_i}}(\alpha_{i0}|0\rangle + \alpha_{i1}|1\rangle)$. If we perform a measurement in the computational basis on the two qubits, then the probability that the outcome of measurement is two-bit classical information ij is $p_{ij} = |\alpha_{ij}|^2$, and the post-measurement state of the two qubits is the basis state $|ij\rangle$, for any $i, j = 0, 1$.

It is well-known that quantum measurements in other bases can be carried out by combining unitary transformation and measurement in the computational basis.

D. Notation

In this subsection, we introduce some set-theoretic notation that will be needed in what follows. Let X be a set, and let $\mathcal{P} = \{X_t : t \in T\}$, where T is a nonempty index set. If $X \supseteq \bigcup_{t\in T} X_t$, and $X_t \cap X_{t'} = \emptyset$ whenever $t \neq t'$, then $\mathcal{P}$ is called a partial partition of X. In particular, if $X = \bigcup_{t\in T} X_t$, then partial partition $\mathcal{P}$ is called a partition of X. If $f : X \to Y$ and $g : Y \to Z$ are two mappings, then we write $f \circ g$ for the composition of f and g; that is, $(f \circ g)(x) = g(f(x))$ for all $x \in X$. Let $f : X \to Y$ be a mapping and $Z \subseteq X$. Then the restriction of f on Z is defined to be the mapping $f|Z : Z \to Y$ such that $(f|Z)(x) = f(x)$ for all $x \in Z$. If $X_1 \cap X_2 = \emptyset$, and $f_1 : X_1 \to Y$ and $f_2 : X_2 \to Y$

are two mappings, then the merging of f_1 and f_2 is defined to be the mapping $f_1 \cup f_2 : X_1 \cup X_2 \to Y$,

$$(f_1 \cup f_2)(x) = \begin{cases} f_1(x) \text{ if } x \in X_1, \\ f_2(x) \text{ if } x \in X_2. \end{cases}$$

III. Primitive Actions

Let $\mathcal{N}$ be a (finite or countably infinite) set of qubit names. Usually, $\mathcal{N}$ will be taken as the set of nonnegative integers or one of its subsets, e.g. an initial segment $n = \{0, 1, ..., n-1\}$ for some $n \geq 0$. Let $\mathcal{G}$ be a set of quantum gates. For each $U \in \mathcal{G}$, we write $ar(U)$ for the arity of U, i.e. $U : \mathcal{H}_2^{\otimes ar(U)} \to \mathcal{H}_2^{\otimes ar(U)}$ is a unitary operator acting on $ar(U)-$qubits.

We choose to use a single scheme of primitive actions.

Definition 3.1: The primitive actions generated by $\mathcal{G}$ over $\mathcal{N}$ are of the form:

$$M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}] \tag{2}$$

where $I \subseteq \mathcal{N}$, $U_l \in \mathcal{G}$, f_l is a computable function and $h_l : \{0, 1, ..., ar(U_l) - 1\} \to \mathcal{N}$ is a one-to-one mapping for each $l \leq k$, and it is required that

$$I \cap \bigcup_{l=1}^{k} ran(h_l) = \emptyset. \tag{3}$$

Their domain and codomain are defined by

$$dom(M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}]) = I \cup \bigcup_{l=1}^{k} ran(h_l),$$

$$codom(M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}]) = \bigcup_{l=1}^{k} ran(h_l).$$

Intuitively, we use the primitive action (2) to denote the composed action consisting of the following three steps:

- *Measurement.* A measurement in the computational basis is performed on the $I-$qubits, leaving the $(\mathcal{N} \setminus I)-$qubits unchanged;
- *Classical communications.* The outcome $t \in \{0, 1, ..., 2^{|I|} - 1\}$ is then broadcast to the $ran(h_1)-$qubits,..., $ran(h_k)-$qubits; and
- *Unitary transformations.* For each $l \leq k$, $f_l(t)$ copies of U_l are applied to the $ran(h_l)-$qubits, where the $ran(h_l)-$qubits are arranged according to the ordering given by h_l, i.e. the $h_l(i)-$qubit is the $(i+1)$th qubit to which U_l is applied for all $i \leq ar(U_l) - 1$.

Although a primitive action consists of three steps, it will always be treated as a single entity.

The condition (3) means that the measurement on the $I-$qubits destroyed the $I-$indexed subsystem, the subsystem stores classical information but not qubits, and thus the subsequent unitary transformations are not allowed to act on it. Note that the ranges of h_{l_1} and h_{l_2} are not required to be disjoint for different l_1 and l_2. Thus, the ordering of $U_1, ..., U_k$ in the primitive action (2) cannot be ignored. Of course, it will be shown in the sequel that the positions of $U_1, ..., U_k$ can be exchanged when the ranges of $h_1, ..., h_k$ are pairwise disjoint.

It is worth noting that the classical information extracted by the measurement is used in the unitary transformation step. It should also be noted that classical computation is needed in this step in order to compute the values $f_l(t)$. To simplify the presentation, classical computational ability of each subsystem is assumed to be unbounded, and thus classical computational complexity is always ignored.

For any $I \subseteq \mathcal{N}$, we often write I as a sequence of its elements. Sometimes, the ordering of elements of I in this sequence is unimportant. We write Id_I for the identity operator on the $I-$qubits. A one-to-one mapping $h : \{0, 1, ..., n-1\} \to \mathcal{N}$ is often written as the sequence $h(0), h(1), ..., h(n-1)$. Note that usually the ordering of members in $ran(h_l)$ determined by h_l in the primitive action (2) cannot be ignored because U_l is not necessarily completely symmetric. For example, $CNOT_{1,2}$ stands for the controlled NOT gate with the first qubit as the control qubit and the second qubit as the target qubit, but $CNOT_{2,1}$ stands for the controlled NOT gate where the second qubit is the control qubit and the first qubit is the target qubit.

The motivation of taking a general scheme of primitive actions is to guarantee that the model developed in this paper can be used as widely as possible. In a concrete application, of course, only a special (usually very small) class of primitive actions will considered. Two special classes of primitive actions will be used frequently in the sequel:

- If $I = \emptyset$, then the primitive action (2) becomes a sequence of unitary transformations, without any measurement. In particular, if $k = 1, U_1 = U$ and $f_1(t) = 1$, then the primitive action (2) is exactly the unitary operator U acting on $ran(h_1)$, and we shall simple write $U_{h(0),h(1),...,h(ar(U)-1)}$ for this action.
- If $k = 0$, then the function of the primitive action (2) is to trace out the $I-$qubits; that is, we perform a measurement (in the computational basis) on the $I-$qubits, but the outcome of measurement is ignored. (Since $k = 0$, we have nowhere to use the classical information gained by the measurement.) In this case, we shall simply write M_I for the primitive action.

Now we formally define how a primitive action is applied to a quantum state. To this end, we need to introduce an auxiliary notation for ensembles. For any finite subsets I, J of $\mathcal{N}$ with $I \cap J = \emptyset$, an $I-$indexed ensemble in $\mathcal{H}_2^{\otimes J}$ is of the form

$$\{|(p_t, |\psi_t\rangle) : t \in 2^I|\}, \tag{4}$$

where $|\psi_t\rangle \in \mathcal{H}_2^{\otimes J}$ is a pure state for each t. We often use $t \in 2^I$ as the binary representation of a nonnegative integer smaller than $2^{|I|}$, i.e. $t = t(i_0)2^{|I|-1} + t(i_1)2^{|I|-2} ... + t(i_{|I|-1})2^0$ whenever I is written as $i_0, i_1, ..., i_{|I|-1}$ (and thus $|t\rangle = |t(i_0)t(i_1)...t(i_{|I|-1})\rangle$ is a computational basis state of the $I-$qubits). The aim of introducing such a notation is to provide a convenient way of representing quantum measurement in the computational basis. We consider a quantum system consisting of $I \cup J-$indexed qubits, where $I \cap J = \emptyset$. If a measurement is performed on the $I-$indexed subsystem, then the outcome will be an $I-$indexed ensemble in $\mathcal{H}_2^{\otimes J}$. In this way, the post-measurement state of the measured subsystem (i.e. the $I-$qubits) is discarded, although the classical information about it is indeed (implicitly) recorded in the ensemble. Discarding the $J-$subsystem allows us to considerably simplify the presentation, but it is still there as a physical system and can be reused later, sometimes after renaming. Note that in the notation (4), only the probabilities and the states after measurements are explicitly displayed, and the corresponding measurement outcomes (the classical information extracted by the measurement) t are implicitly encoded in the subscripts of its components $(p_t, |\psi_t\rangle)$. To explicitly express the classical information obtained in the measurement, we can simply add t

into the $2-$tuple $(p_t, |\psi_t\rangle)$ so that is is enlarged to the $3-$tuple $(t, p_t, |\psi_t\rangle)$. In this paper, however, we choose to use the simpler notation (4) since it is good enough for our purpose.

Suppose that J is a finite set satisfying

$$I \cup \bigcup_{l=1}^{k} ran(h_l) \subseteq J \subseteq \mathcal{N}. \tag{5}$$

For any pure state $|\psi\rangle \in \mathcal{H}_2^{\otimes J}$, if $|\psi\rangle = \sum_{t\in 2^I} \alpha_t |t\rangle_I |\widetilde{\psi}_t\rangle$, where $|\widetilde{\psi}_t\rangle \in \mathcal{H}_2^{\otimes(J\setminus I)}$ is a pure state for each t, then

$$M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}](|\psi\rangle) \tag{6}$$

is defined to be the $I-$indexed ensemble $\{|(|\alpha_t|^2, |\varphi_t\rangle) : t \in 2^I|\}$ in $\mathcal{H}_2^{\otimes(J\setminus I)}$, where $|\varphi_t\rangle \stackrel{def}{=} V_k(t)...V_1(t)|\widetilde{\psi}_t\rangle$, and $V_l(t) \stackrel{def}{=} U_{lh_l}^{f_l(t)} \otimes Id_{J\setminus I\setminus ran(h_l)}$ for each $t \in 2^I$ and $l \leq k$. In the above defining equation, $U_{lh_l}^{f_l(t)}$ stands for the composition of $f_l(t)$ copies of U_l acting on $ran(h_l)$, and $ran(h_l)-$qubits are ordered according to h_l. More precisely, we choose an arbitrary bijection $h_l' : \{ar(U_l), ar(U_l)+1, ..., |J\setminus I|\} \to J \setminus I \setminus ran(h_l)$. Then $g_l \stackrel{def}{=} h_l \cup h_l' : |J\setminus I| \to J\setminus I$ is a bijection, and we define:

$$V_l(t)(|\varphi\rangle) \stackrel{def}{=} g_l((U_l^{f_l(t)} \otimes Id_{|J\setminus I\setminus ran(h_l)|})g_l^{-1}(|\varphi\rangle))$$

for any $|\varphi\rangle$ in $\mathcal{H}_2^{\otimes(J\setminus I)}$, where $Id_{|J\setminus I\setminus ran(h_l)|}$ is the identity operator on the $|J\setminus I\setminus ran(h_l)|-$qubits, and $|J\setminus I\setminus ran(h_l)|$ is a nonnegative integer and treated as the set of all nonnegative integers smaller than it. In the definition of Eq. (6), we keep track of all the measurement outcomes throughout the computation. This is because the behavior of a distributed quantum computing system is usually analyzed in such a way in the existing literature. But the problem is that the obtained ensemble could be very large. So, we often need to consider the reduction of an ensemble to minimize its size in applications.

From Eq. (5), it can be seen that the domain J of the quantum state $|\psi\rangle$ in (6) may be truly larger than the domain $I \cup \bigcup_{l=1}^{k} ran(h_l)$ of the primitive action in (6) and thus the $(J \setminus I \cup \bigcup_{l=1}^{k} ran(h_l))-$indexed subsystem of $|\psi\rangle$ is left unchanged. If we consider the primitive action in (6) independently from its environment, it is reasonable to define (6) only for the quantum states with the same domain as the primitive action. However, a primitive action is always connected to/by other primitive actions whose domains may be different to form a big quantum circuit. To examine the computational behavior of such a circuit, it is necessary to define the effect of this primitive action on quantum states which contains some qubits occurring not in the domain of this action but in the domains of the other actions.

A primitive action may include a destructive measurement in the sense that some qubits are discarded after the measurement. So, it is reasonable to also include the possibility of adding new qubits. A common snapshot of distributed quantum computing is: a local party prepares a set of ancilla qubits, has them interacting with some other qubits, measures the ancilla qubits, and broadcasts the outcome; then certain unitary transformations are performed, conditioned on the measurement outcome. At the next step, some new ancillas are prepared (or some old ones are reset). Except the preparation of ancilla qubits, the above picture is exactly what a primitive action describes. However, a single primitive action cannot depict the mechanism of adding new qubits. It will be implicitly realized by concatenation of circuits defined below.

To illustrate the above definition, we consider a simple example. Let

$$|\psi\rangle = \frac{1}{\sqrt{2}}|011\rangle + \frac{1}{2}|101\rangle + \frac{1}{2}|110\rangle. \tag{7}$$

Then

$$M_1^t[H_0^t, CNOT_{2,0}^{1-t}](|\psi\rangle_{0,1,2})$$
$$= \{(\frac{1}{4}, |01\rangle), (\frac{3}{4}, \frac{1}{\sqrt{6}}|00\rangle + \frac{1}{\sqrt{3}}|01\rangle - \frac{1}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{3}}|11\rangle)\},$$

and it is an ensemble in $\mathcal{H}_2^{\otimes\{0,2\}}$ (the subscripts $0, 2$ of the basis states $|ij\rangle$, $(i, j = 0, 1)$ are omitted in the above equation).

The performance of primitive actions on pure states can be generalized to the case of ensembles in a natural way. Assume that J and K are finite subsets of $\mathcal{N}$ and $J \cap K = \emptyset$. Let $\mathcal{E} = \{|(p_t, |\psi_t\rangle) : t \in 2^J|\}$ be a $J-$indexed ensemble in $\mathcal{H}_2^{\otimes K}$. If $I \cup \bigcup_{l=1}^{k} ran(h_l) \subseteq K$, and for each $t \in 2^J$, the outcome of the primitive action in (6) performing on $|\psi_t\rangle$ is already defined, say,

$$M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}](|\psi_t\rangle) = \{|(p_{t,s}, |\psi_{t,s}\rangle) : s \in 2^I|\},$$

then

$$M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}](\mathcal{E}) \stackrel{def}{=} \{|(q_r, |\varphi_r\rangle) : r \in 2^{J\cup I}|\}, \tag{8}$$

where $q_r = p_{r|J} \cdot p_{r|J,r|I}$, $\varphi_r = |\psi_{r|J,r|I}\rangle$, and $r|I$, $r|J$ are the restrictions of r on I and J, respectively, for each r. It is a $J \cup I-$indexed ensemble in $\mathcal{H}_2^{(K\setminus I)}$. In particular, we define: $M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}](\emptyset) \stackrel{def}{=} \emptyset$.

As an example, let $\mathcal{E} = \{(\frac{1}{3}, |\psi\rangle_{0,1,2}), (\frac{2}{3}, |E_3\rangle_{0,1,2})\}$, where $|\psi\rangle$ is given by Eq. (7). Then

$$M_1^t[H_0^t, CNOT_{2,0}^{1-t}](\mathcal{E})$$
$$= \{(\frac{1}{3}, |00\rangle), (\frac{1}{12}, |01\rangle), (\frac{1}{3}, \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)),$$
$$(\frac{1}{4}, \frac{1}{\sqrt{6}}|00\rangle + \frac{1}{\sqrt{3}}|01\rangle - \frac{1}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{3}}|11\rangle)\}$$

is an ensemble in $\mathcal{H}_2^{\otimes\{0,2\}}$.

IV. Circuits

In this paper, both centralized quantum computing and distributed quantum computing will be represented by quantum circuits. The difference between centralized quantum computing and distributed quantum computing is that a circuit for the former is always treated as a single system, whereas a circuit for the latter is usually divided into several subsystems, connected by classical or quantum communication links (see Subsection IV-C below). Intuitively, a circuit consists of a set of primitive actions, connected by quantum wires that carry qubits, together with certain quantum resources provided a priori (usually entanglements between some parties as quantum communication links). A circuit $\mathcal{C}$ will be used to express a computation of which the inputs are $dom(\mathcal{C})-$qubits, and the outputs are $codom(\mathcal{C})-$qubits, where $dom(\mathcal{C})$ and $codom(\mathcal{C})$ stands for the domain and codomain of $\mathcal{C}$, respectively. Formally, we have:

Definition 4.1: Quantum circuits generated by $\mathcal{G}$ over $\mathcal{N}$ and their domains and codomains are recursively defined as follows:

- For any finite subsets I and J of $\mathcal{N}$, $\mathbf{0}_{I,J}$ is a circuit, called inactive circuit from I to J, and $dom(\mathbf{0}_{I,J}) = I$ and $codom(\mathbf{0}_{I,J}) = J$.

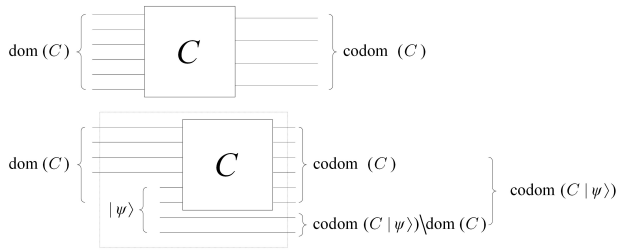

Fig. 1. Circuit composed with physical resource

- If A is a primitive action generated by $\mathcal{G}$ over $\mathcal{N}$, then A is a circuit, and $dom(A)$ and $codom(A)$ are defined as in Definition 3.1.
- If $\mathcal{C}$ is a circuit, and $|\psi\rangle$ is a quantum state, then $\mathcal{C}|\psi\rangle$ is also a circuit, and

$$dom(\mathcal{C}|\psi\rangle) = dom(\mathcal{C}) \setminus dom(|\psi\rangle),$$
$$codom(\mathcal{C}|\psi\rangle) = codom(\mathcal{C}) \cup [dom(|\psi\rangle) \setminus dom(\mathcal{C})].$$

- If $\mathcal{C}$ is a circuit, and $\theta : \mathcal{N} \to \mathcal{N}$ is a bijection, called a renaming function, then $\mathcal{C}[\theta]$ is a circuit, and

$$dom(\mathcal{C}[\theta]) = \theta(dom(\mathcal{C})),$$
$$codom(\mathcal{C}[\theta]) = \theta(codom(\mathcal{C})).$$

- If $\mathcal{C}_1$ and $\mathcal{C}_2$ are circuits, and

$$[dom(\mathcal{C}_1) \setminus codom(\mathcal{C}_1)] \cap dom(\mathcal{C}_2) = \emptyset, \tag{9}$$

then the concatenation (or sequential composition) $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2$ of $\mathcal{C}_1$ and $\mathcal{C}_2$ is a also circuit, and

$$dom(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) = dom(\mathcal{C}_1) \cup [dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_1)],$$
$$codom(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) = codom(\mathcal{C}_2) \cup [codom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2)].$$

We shall use $\mathbf{0}_{I,J}$ to denote the action that aborts or a computing device that outputs nothing no matter what the input is. The reason of introducing the notion of inactive circuit is mainly technical. Indeed, it enables us to considerably simplify our presentation (see Proposition 5.2.2 below for example). The function of a primitive action was already explained in the last section. The circuit $\mathcal{C}|\psi\rangle$ deserves a careful explanation. At the first glance, it seems unreasonable to treat $\mathcal{C}|\psi\rangle$ as a circuit because it is a circuit $\mathcal{C}$ plus a quantum state $|\psi\rangle$, which may specify the input to the circuit $\mathcal{C}$ completely, partially, or not at all. However, our design decision is that in $\mathcal{C}|\psi\rangle$, both $\mathcal{C}$ and $|\psi\rangle$ are seen as physical devices. The quantum state $|\psi\rangle$ is a physical resource and it is provided at the beginning. It is not seen as an input to the circuit $\mathcal{C}$ although $\mathcal{C}$ will be applied to it in a computation. The reason is that $|\psi\rangle$ is fixed in $\mathcal{C}|\psi\rangle$, but an arbitrary state can be an input to a circuit provided its domain is consistent with that of the circuit. This point clearly explains the defining equation of $dom(\mathcal{C}|\psi\rangle)$, where the domain of $|\psi\rangle$, which is the set of qubit names included in $|\psi\rangle$, is removed from the domain of the circuit $\mathcal{C}|\psi\rangle$ composed of $\mathcal{C}$ and $|\psi\rangle$. In contrast, $|\psi\rangle$ contributes to the codomain of the circuit $\mathcal{C}|\psi\rangle$. Suppose that in a computational step an input $|\varphi\rangle$ is fed into the circuit $\mathcal{C}|\psi\rangle$. Then the circuit $\mathcal{C}$ is applied to both $|\varphi\rangle$ and the part of $|\psi\rangle$ in $\mathcal{H}_2^{\otimes dom(\mathcal{C})}$ and produces an output, say, $|\varphi'\rangle$ whose domain is equal to $codom(\mathcal{C})$. However, the part of $|\psi\rangle$ not in $\mathcal{H}_2^{\otimes dom(\mathcal{C})}$, written $|\psi'\rangle$, is left unchanged and can be used in the later computational steps. So, it is reasonable to conceive that the output of the whole circuit $\mathcal{C}|\psi\rangle$ is $|\varphi'\rangle$ together with $|\psi'\rangle$, and $dom(|\psi\rangle) \setminus dom(\mathcal{C})$ should be collected in the codomain of $\mathcal{C}|\psi\rangle$. This can be illustrated even more clearly by Fig. 1. Obviously, $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2$ is the concatenation (or sequential composition) of $\mathcal{C}_1$ and $\mathcal{C}_2$. The reason for choosing the notation "$\Rrightarrow$" is that in $C_1 \Rrightarrow C_2$, the direction of the arrow indicates the time flow from C_1 to C_2, and the three bars means that there are some wires connecting C_1 and C_2. It should be noted that we do not require $codom(\mathcal{C}_1) \subseteq dom(\mathcal{C}_2)$. Indeed, it is even allowed that $codom(\mathcal{C}_1) \cap dom(\mathcal{C}_2) = \emptyset$. This is exactly the reason that circuits can be used to describe not only centralized quantum computing but also distributed quantum computing. It also provides us with the mechanism of introducing new qubits. The condition given in Eq. (9) indicates that if a qubit name is consumed in a computational step, i.e. a quantum measurement is performed on it, then it cannot be used in the later steps. This seems a serious objection, but it can be easily remedied by renaming.

For simplicity, we often drop the subscripts I, J of $\mathbf{0}_{I,J}$ when they may be determined by the context or they are irrelevant. It should be pointed out that $dom(|\psi\rangle)$ in the second clause of the above definition is allowed to be empty. In this case, $|\psi\rangle$ will be dropped in $\mathcal{C}|\psi\rangle$. If $n_1, ..., n_k \in \mathcal{N}$ and $\theta(n) = n$ for all $n \in \mathcal{N} \setminus \{n_1, ..., n_k\}$, then we write:

$$\mathcal{C}[\theta(n_1)/n_1, ..., \theta(n_k)/n_k] \tag{10}$$

for $\mathcal{C}[\theta]$. Also, we shall write $\mathcal{C}[\theta(n)/n : n \in \mathcal{M}]$ for $\mathcal{C}[\theta]$ if $\mathcal{M} \subset \mathcal{N}$ and $\theta(n) = n$ for all $n \in \mathcal{N} \setminus \mathcal{M}$.

The qubit names in the domain and codomain of a circuit can be seen from outside, and they are the ports that the circuit will use to establish connections with its environment. Sometimes, we need to consider all qubit names involved in a circuit, not only those in its domain and codomain. To this end, we introduce the notion of the universe of a circuit.

Definition 4.2: The universe $D(\mathcal{C})$ of circuit $\mathcal{C}$ is recursively defined as follows:

- $D(\mathbf{0}_{I,J}) = I \cup J$;
- $D(M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}]) = I \cup \bigcup_{l=1}^k ran(h_l)$;
- $D(\mathcal{C}|\psi\rangle) = D(\mathcal{C}) \cup dom(|\psi\rangle)$;
- $D(\mathcal{C}[\theta]) = \theta(D(\mathcal{C}))$;
- $D(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) = D(\mathcal{C}_1) \cup D(\mathcal{C}_2)$.

It is obvious that $dom(\mathcal{C}), codom(\mathcal{C}) \subseteq D(\mathcal{C})$. However, it is possible that $dom(\mathcal{C}) \cup codom(\mathcal{C}) \neq D(\mathcal{C})$ because some qubits names in $D(\mathcal{C}) \setminus dom(\mathcal{C}) \cup codom(\mathcal{C})$ may be consumed in $\mathcal{C}$ and they cannot be seen from outside; in particular, some qubits in the $dom(\mathcal{C}') \cap dom(|\psi\rangle)-$system may be destroyed by measurements when $\mathcal{C} = \mathcal{C}'|\psi\rangle$.

Examples of circuits will be presented in Section VI. Now we turn to characterize computational behavior of a circuit. Each circuit $\mathcal{C}$ defines a mapping from ensembles to ensembles. To present a formal definition of such a mapping, we need an auxiliary notation. Assume that I, J are finite subsets of $\mathcal{N}$ and $I \cap J = \emptyset$. If $\mathcal{E}$ is an ensemble in $\mathcal{H}_2^{\otimes I}$ and $\mathcal{F}$ is an ensemble in $\mathcal{H}_2^{\otimes J}$, then their tensor product is defined to be $\mathcal{E} \otimes \mathcal{F} = \{|(pq, |\varphi\rangle|\psi\rangle)\rangle) : (p, |\varphi\rangle) \in \mathcal{E} \text{ and } (q, |\psi\rangle) \in \mathcal{F}|\}$. Obviously, it is an ensemble in $\mathcal{H}_2^{\otimes (I \cup J)}$. In particular, if $\mathcal{E}$ is an ensemble in $\mathcal{H}_2^{\otimes I}$ and $|\psi\rangle$ is a pure state in $\mathcal{H}_2^{\otimes J}$, then we write $\mathcal{E} \otimes |\psi\rangle = \{|(p, |\varphi\rangle|\psi\rangle) : (p, |\varphi\rangle) \in \mathcal{E})|\}$.

Definition 4.3: Let $\mathcal{C}$ be a circuit and $\mathcal{E}$ an ensemble with $dom(\mathcal{C}) \subseteq dom(\mathcal{E})$. Then the computational outcome $\mathcal{C}(\mathcal{E})$ of $\mathcal{C}$ on input $\mathcal{E}$ is defined recursively as follows:

- If $\mathcal{C} = \mathbf{0}$, then $\mathcal{C}(\mathcal{E}) \stackrel{def}{=} \emptyset$.

- If $\mathcal{C}$ is a primitive action, then $\mathcal{C}(\mathcal{E})$ is defined by Eq. (8).
- If $\mathcal{C} = \mathcal{C}'|\psi\rangle$, then $\mathcal{C}(\mathcal{E}) \stackrel{def}{=} \emptyset$ when $dom(\mathcal{E}) \cap dom(|\psi\rangle) \neq \emptyset$, and $\mathcal{C}(\mathcal{E}) \stackrel{def}{=} \mathcal{C}'(\mathcal{E} \otimes |\psi\rangle)$ when $dom(\mathcal{E}) \cap dom(|\psi\rangle) = \emptyset$.
- If $\mathcal{C} = \mathcal{C}'[\theta]$, then $\mathcal{C}(\mathcal{E}) \stackrel{def}{=} \theta(\mathcal{C}'(\theta^{-1}(\mathcal{E})))$.
- If $\mathcal{C} = \mathcal{C}_1 \Rrightarrow \mathcal{C}_2$, then $\mathcal{C}(\mathcal{E}) \stackrel{def}{=} \mathcal{C}_2(\mathcal{C}_1(\mathcal{E}))$.

The equation $\mathcal{C}(\mathcal{E}) = \mathcal{F}$ will be often visualized by the transition $\mathcal{E} \stackrel{\mathcal{C}}{\rightarrow} \mathcal{F}$. It is worth noting that the domain of an input to a circuit is not necessarily equal to the domain of the circuit, and the former is allowed to be bigger than the latter. One of the reasons for this design decision is that a circuit is often embedded into a bigger system. On the other hand, this design decision allows us to define the effect of two connected circuits $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2$ in a very convenient way. One thing in the above definition deserving an explanation is the first part of the third clause. Clearly, the only reasonable way of defining $(\mathcal{C}'|\psi\rangle)(\mathcal{E})$ is to put $(\mathcal{C}'|\psi\rangle)(\mathcal{E}) = \mathcal{C}'(\mathcal{E} \otimes |\psi\rangle)$. In the case of $dom(\mathcal{E}) \cap dom(|\psi\rangle) \neq \emptyset$, however, a conflict arises in the domains of the existing resource $|\psi\rangle$ and the input $\mathcal{E}$. The tensor product $\mathcal{E} \otimes |\psi\rangle$ is not well-defined, and the computation $\mathcal{C}'|\psi\rangle(\mathcal{E})$ is then blocked.

The next lemma gives some basic properties of computation by a circuit. The first part shows that the computation of a circuit on an ensemble may be simply carried out by the computations on the pure states in the ensemble. The second part implies that the empty computational result of a circuit does not come from the input. Indeed, it is produced by certain inactive components of the circuit. The third part indicates that a circuit cannot generate entanglement with qubits outside its universe, and it also shows that the part of an input not in the universe of a circuit is left unchanged in the computational process described by the circuit.

Lemma 4.1: 1) Let $\mathcal{E} = \{|(p_t, |\psi_t\rangle) : t \in T|\}$. If $\mathcal{C}(|\psi_t\rangle) = \{|(q_{t,s}, |\varphi_{t,s}\rangle) : s \in S_t|\}$ for each $t \in T$, then $\mathcal{C}(\mathcal{E}) = \{|(p_t \cdot q_{t,s}, |\varphi_{t,s}\rangle) : t \in T, s \in S_t|\}$.

2) If $\mathcal{E} \neq \emptyset$ and $\mathcal{C}(\mathcal{E}) = \emptyset$, then $\mathcal{C}(\mathcal{E}') = \emptyset$ for any ensemble $\mathcal{E}'$ with $dom(\mathcal{E}') = dom(\mathcal{E})$.

3) If $dom(\mathcal{E}) \cap dom(\mathcal{F}) = \emptyset$ and $dom(\mathcal{F}) \cap D(\mathcal{C}) = \emptyset$, then $\mathcal{C}(\mathcal{E} \otimes \mathcal{F}) = \mathcal{C}(\mathcal{E}) \otimes \mathcal{F}$.

Proof. It is routine by induction on the length of $\mathcal{C}$. □

The following proposition presents a way to figure out the domain of the output of a circuit from the domain and codomain of the circuit and the domain of the input.

Proposition 4.1: Let $\mathcal{C}$ be a circuit and $\mathcal{E}$ an ensemble. If $\mathcal{C}(\mathcal{E}) \neq \emptyset$, then we have:

$$dom(\mathcal{C}(\mathcal{E})) = codom(\mathcal{C}) \cup [dom(\mathcal{E}) \setminus dom(\mathcal{C})]. \quad (11)$$

Proof. It is quite involved, and we put it into the appendix. □

A potential application of the above proposition would be to give a type system for quantum computing. A type system of a programming language defines the way that the values and expressions are classified into types and the way that those types are manipulated. Type systems have been successfully applied in programming for classical computers, including safety improvement, optimization, documentation and abstraction. Proposition 4.1 can be used to develop a type checking algorithm for distributed quantum computing.

A. Equivalence of Circuits

It is possible that the constructions of two circuits are significantly different but their computational abilities are the same. Two circuits of the same computational ability are defined to be equivalent. We first consider the inputs with a fixed domain.

Definition 4.4: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two circuits, and let I be a finite subset of $\mathcal{N}$ such that $dom(\mathcal{C}_1), dom(\mathcal{C}_2) \subseteq I$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be $I-$equivalent, written $\mathcal{C}_1 =_I \mathcal{C}_2$, if $\mathcal{C}_1(|\psi\rangle) = \mathcal{C}_2(|\psi\rangle)$ for all pure states $|\psi\rangle$ in $\mathcal{H}_2^{\otimes I}$.

The above definition of equivalence was presented based on inputs of pure states. The next lemma shows that it can also be given with inputs of ensembles.

Lemma 4.2: If $\mathcal{C}_1 =_I \mathcal{C}_2$, then $\mathcal{C}_1(\mathcal{E}) = \mathcal{C}_2(\mathcal{E})$ for all ensembles $\mathcal{E}$ with $dom(\mathcal{E}) = I$.

Proof. Immediate from Lemma 4.1. □

A stronger equivalence between circuits is given by the next definition. The difference between it and Definition 4.4 is that in the later the set I of qubit names is fixed, but in the former I is allowed to be any set of qubit names bigger than the domains of the circuits under consideration.

Definition 4.5: Two circuits $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be equivalent, written $\mathcal{C}_1 = \mathcal{C}_2$, if

1) $dom(\mathcal{C}_1) = dom(\mathcal{C}_2)$;
2) $\mathcal{C}_1 =_I \mathcal{C}_2$ for all $I \supseteq dom(\mathcal{C}_1)$.

One may guess that Clause 2 in the above definition can be weakened as $\mathcal{C}_1 =_{dom(\mathcal{C}_1)} \mathcal{C}_2$. But the following trivial example indicates that it is not the case.

Example 4.1: Let $\mathcal{C}_1 = X_1$ and $\mathcal{C}_2 = (X_1 \Rrightarrow M_2)|0\rangle_2$. Then $dom(\mathcal{C}_1) = dom(\mathcal{C}_2) = \{1\}$, and it is easy to see that $\mathcal{C}_1|\psi\rangle_1 = \mathcal{C}_2|\psi\rangle_1$ for all qubits $|\psi\rangle$. However, $\mathcal{C}_1|00\rangle_{12} = (X|0\rangle_1)|0\rangle_2$, $\mathcal{C}_2|00\rangle_{12} = \emptyset$, and thus $\mathcal{C}_1 \neq \mathcal{C}_2$.

B. Entanglement Resources and Classical Communications

We are often concerned with the amount of entanglement resource consumed and the amount of classical communication needed in distributed quantum computing. Their formal definitions can be easily given by induction on the length of a circuit.

Definition 4.6: The entanglement resources $eres(\mathcal{C})$ consumed in $\mathcal{C}$ is a multi-set of quantum states, and it is recursively defined as follows:

- $eres(\mathbf{0}) = \emptyset$;
- $eres(\mathcal{C}) = \emptyset$ if $\mathcal{C}$ is a primitive action;
- $eres(\mathcal{C}|\psi\rangle) = eres(\mathcal{C}) \cup \{||\psi\rangle|\}$;
- $eres(\mathcal{C}[\theta]) = \theta(eres(\mathcal{C}))$;
- $eres(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) = eres(\mathcal{C}_1) \cup eres(\mathcal{C}_2)$.

We use the term ebit to mean a maximally entangled two-qubit state. Thus, we say that the circuit $\mathcal{C}$ uses $\sum_{i=1}^{m} k_i$ ebits if $eres(\mathcal{C}) = \{||\psi_1\rangle, ..., |\psi_m\rangle|\}$, and $|\psi_i\rangle$ is the tensor product of k_i copies of a maximally entangled two-qubit state for all $i \leq m$.

Definition 4.7: The number $cbit(\mathcal{C})$ of classical communication bits in circuit $\mathcal{C}$ is recursively defined as follows:

- $cbit(\mathbf{0}) = 0$;
- $cbit(M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}]) = k \cdot |I|$;
- $cbit(\mathcal{C}|\psi\rangle) = cbit(\mathcal{C})$;
- $cbit(\mathcal{C}[\theta]) = cbit(\mathcal{C})$;
- $cbit(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) = cbit(\mathcal{C}_1) + cbit(\mathcal{C}_2)$.

We often say that $\mathcal{C}$ uses $cbit(\mathcal{C})$ cbits.

C. Partitions of Subsystems

To describe how a distributed quantum computing system is divided into several subsystems, we introduce the following:

Definition 4.8: Let $\mathcal{P} = \{\mathcal{N}_t : t \in T\}$ be a partition of $\mathcal{N}$.

- $\mathbf{0}$ always respects $\mathcal{P}$;

- $M_I^t[U_{1h_1}^{f_1(t)},...,U_{kh_k}^{f_k(t)}]$ respects $\mathcal{P}$ whenever $I \subseteq \mathcal{N}_{t_0}$ for some $t_0 \in T$, and for each $j \leq k$, $ran(h_j) \subseteq \mathcal{N}_{t_j}$ for some $t_j \in T$;
- $\mathcal{C}|\psi\rangle$ respects $\mathcal{P}$ if $\mathcal{C}$ respects $\mathcal{P}$;
- $\mathcal{C}[\theta]$ respects $\mathcal{P}$ if $\mathcal{C}$ respects $\theta^{-1}(\mathcal{P}) = \{\theta^{-1}(\mathcal{N}_t) : t \in T\}$;
- $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2$ respects $\mathcal{P}$ if both $\mathcal{C}_1$ and $\mathcal{C}_2$ respect $\mathcal{P}$.

Let $\mathcal{C}$ be a circuit and $\mathcal{P} = \{\mathcal{N}_t : t \in T\}$ a partial partition of $D(\mathcal{C})$. We often simply say that $\mathcal{C}$ respects $\mathcal{P}$ when $\mathcal{C}$ respects the partition $\mathcal{P} \cup \{\mathcal{N} \setminus D(\mathcal{C})\}$. Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two sets of qubit names. If $\mathcal{C}$ respects $\mathcal{P} = \{\mathcal{N}_t : t \in T\}$, and $\mathcal{M}_i \subseteq \mathcal{N}_{t_i}$ $(i = 1, 2)$ for different $t_1, t_2 \in T$, then we say that $\mathcal{C}$ separates $\mathcal{M}_1$ from $\mathcal{M}_2$.

We see from the above definition that in distributed quantum computation both quantum measurements and unitary transformations can only be performed on local subsystems. Classical information extracted by a measurement on one subsystem can be passed to other subsystems. Also, entanglement resources are allowed to reside between different subsystems, and thus to connect them. In other words, many subsystems can share a single quantum resource in a distributed system.

When two circuits $\mathcal{C}_1$ and $\mathcal{C}_2$ are considered as distributed computing systems, the equivalence $\mathcal{C}_1 =_I \mathcal{C}_2$ introduced in Definition 4.4 is no longer suitable because in a distributed system it is reasonable to require that the inputs of the subsystems participating the computation are independent to each other, but the state $|\psi\rangle$ in Definition 4.4 is the input of the whole system and it may be entangled with respect to these subsystems. So, we introduce the following:

Definition 4.9: Let $\mathcal{C}_1$, $\mathcal{C}_1$ and I be as in Definition 4.4, and let $\mathcal{P}$ be a partial partition of $\mathcal{N}$. Suppose that both $\mathcal{C}_1$ and $\mathcal{C}_2$ respect $\mathcal{P}$, and $\{I \cap N_t : t \in T \text{ and } I \cap N_t \neq \emptyset\} = \{I_1, ..., I_m\}$. If for any $|\psi_i\rangle \in \mathcal{H}_2^{\otimes I_i}$ $(i = 1, ..., m)$, $\mathcal{C}_1(\bigotimes_{i=1}^m |\psi_i\rangle) = \mathcal{C}_2(\bigotimes_{i=1}^m |\psi_i\rangle)$, then $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be $(\mathcal{P}, I)-$equivalent, and we write $\mathcal{C}_1 =_{\mathcal{P},I} \mathcal{C}_2$.

Let $\mathcal{P} = \{\mathcal{N}_t : t \in T\}$ and $\mathcal{P}' = \{\mathcal{N}'_{t'} : t' \in T'\}$ be two partial partitions of $\mathcal{N}$. Obviously, if $\mathcal{P}$ is a refinement of $\mathcal{P}'$ with respect to I; that is, for each $t \in T$, there exists $t' \in T'$ such that $\mathcal{N}_t \cap I \subseteq \mathcal{N}'_{t'} \cap I$, then $\mathcal{C}_1 =_{\mathcal{P}',I} \mathcal{C}_2$ implies $\mathcal{C}_1 =_{\mathcal{P},I} \mathcal{C}_2$. In particular, $\mathcal{C}_1 =_I \mathcal{C}_2$ implies $\mathcal{C}_1 =_{\mathcal{P},I} \mathcal{C}_2$ for all $\mathcal{P}$. Conversely, $\mathcal{C}_1 =_{\mathcal{P},I} \mathcal{C}_2$ is equivalent to $\mathcal{C}_1 =_I \mathcal{C}_2$ when $I \subseteq \mathcal{N}_t$ for some $t \in T$, but it is not the case in general. It is interesting to note that $\mathcal{C}_1 =_I \mathcal{C}_2$ and $\mathcal{C}_1 =_{\mathcal{P},I} \mathcal{C}_2$ always coincide in the setting of classical computing where entanglement does not exist. So, the difference between the two equivalences is an important fact that distinguishes quantum computing from classical computing. However, such a difference has been treated carelessly in some physical literature; for example, a quantum circuit was presented in Figure 1 of [7] to show that one bit of classical communication in each direction and one shared ebit is necessary and sufficient for the non-local implementation of a $CNOT$ gate ([7], Theorem 1). We write NLC for this circuit and put $I = \{A, B\}$ and $\mathcal{P} = \{\{A\}, \{B\}\}$. In the sufficiency part of the proof of Theorem 1 in [7], it was asserted that $NLC =_I CNOT[1/A, 2/B]$, but in fact only a weaker conclusion, $NLC =_{\mathcal{P},I} CNOT[1/A, 2/B]$, was verified. A formal language such as the one proposed in the current paper may help us to avoid such a careless reasoning.

V. Basic Algebraic Laws for Circuits

The basic properties of circuits are collected in the following two propositions. We first need to introduce an auxiliary notation. Let $U \in \mathcal{G}$ with $ar(U) = n$, and let σ be a permutation of $0, 1, ..., n-1$, i.e. a bijection from $n = \{0, 1, ..., n-1\}$ onto itself. If $U = \bigotimes_{k=0}^{n-1} U_k$, where each U_k is a single-qubit gate acting on the kth qubit, then $\sigma(U) \stackrel{def}{=} \bigotimes_{k=0}^{n-1} U_{\sigma(k)}$. More precisely,

$$\sigma(U) \bigotimes_{k=0}^{n-1} |b_k\rangle \stackrel{def}{=} \bigotimes_{k=0}^{n-1} (U_{\sigma(k)}|b_k\rangle)_k$$

for any $b_k \in \{0, 1\}$, $k = 0, 1, ..., n-1$. By linearity the above defining equation can be easily extended to the general case represented by Eq. (1).

The next proposition gives some basic properties of a primitive action or two connected primitive actions.

Proposition 5.1: 1) Two sequential unitary transformations can be combined: $U_h \Rrightarrow V_h = (VU)_h$.

2) Two independent unitary transformations can be merged: if $ran(h) \cap ran(g) = \emptyset$, then $U_h \Rrightarrow V_g = (U \otimes V)_{h \oplus g}$, where

$$(h \oplus g)(k) = \begin{cases} h(k) \text{ if } k \leq ar(U) - 1, \\ g(k - ar(U)) \text{ if } \begin{array}{l} ar(U) \leq k \leq \\ ar(U) + ar(V) - 1. \end{array} \end{cases}$$

In this case, U_h and V_g commutes, i.e. $U_h \Rrightarrow V_g = V_g \Rrightarrow U_h$, up to a renaming of qubits.

3) Changing operands of unitary transformations in primitive actions:

$$\begin{aligned} &M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}] \\ &= M_I^t[(g_1 \circ h_1^{-1})(U_1)_{g_1}^{f_1(t)}, ..., (g_k \circ h_k^{-1})(U_k)_{g_k}^{f_k(t)}]. \end{aligned}$$

4) Commutativity of independent unitary transformations in primitive actions: if $l \leq k-1$ and $ran(h_l) \cap ran(h_{l+1}) = \emptyset$, then

$$\begin{aligned} &M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{lh_l}^{f_l(t)}, U_{(l+1)h_{l+1}}^{f_{l+1}(t)}, ..., U_{kh_k}^{f_k(t)}] \\ &= M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{(l+1)h_{l+1}}^{f_{l+1}(t)}, U_{lh_l}^{f_l(t)}, ..., U_{kh_k}^{f_k(t)}]. \end{aligned}$$

5) Two independent sequential measurements can be combined: if $I \cap J = I \cap ran(g_n) = ran(h_l) \cap J = \emptyset$ for all $l \leq k$ and $n \leq m$, then

$$\begin{aligned} &M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}] \Rrightarrow M_J^u[V_{1d_1}^{g_1(u)}, ..., V_{md_m}^{g_m(u)}] \\ &= M_{I \cup J}^v[U_{1h_1}^{f_1(v|I)}, ..., U_{kh_k}^{f_k(v|I)}, V_{1d_1}^{g_1(v|J)}, ..., V_{md_m}^{g_n(v|J)}]. \end{aligned}$$

6) Renaming in primitive actions:

$$\begin{aligned} &M_I^t[U_{1h_1}^{f_1(t)}, ..., U_{kh_k}^{f_k(t)}][\theta] \\ &\qquad = M_{\theta(I)}^t[U_{1(h_1 \circ \theta)}^{f_1(t)}, ..., U_{k(h_k \circ \theta)}^{f_k(t)}]. \end{aligned}$$

Proof. See the appendix. □

The following proposition presents some structural properties of circuits.

Proposition 5.2: 1) Inactive law: $\mathbf{0}|\psi\rangle = \mathbf{0}$, $\mathbf{0}[\theta] = \mathbf{0}$, $\mathbf{0} \Rrightarrow \mathcal{C} = \mathbf{0}$, and $\mathcal{C} \Rrightarrow \mathbf{0} = \mathbf{0}$. Here the notation is overloading. To simplify the presentation, we ignore the domain and codomain of $\mathbf{0}$ which may be different in these four equalities.

2) Putting resources together: if $dom(|\psi_1\rangle) \cap dom(|\psi_2\rangle) \neq \emptyset$ then $(\mathcal{C}|\psi_1\rangle)|\psi_2\rangle = \mathbf{0}$, and if $dom(|\psi_1\rangle) \cap dom(|\psi_2\rangle) = \emptyset$ then $(\mathcal{C}|\psi_1\rangle)|\psi_2\rangle = \mathcal{C}(|\psi_1\rangle \otimes |\psi_2\rangle)$.

3) Renaming laws:

a) $\mathcal{C}[id_{\mathcal{N}}] = \mathcal{C}$, where $id_{\mathcal{N}}$ is the identity mapping from $\mathcal{N}$ onto itself.

b) $\mathcal{C}[\theta] = \mathcal{C}[\theta']$ if $\theta(dom(\mathcal{C})) = \theta'(dom(\mathcal{C}))$, $\theta(codom(\mathcal{C})) = \theta'(codom(\mathcal{C}))$, and θ and θ' coincide in $\theta(dom(\mathcal{C})) \setminus \theta(codom(\mathcal{C}))$.
c) $\mathcal{C}[\theta][\theta'] = \mathcal{C}[\theta \circ \theta']$.

4) Commutativity for independent circuits: if $D(\mathcal{C}_1) \cap D(\mathcal{C}_2) = \emptyset$, then we have $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2 = \mathcal{C}_2 \Rrightarrow \mathcal{C}_1$.
5) Associativity: $(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) \Rrightarrow \mathcal{C}_3 = \mathcal{C}_1 \Rrightarrow (\mathcal{C}_2 \Rrightarrow \mathcal{C}_3)$.
6) Distributivity of renaming over concatenation: $(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)[\theta] = \mathcal{C}_1[\theta] \Rrightarrow \mathcal{C}_2[\theta]$.
7) Distributivity of renaming over resource: $\mathcal{C}|\psi\rangle[\theta] = \mathcal{C}[\theta]\theta(|\psi\rangle)$, and $\mathcal{C}[\theta]|\psi\rangle = \mathcal{C}\theta^{-1}(|\psi\rangle)[\theta]$.
8) Moving resource through concatenation: $(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)|\psi\rangle = \mathcal{C}_1|\psi\rangle \Rrightarrow \mathcal{C}_2$, and if $D(\mathcal{C}_1) \cap dom(|\psi\rangle) = \emptyset$ then $(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)|\psi\rangle = \mathcal{C}_1 \Rrightarrow \mathcal{C}_2|\psi\rangle$.
9) Congruence laws: if $\mathcal{C}_1 = \mathcal{C}_2$, then we have:
   a) $\mathcal{C}_1|\psi\rangle = \mathcal{C}_2|\psi\rangle$;
   b) $\mathcal{C}_1[\theta] = \mathcal{C}_2[\theta]$; and
   c) $\mathcal{C}_1 \Rrightarrow \mathcal{C} = \mathcal{C}_2 \Rrightarrow \mathcal{C}$ and $\mathcal{C} \Rrightarrow \mathcal{C}_1 = \mathcal{C} \Rrightarrow \mathcal{C}_2$.

Proof. See the appendix. □

The first part of Clause 2) in the above proposition looks a little bit strange. At the first glance, one may wonder why should the effect of a circuit in which two subsystems share some qubits be a null program; in particular, it is common in a quantum circuit that two subsystems are entangled through some middle qubits. In fact, here the condition of $dom(|\psi_1\rangle) \cap dom(|\psi_2\rangle) \neq \emptyset$ means that there is a conflict of qubit names in circuit $(\mathcal{C}|\psi_1\rangle)|\psi_2\rangle$ (see the paragraphs after Definitions 4.1 and 4.3), and we want to express the idea that conflicts of qubit names would create illegal circuits. An alternative way to do this is to exclude such a case in the step of defining quantum circuits by adding the condition of $dom(\mathcal{C}) \cap dom(|\psi\rangle) = \emptyset$ in the third clause of Definition 4.1. However, it would make the presentation much more complicated; e.g. the induction proof of Proposition 4.1.

The Clause 5 of Proposition 5.2 asserts that the sequential composition $\Rrightarrow$ enjoys associativity. So, we can write $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2 \Rrightarrow ... \Rrightarrow \mathcal{C}_n$ without ambiguity. Furthermore, we shall write $\prod_{i=1}^{n} \mathcal{C}_i$ as an abbreviation of $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2 \Rrightarrow ... \Rrightarrow \mathcal{C}_n$.

A. Normal Forms

We now introduce a normal form of circuit in which all resources are put at the beginnings of primitive actions.

Definition 5.1: A normal form of circuit is defined to be a circuit of the form $A_1|\psi_1\rangle \Rrightarrow A_2|\psi_2\rangle \Rrightarrow ... \Rrightarrow A_n|\psi_n\rangle$, where all A_i are primitive actions.

Let Φ_1 and Φ_2 be two finite multi-sets of quantum states. Then Φ_2 is called a simple variant of Φ_1, written $\Phi_1 \approx \Phi_2$, if Φ_2 can be obtained from Φ_1 by a finite number of applications of the following manipulation:

- Take a finite number of elements $\{||\varphi_i\rangle|\}$ from Φ_1 with $dom(|\varphi_{i_1}\rangle) \cap dom(|\varphi_{i_2}\rangle) = \emptyset$ for any different i_1 and i_2, and replace them by their tensor product $\bigotimes_i |\varphi_i\rangle$.

Transforming a quantum circuit to its normal form can help us to recognize more clearly the role of physical resources in distributed quantum computing. The following propositions warrants the existence of normal form of each circuit.

Proposition 5.3: (Normal Form) For any circuit $\mathcal{C}$, if $\mathcal{C} \neq \mathbf{0}$, then there exists a normal form $\mathcal{C}'$ such that

1) $\mathcal{C} = \mathcal{C}'$;
2) $cbit(\mathcal{C}) = cbit(\mathcal{C}')$;
3) $eres(\mathcal{C}) \approx eres(\mathcal{C}')$; and
4) for any partition $\mathcal{P}$, $\mathcal{C}$ respects $\mathcal{P}$ if and only if $\mathcal{C}'$ respects $\mathcal{P}$.

Proof. With Proposition 5.2, it is routine by induction on the length of $\mathcal{C}$. □

VI. Illustrative Examples

In this section, we present some examples to show how the formal language designed in this paper and the algebraic laws given in the last section can be used in describing and reasoning about distributed quantum systems. Due to the limit of space, we only consider some variants and generalizations of quantum teleportation, one of the most famous quantum protocols.

A. Quantum Teleportation

Suppose that Alice and Bob generated a maximally entangled two qubit state $|E\rangle$, each taking one qubit of it. Alice is asked to send a qubit to Bob. She does not know the state of the qubit and can only send classical information to Bob.

A solution to the above problem, called quantum teleportation, was discovered by Bennet, Brassard, Crépeau, Jozsa, Peres and Wootters [1]. Now quantum teleportation is widely used as a basic component of various quantum communication protocols. In the previous literature, quantum teleportation was often presented as a circuit graph due to lack of suitable algebraic language. However, using the language defined in the previous sections, quantum teleprtation may be simply expressed by the following algebraic equation:

$$TEL = CNOT_{1,2}|E\rangle_{2,3} \Rrightarrow H_1 \Rrightarrow M_2^t[X_3^t] \Rrightarrow M_1^u[Z_3^u].$$

Proposition 6.1: The circuit TEL can teleport a qubit in any environment, even if the qubit is entangled with the environment. Formally, if $k \geq 3$ then for any $|\psi\rangle \in \mathcal{H}_2^{\otimes(k-2)}$ we have $TEL|\psi\rangle_{1,4,...,k} = |\psi\rangle_{3,...,k}$, and TEL separates qubit names 3 from $1, 2$ and it uses 2 cbits and 1 ebit.

Proof. We can write $|\psi\rangle_{1,4,...,k} = \alpha|0\rangle_1|\psi_0\rangle_{4,...,k} + \beta|1\rangle_1|\psi_1\rangle_{4,...,k}$. For simplicity, the subscripts $4, ..., k$ will be dropped in $|\psi_i\rangle_{4,...,k}$ for $i = 0, 1$. Then the performance of TEL is shown as follows:

$$\begin{aligned}
&|E\rangle_{2,3}|\psi\rangle_{1,4,...k} = \frac{1}{\sqrt{2}}(\alpha|0\rangle_1|\psi_0\rangle + \beta|1\rangle_1|\psi_1\rangle)(|00\rangle + |11\rangle)_{2,3} \\
&\overset{CNOT_{1,2}}{\to} \frac{1}{\sqrt{2}}[\alpha|0\rangle_1(|00\rangle + |11\rangle)_{2,3}|\psi_0\rangle + \\
&\qquad\qquad \beta|1\rangle_1(|10\rangle + |01\rangle)_{2,3}|\psi_1\rangle] \\
&\overset{H_1}{\to} \frac{1}{2}[\alpha(|0\rangle + |1\rangle)_1(|00\rangle + |11\rangle)_{2,3}|\psi_0\rangle + \\
&\qquad\qquad \beta(|0\rangle - |1\rangle)_1(|10\rangle + |01\rangle)_{2,3}|\psi_1\rangle] \\
&\overset{M_2^t[X_3^t]}{\to} \frac{1}{\sqrt{2}}[\alpha(|0\rangle + |1\rangle)_1|0\rangle_3|\psi_0\rangle + \beta(|0\rangle - |1\rangle)_1|1\rangle_3|\psi_1\rangle] \\
&\overset{M_1^u[Z_3^u]}{\to} \alpha|0\rangle_3|\psi_0\rangle + \beta|1\rangle_3|\psi_1\rangle = |\psi\rangle_{3,...,k} = TEL|\psi\rangle_{1,4,...,k}.
\end{aligned}$$

□

We now consider a decomposition of TEL suggested by Yimsiriwattana and Lomonaco [25]. This decomposition is given in terms of a cat-like generator and a disentangler. The cat-like generator is constructed by a CNOT gate, local operations (i.e. one measurement and $X-$gates) and classical communication:

$$CAT_{m+1} = CNOT_{1,2}|E_m\rangle_{2,...,m+1} \Rrightarrow M_2^t[X_3^t, ..., X_{m+1}^t].$$

Give a qubit $|\psi\rangle = \alpha|0\rangle + \beta|0\rangle$ and an $m-$qubit cat (GHZ) state $|E_m\rangle$. Then a cat-like state $|\psi_m\rangle = \alpha|0\rangle^{\otimes m} + \beta|1\rangle^{\otimes m}$ can be generated as follows:

$$\begin{aligned}
&|\psi\rangle_1|E_m\rangle_{2,\ldots,m+1} = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|0\rangle^{\otimes m} + |1\rangle^{\otimes m}) \\
&\overset{CNOT_{1,2}}{\rightarrow} \frac{1}{\sqrt{2}}[\alpha|0\rangle(|0\rangle^{\otimes m} + |1\rangle^{\otimes m}) + \\
&\qquad \beta|1\rangle(|1\rangle|0\rangle^{\otimes(m-1)} + |0\rangle|1\rangle^{\otimes(m-1)})] \\
&\overset{M_2^t[X_3^t,\ldots,X_{m+1}^t]}{\rightarrow} (\alpha|0\rangle^{\otimes m} + \beta|1\rangle^{\otimes m})_{1,3,\ldots,m+1} \\
&= CAT_{m+1}|\psi\rangle_1.
\end{aligned} \tag{12}$$

We construct the disentangler as follows:

$$DIS_m = \prod_{i=2}^{m} H_i \Rrightarrow M_{2,3,\ldots,m}^t[Z_1^{f(t)}],$$

where $f(t) = \sum_{i=2}^{m} t(i)$ for each $t \in 2^{\{2,3,\ldots,m\}}$. Then a cat-like state $|\psi_m\rangle$ can be transformed by DIS_m into states $|\psi\rangle$:

$$\begin{aligned}
&|\psi_m\rangle_{1,\ldots,m} \overset{H_2}{\rightarrow}\overset{H_3}{\rightarrow} \ldots \overset{H_m}{\rightarrow} \\
&\qquad \frac{1}{2^{\frac{m-1}{2}}}[\alpha|0\rangle(|0\rangle + |1\rangle)^{\otimes(m-1)} + \beta|1\rangle(|0\rangle - |1\rangle)^{\otimes(m-1)}] \\
&= \frac{1}{2^{\frac{m-1}{2}}} \sum_{t=0}^{2^{m-1}-1} (\alpha|0\rangle + (-1)^{f(t)}\beta|1\rangle)|t\rangle \\
&\overset{M_{2,3,\ldots,m}^t[Z_1^{f(t)}]}{\rightarrow} |\psi\rangle_1 = DIS_m|\psi_m\rangle_{1,\ldots,m}.
\end{aligned} \tag{13}$$

Yimsiriwattana and Lomonaco's decomposition of TEL may be conveniently described in the language presented in this paper, and its correctness can be proved through a series of simple algebraic manipulations by employing several algebraic laws given in the last section.

Proposition 6.2: The teleportation circuit is the composition of a cat-like generator and a (renamed) disentangler: $TEL = CAT_3 \Rrightarrow DIS_2[1/2, 3/1]$, where $[1/2, 3/1]$ means that the qubit names $2, 1$ are substituted by $1, 3$ respectively, and the other qubit names are left unchanged (see the notation convention for renaming, Eq. (10)).

Proof. This can be done by combining Eqs. (12) and (13) directly. As a simpler proof, we have:

$$\begin{aligned}
&CAT_3 \Rrightarrow DIS_2[1/2, 3/1] = \\
&\quad CAT_3 \Rrightarrow H_2[1/2, 3/1] \Rrightarrow M_2^t[Z_1^t][1/2, 3/1] \quad \text{(Prop. 5.2.6)} \\
&= CAT_3 \Rrightarrow H_1 \Rrightarrow M_1^t[Z_3^t] \quad \text{(Prop. 5.1.6)} \\
&= CNOT_{1,2} \Rrightarrow M_2^t[X_3^t] \Rrightarrow H_1 \Rrightarrow M_1^t[Z_3^t] \\
&= CNOT_{1,2} \Rrightarrow H_1 \Rrightarrow M_2^t[X_3^t] \Rrightarrow M_1^t[Z_3^t] \quad \text{(Prop. 5.2.6)} \\
&= TEL. \ \square
\end{aligned}$$

B. Remote Implementation of Quantum Circuits

A straightforward application of teleportation gives a remote implementation of a quantum circuit. In this subsection, we use symbols P, Q, R, S, T with or without subscripts to denote qubit names.

The following proposition shows that two qubits in a circuit can be moved to two locations far from each other by using teleportation.

Proposition 6.3: Let $\mathcal{C}$ be a circuit with $R \in dom(\mathcal{C})$, $R \in codom(\mathcal{C})$, and $P \notin D(\mathcal{C})$. Then we have:

$$\begin{aligned}
\mathcal{C}[P/R] &= TEL[P/1, Q_1/2, R/3] \\
&\Rrightarrow \mathcal{C} \Rrightarrow TEL[R/1, Q_2/2, P/3].
\end{aligned}$$

The right-hand side circuit uses 2 ebits and 4 cbits, and it separates P from qubit names in $D(\mathcal{C}) \setminus \{R\}$ but the left-hand side does not.

Proof. We write LHS and RHS for the left-hand and right-hand side circuits, respectively. A routine calculation shows that $dom(LHS) = dom(RHS)$ and $codom(LHS) = codom(RHS)$. Furthermore, for any $T_1, \ldots, T_k$ with $dom(\mathcal{C}) \subseteq \{R, T_1, \ldots, T_k\}$, and for any $|\psi\rangle \in \mathcal{H}_2^{\otimes(k+1)}$, assume that $\mathcal{C}(|\psi\rangle_{R,T_1,\ldots,T_k}) = |\varphi\rangle_{R,S_1,\ldots,S_l}$. Then using Proposition 6.1 we have:

$$\begin{aligned}
&|\psi\rangle_{P,T_1,\ldots,T_k} \overset{TEL[P/1,Q_1/2,R/3]}{\rightarrow} |\psi\rangle_{R,T_1,\ldots,T_k} \overset{\mathcal{C}}{\rightarrow} |\varphi\rangle_{R,S_1,\ldots,S_l} \\
&\overset{TEL[R/1,Q_2/2,P/3]}{\rightarrow} |\varphi\rangle_{P,S_1,\ldots,S_l} = RHS(|\psi\rangle_{P,T_1,\ldots,T_k}).
\end{aligned}$$

On the other hand, it follows that

$$\begin{aligned}
&LHS(|\psi\rangle_{P,T_1,\ldots,T_k}) = [P/R](\mathcal{C}(|\psi\rangle_{R,T_1,\ldots,T_k})) \\
&= [P/R](|\varphi\rangle_{R,S_1,\ldots,S_l}) = |\varphi\rangle_{P,S_1,\ldots,S_l}. \ \square
\end{aligned}$$

Obviously, repeated applications of the above proposition can help us to separate more qubits in a circuit from each other.

We now turn to show that two steps in quantum computing can be implemented separately in two locations far from each other by using teleportation.

Proposition 6.4: Let $\mathcal{P}, \mathcal{P}_0 \subseteq \mathcal{N}$, and let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two circuits with $codom(\mathcal{C}_1) \cap dom(\mathcal{C}_2) = \mathcal{P}$ and $codom(\mathcal{C}_2) \cap \mathcal{P} = \mathcal{P}_0$. Then we have:

$$\begin{aligned}
\mathcal{C}_1 \Rrightarrow \mathcal{C}_2 = \mathcal{C}_1 &\Rrightarrow \prod_{P \in \mathcal{P}} TEL[P/1, P'/2, P''/3] \\
&\Rrightarrow \mathcal{C}_2[P''/P : P \in \mathcal{P}] \\
&\Rrightarrow \prod_{P \in \mathcal{P}_0} TEL[P''/1, P'''/2, P/3], \text{ and}
\end{aligned}$$

1) The right-hand side circuit respects the partition $\{\mathcal{P}' \cup dom(\mathcal{C}_1) \cup codom(\mathcal{C}_1) \setminus \mathcal{P}, \mathcal{P}'' \cup \mathcal{P}''' \cup dom(\mathcal{C}_2) \cup codom(\mathcal{C}_2) \setminus \mathcal{P}\}$, where $\mathcal{P}' = \{P' : P \in \mathcal{P}\}$, and $\mathcal{P}'', \mathcal{P}'''$ are defined similarly.
2) The right-hand side uses $|\mathcal{P}| + |\mathcal{P}_0|$ ebits and $2(|\mathcal{P}| + |\mathcal{P}_0|)$ cbits, where $|\mathcal{Q}|$ stands for the number of elements in $\mathcal{Q}$.

Proof. The idea is similar to the proof of Proposition 6.3, but the details are much more complicated. We omit the complicated but routine details here. $\square$

van Meter, Munro, Nemoto and Itoh [21] distinguished two schemes of applications of teleportation in distributed quantum computing. When two qubits in different nodes are required to interact, we have the following two choices: (1) *teledata* - moving data (qubits) from node to the other, and then performing the shared gates; (2) *telegate* - using a teleported gate [11] directly on the qubits, without moving them. Indeed, the above two propositions give a (partial) formal description of teledata and a verification of its correctness. In the next section, a special case of telegate will be formally described in the algebraic language introduced in the present paper.

C. Remotely Controlled Gates

A distributed implementation of a controlled gate was proposed by Eisert, Jacobs, Papadopoulos and Plenio [7] and Collins,

Linden and Popescu [4]. Their main results can be recast in a precise and convenient way by employing the formal language for distributed quantum computing developed in this paper. Let us consider controlled gate $C^{(n)}(U)$, where $ar(U) = k$, and let $\mathcal{N} = \{P_1, Q_1, ..., P_n, Q_n, T_1, ..., T_{n+k}\}$. Suppose that there are n agents, and the ith agent posseses two qubits P_i and Q_i for each $i \leq n$. These agents are far from each other, but they are going to work together to implement a remote control of $C^{(n)}(U)$. For every $i \leq n$, the ith agent will use the P_i qubit as his control qubit, and furthermore we assume that Q_i and T_i share a maximally entangled state. Then we have:

Proposition 6.5: A nonlocal $C^{(n)}(U)$ can be implemented by local operations and classical communication between entangled subsystems:

$$\begin{aligned} C^{(n)}(U)_{P_1,...,P_n,T_{n+1},...,T_{n+k}} &= \prod_{i=1}^{n} CAT_3[P_i/1, Q_i/2, T_i/3] \\ \Rrightarrow C^{(n)}(U)_{T_1,...,T_{n+k}} &\Rrightarrow \prod_{i=1}^{n} DIS_2[P_i/1, T_i/2]. \end{aligned} \tag{14}$$

The right-hand side circuit uses $2n$ cbits and n ebits, and it respects the partition $\{\{P_1, Q_1\}, ..., \{P_n, Q_n\}, \{T_1, ..., T_{n+k}\}\}$, but the left-hand side one does not.

A graph representing the quantum circuit in the right-hand side of Eq. (14) must be very big and complicated. Eq. (14) demonstrates once again the advantage of the formal language defined in the present paper.

To prove the above proposition, we first need the following lemma, which can be seen as a component of the above proposition.

Lemma 6.1: For any $R_1, ..., R_{n+k}$ and $i \leq n$, we have:

$$\begin{aligned} C^{(n)}(U)_{R_1,...,R_{i-1},P_i,R_{i+1},...,R_{n+k}} &= CAT_3[P_i/1, Q_i/2, R_i/3] \\ \Rrightarrow C^{(n)}(U)_{R_1,...,R_{n+k}} &\Rrightarrow DIS_2[P_i/1, R_i/2]. \end{aligned}$$

Proof. We observe that $CAT_3|j\rangle_1 = |j\rangle_1|j\rangle_3$ for $j = 0, 1$. Then for any $j_1, ..., j_n \in \{0, 1\}$ and $|\psi\rangle \in \mathcal{H}_2^{\otimes\{T_{n+1},...,T_{n+k}\}}$, we have

$$\begin{aligned} |j_1...j_n\rangle_{P_1...P_n}|\psi\rangle &\xrightarrow{\prod_{i=1}^{n} CAT_3[P_i/1,Q_i/2,T_i/3]} \bigotimes_{i=1}^{n} |j_i j_i\rangle_{P_i T_i}|\psi\rangle \\ &\xrightarrow{C^{(n)}(U)_{T_1,...,T_{n+k}}} \bigotimes_{i=1}^{n} |j_i j_i\rangle_{P_i T_i} U^{j_1...j_n}|\psi\rangle \\ &\xrightarrow{\prod_{i=1}^{n} DIS_2[P_i/1,T_i/2]} \bigotimes_{i=1}^{n} |j_i\rangle_{P_i} U^{j_1...j_n}|\psi\rangle \end{aligned}$$

because $DIS_2|j\rangle_1|j\rangle_2 = |j\rangle_1$ for $j = 0, 1$. □

Proof of Proposition 6.5. By Propositions 5.2.2, 5.2.6, 5.2.10 and 5.2.11 and 6.1, we obtain:

$$\begin{aligned} RHS &= \prod_{i=2}^{n} CAT_3[P_i/1, Q_i/2, T_i/3] \\ &\quad \Rrightarrow (CAT_3[P_1/1, Q_1/2, R_1/3] \\ &\quad \Rrightarrow C^{(n)}(U)_{R_1,...,R_{n+k}} \Rrightarrow DIS_2[P_1/1, R_1/2]) \\ &\quad \Rrightarrow \prod_{i=2}^{n} DIS_2[P_i/1, T_i/2] \\ &= \prod_{i=2}^{n} CAT_3[P_i/1, Q_i/2, T_i/3] \\ &\quad \Rrightarrow C^{(n)}(U)_{P_1,R_2,...,R_{n+k}} \Rrightarrow \prod_{i=2}^{n} DIS_2[P_i/1, T_i/2]. \end{aligned}$$

Therefore, repeating the above process n times, we complete the proof. □

VII. Conclusion

To provide formal methods for specifying and verifying distributed quantum systems, we design an algebraic language in which unitary transformations and quantum measurements as well as classical communications and use of quantum resources can be expressed in a convenient and compact way. Several examples are presented to illustrate the expressive power of this language, and some basic algebraic laws are established for distributed quantum computing. One unsolved fundamental problem is to prove the following:

Conjecture 7.1: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two circuits, and let I and J be two finite subsets of $\mathcal{N}$ such that $dom(\mathcal{C}_1), dom(\mathcal{C}_2) \subseteq I$ and $J \cap dom(\mathcal{C}_1) = J \cap dom(\mathcal{C}_2) = \emptyset$. Then $\mathcal{C}_1 =_I \mathcal{C}_2$ implies $\mathcal{C}_1 =_{I \cup J} \mathcal{C}_2$.

The intuitive meaning of the above conjecture is that if two circuits are equivalent in a smaller environment then their equivalence will be preserved when they are put into a bigger environment.

This paper is merely the first step of a long-term project of algebraic studies of quantum circuits for distributed quantum computing. It is worth noting that the algebraic laws given in the current paper are all structural laws which do not depend on special properties of the involved unitary operators and quantum measurements. As the next step, we shall choose a universal (or approximately universal) class of unitary operators and systematically examine algebraic properties of quantum circuits generated by the chosen unitary operators. In particular, we hope to isolate some fundamental laws (axioms) which are adequate for equational reasoning about these circuits. The difference between these laws and the laws established in this paper is that the former will heavily depend on special properties of the chosen unitary operators.

It should be pointed out that quantum circuit expressions written in the language defined in this paper appear to be quite different from Boolean expressions although their functions are similar. The reason is two-fold. First, Boolean expressions are usually written in terms of three special logical connectives, namely, negation, conjunction and disjunction, whereas in this paper unitary operators are treated in an abstract way. Quantum circuit expressions will become more similar to Boolean expressions whenever we choose to consider only some special

unitary operators; for example one-qubit and two-qubit gates. Second, negation, conjunction and disjunction enjoy some nice operational properties such as the de Morgan law, distributivity of conjunction over disjunction and disjunction over conjunction. These properties enable us to manipulate Boolean expressions effectively; for example Boolean expressions have their conjunctive and disjunctive normal forms. However, as mentioned in the above paragraph, such operational properties are still to be found for quantum circuits.

Distributed quantum computing is an emerging area, and many very interesting topics are still untouched. As was pointed out in the introduction, major work in the area of distributed quantum computing were devoted to the following two topics: (1) finding quantum algorithms for solving problems from classical distributed computing; and (2) using many small capacity quantum computers to simulate a large capacity quantum computer. However, research on both topics are at the very beginning. Teleportation between two parties has been widely used in distributed quantum computing; see Section VI for examples. However, many-partite teleportation have still not been understood well. Recently, Wang and the author [23], [24] generalized the teleportation and super-dense coding protocols to the case of more than two parties. An interesting problem for further studies is to exploit the power of these new protocols in distributed quantum computing. As is well-known, one of the most important applications of quantum computing is the simulation of quantum systems. So, another interesting problem would be to explore the possibility of using distributed quantum computing in simulation of quantum many-body systems. Compared to classical distributed computing, an entirely new topic is to exploit the power of entanglement in distributed quantum computing and to understand further the role of entanglement in computing in general [15], [6].

In recent years, Gay and Nagarajan [9], [10], Jorrand and Lalire [13], [14], [16], [17] and Feng, Duan, Ji and the author [8], [27] proposed process algebra approaches to distributed and concurrent quantum computing. The main purpose of these works is quite different from that of this paper, and they mainly aimed to provide formal models for verifying quantum communication protocols. The relationship between quantum process algebras and the language defined in this paper is similar to that between classical process algebras and Boolean algebra. Roughly speaking, the former is suited to high-level formal specification of distributed quantum computing, and the later will mainly be used to describe low-level circuit implementation. It is very interesting to further clarify the relationship between the formal models introduced in [9], [10], [13], [14], [16], [17], [8], [27] and the language designed in this paper.

APPENDIX I
PROOF OF PROPOSITION 4.1

We proceed by induction on the length of $\mathcal{C}$. The trick is to simultaneously prove our conclusion and the following:

- *Claim.* If $\mathcal{C}(\mathcal{E}) \neq \emptyset$, then $dom(\mathcal{E}) \cap codom(\mathcal{C}) \subseteq dom(\mathcal{C})$.

We consider the following cases:

- Case 1. $\mathcal{C} = \mathbf{0}$. Obvious.
- Case 2. $\mathcal{C}$ is a primitive action. The proof for this case is routine.
- Case 3. $\mathcal{C} = \mathcal{C}'|\psi\rangle$. We first prove the above claim. If $\mathcal{C}(\mathcal{E}) \neq \emptyset$, then $dom(\mathcal{E}) \cap dom(|\psi\rangle) = \emptyset$ and $\mathcal{C}(\mathcal{E}) = \mathcal{C}'(\mathcal{E} \otimes |\psi\rangle)$. Thus, for any $n \in \mathcal{N}$, if $n \in dom(\mathcal{E})$ and $n \in codom(\mathcal{C}) = codom(\mathcal{C}') \cup [dom(|\psi\rangle) \setminus dom(\mathcal{C}')]$, then we have $n \notin dom(|\psi\rangle)$. This leads to $n \in codom(\mathcal{C}')$. By the induction hypothesis on $\mathcal{C}'$ we obtain $dom(\mathcal{E} \otimes |\psi\rangle) \cap codom(\mathcal{C}') \subseteq dom(\mathcal{C}')$. Therefore, it holds that $n \in dom(\mathcal{C}')$, and furthermore we have $n \in dom(\mathcal{C}') \setminus dom(|\psi\rangle) = dom(\mathcal{C})$.

  Second, we prove Eq. (11). If $\mathcal{C}(\mathcal{E}) \neq \emptyset$, then $dom(\mathcal{E}) \cap dom(|\psi\rangle) = \emptyset$, and it holds that $dom(\mathcal{E}) \setminus dom(\mathcal{C}) = dom(\mathcal{E}) \setminus (dom(\mathcal{C}') \setminus dom(|\psi\rangle)) = dom(\mathcal{E}) \setminus dom(\mathcal{C}')$, and $codom(\mathcal{C}) \cup [dom(\mathcal{E}) \setminus dom(\mathcal{C})] = codom(\mathcal{C}') \cup (dom(|\psi\rangle) \setminus dom(\mathcal{C}')) \cup (dom(\mathcal{E}) \setminus dom(\mathcal{C}')) = codom(\mathcal{C}') \cup (dom(\mathcal{E}) \cup dom(|\psi\rangle) \setminus dom(\mathcal{C}')) = dom(\mathcal{C}'(\mathcal{E} \otimes |\psi\rangle)) = dom(\mathcal{C}(\mathcal{E}))$.
- Case 4. $\mathcal{C} = \mathcal{C}'[\theta]$. To prove the above claim, assume that $\mathcal{C}(\mathcal{E}) = \theta(\mathcal{C}'(\theta^{-1}(\mathcal{E}))) \neq \emptyset$, then $\mathcal{C}'(\theta^{-1}(\mathcal{E})) \neq \emptyset$, and the induction hypothesis asserts that $dom(\theta^{-1}(\mathcal{E})) \cap codom(\mathcal{C}') \subseteq dom(\mathcal{C}')$. This yields $dom(\mathcal{E}) \cap codom(\mathcal{C}) = \theta\theta^{-1}(dom(\mathcal{E})) \cap \theta(codom(\mathcal{C}')) = \theta(dom(\theta^{-1}(\mathcal{E})) \cap codom(\mathcal{C}')) \subseteq \theta(dom(\mathcal{C}')) = dom(\mathcal{C})$. On the other hand, we have: $dom(\mathcal{C}(\mathcal{E})) = dom(\theta(\mathcal{C}'(\theta^{-1}(\mathcal{E}))) = \theta(dom(\mathcal{C}'(\theta^{-1}(\mathcal{E}))) = \theta(codom(\mathcal{C}') \cup [dom(\theta^{-1}(\mathcal{E})) \setminus dom(\mathcal{C}')]) = \theta(codom(\mathcal{C}')) \cup [\theta\theta^{-1}(dom(\mathcal{E})) \setminus \theta(dom(\mathcal{C}'))] = codom(\mathcal{C}) \cup [dom(\mathcal{E}) \setminus dom(\mathcal{C})]$.
- Case 5. $\mathcal{C} = \mathcal{C}_1 \Rrightarrow \mathcal{C}_2$. Suppose that $\mathcal{C}(\mathcal{E}) = \mathcal{C}_2(\mathcal{C}_1(\mathcal{E})) \neq \emptyset$. Then $\mathcal{C}_1(\mathcal{E}) \neq \emptyset$, and by the induction hypothesis on $\mathcal{C}_1$, we obtain $dom(\mathcal{E}) \cap [codom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2)] \subseteq dom(\mathcal{E}) \cap codom(\mathcal{C}_1) \subseteq dom(\mathcal{C}_1) \subseteq dom(\mathcal{C})$. Thus, it suffices to show that $dom(\mathcal{E}) \cap codom(\mathcal{C}_2) \subseteq dom(\mathcal{C}) = dom(\mathcal{C}_1) \cup [dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_1)]$ since we have: $dom(\mathcal{E}) \cap codom(\mathcal{C}) = dom(\mathcal{E}) \cap [codom(\mathcal{C}_2) \cup (codom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2))] = [dom(\mathcal{E}) \cap codom(\mathcal{C}_2)] \cup [dom(\mathcal{E}) \cap (codom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2))]$. For any $n \in dom(\mathcal{E}) \cap codom(\mathcal{C}_2)$, we are going to show that $n \in dom(\mathcal{C}_1)$ or $n \in dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_1)$. Indeed, if $n \notin dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_1)$, then $n \notin dom(\mathcal{C}_2)$ or $n \in codom(\mathcal{C}_1)$. For the case of $n \in codom(\mathcal{C}_1)$, the induction hypothesis, together with the fact that $\mathcal{C}_1(\mathcal{E}) \neq \emptyset$, implies that $n \in dom(\mathcal{C}_1)$. For the case of $n \notin dom(\mathcal{C}_2)$, since $\mathcal{C}_2(\mathcal{C}_1(\mathcal{E})) \neq \emptyset$, the induction hypothesis on $\mathcal{C}_2$ leads to $dom(\mathcal{C}_1(\mathcal{E})) \cap codom(\mathcal{C}_2) \subseteq dom(\mathcal{C}_2)$. Noting that $n \in codom(\mathcal{C}_2)$, we obtain $n \notin dom(\mathcal{C}_1(\mathcal{E}))$. Furthermore, by the induction hypothesis we obtain $dom(\mathcal{C}_1(\mathcal{E})) = codom(\mathcal{C}_1) \cup [dom(\mathcal{E}) \setminus dom(\mathcal{C}_1)]$. Therefore, $n \notin dom(\mathcal{E}) \setminus dom(\mathcal{C}_1)$. This implies $n \in dom(\mathcal{C}_1)$ because $n \in dom(\mathcal{E})$, and we complete the proof of the claim.

  To prove Eq. (11), we first obtain:

$$\begin{aligned} dom(\mathcal{C}(\mathcal{E})) &= codom(\mathcal{C}_2) \cup [dom(\mathcal{C}_1(\mathcal{E})) \setminus dom(\mathcal{C}_2)] \\ &= codom(\mathcal{C}_2) \cup \\ &\qquad [codom(\mathcal{C}_1) \cup (dom(\mathcal{E}) \setminus dom(\mathcal{C}_1)) \setminus dom(\mathcal{C}_2)] \\ &= codom(\mathcal{C}_2) \cup [codom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2)] \cup \\ &\qquad [dom(\mathcal{E}) \setminus dom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2)] \\ &= codom(\mathcal{C}) \cup [dom(\mathcal{E}) \setminus dom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2)] \end{aligned}$$

  by using the induction hypothesis. Note that $dom(\mathcal{C}) = dom(\mathcal{C}_1) \cup [dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_1)] \subseteq dom(\mathcal{C}_1) \cup dom(\mathcal{C}_2)$. Then we observe $dom(\mathcal{C}(\mathcal{E})) \subseteq codom(\mathcal{C}) \cup [dom(\mathcal{E}) \setminus dom(\mathcal{C})]$. Conversely, if $n \in dom(\mathcal{E}) \setminus dom(\mathcal{C})$, then we see that $n \in dom(\mathcal{E})$, and $n \notin dom(\mathcal{C})$, which implies $n \notin dom(\mathcal{C}_1)$ and $n \notin dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_1)$. If $\mathcal{C}(\mathcal{E}) =$

$\mathcal{C}_2(\mathcal{C}_1(\mathcal{E})) \neq \emptyset$, then $\mathcal{C}_1(\mathcal{E}) \neq \emptyset$, and we have $dom(\mathcal{E}) \cap codom(\mathcal{C}_1) \subseteq dom(\mathcal{C}_1)$ by the induction hypothesis on $\mathcal{C}_1$. Thus, $n \in dom(\mathcal{E})$ and $n \notin dom(\mathcal{C}_1)$ imply $n \notin codom(\mathcal{C}_1)$. Furthermore, we obtain $n \notin dom(\mathcal{C}_2)$, and $n \in dom(\mathcal{E}) \setminus dom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2)$. Therefore, it follows that $dom(\mathcal{E}) \setminus dom(\mathcal{C}) \subseteq dom(\mathcal{E}) \setminus dom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2)$ and $codom(\mathcal{C}) \cup [dom(\mathcal{E}) \setminus dom(\mathcal{C})] \subseteq dom(\mathcal{C}(\mathcal{E}))$. □

APPENDIX II
PROOF OF PROPOSITION 5.1

We only prove 3 and 5, and the others are left to the reader.

3. It suffices to observe that $(g \circ h^{-1})(U)_g = U_h$. To prove this equality, we first consider the simple case of $U = \bigotimes_{k=1}^{ar(U)} U_k$, where each U_k is a single-qubit gate. If $I \supseteq ran(h)$, then for any $|\psi\rangle = \bigotimes_{i\in I} |\psi_i\rangle_i$, we have $(g \circ h^{-1})(U)_{g^{-1}(i)} = U_{(g\circ h^{-1})(g^{-1}(i))} = U_{h^{-1}(i)}$ for each $i \in ran(h)$, and

$$\begin{aligned}
&(g \circ h^{-1})(U)_g|\psi\rangle \\
&= \bigotimes_{i\in ran(h)} (g \circ h^{-1})(U)_{g^{-1}(i)}|\psi_i\rangle_i \otimes \bigotimes_{i\in I\setminus ran(h)} |\psi_i\rangle_i \\
&= \bigotimes_{i\in ran(h)} (U_{h^{-1}(i)}|\psi_i\rangle_i)_i \otimes \bigotimes_{i\in I\setminus ran(h)} |\psi_i\rangle_i = U_h|\psi\rangle.
\end{aligned}$$

The proof for the general case can be easily achieved by linearity.

5. Any quantum state $|\psi\rangle$ with $dom(|\psi\rangle) \supseteq I \cup J \cup \bigcup_{l=1}^{k} ran(h_l) \cup \bigcup_{n=1}^{m} ran(d_n)$ can be written in the computational basis of $I-$qubits: $|\psi\rangle = \sum_{t\in 2^I} \alpha_t|t\rangle_I|\psi_t\rangle$, where $|\psi_t\rangle$ is in $\mathcal{H}_2^{(\otimes dom(|\psi\rangle)\setminus I)}$ for each t. Since $I \cap J = \emptyset$, we have $J \subseteq dom(|\psi\rangle) \setminus I$, and each $|\psi_t\rangle$ can be written in the computational basis of $J-$qubits: $|\psi_t\rangle = \sum_{u\in 2^J} \beta_{tu}|u\rangle_J|\psi_{tu}\rangle$ where $|\psi_{tu}\rangle$ is in $\mathcal{H}_2^{(\otimes dom(|\psi\rangle)\setminus I\cup J)}$ for each u. Thus, $|\psi\rangle = \sum_{t\in 2^I}\sum_{u\in 2^J} \alpha_t\beta_{tu}|t\rangle_I|u\rangle_J|\psi_{tu}\rangle$. We write LHS and RHS for the circuits in the left-hand and right-hand sides, respectively. Then $RHS(|\psi\rangle) = \{(|\alpha_t\beta_{tu}|^2, V'_m...V'_1U'_k...U'_1|\psi_{tu}\rangle) : t \in I \text{ and } u \in 2^J\}$ where U'_l stands for $U_{lh_l}^{f_l(t)}$ and V'_n for $V_{nd_n}^{g_n(u)}$, $l \leq k$ and $n \leq m$. On the other hand, we have:

$$U'_k...U'_1|\psi_t\rangle = \sum_{u\in 2^J} \beta_{tu}|u\rangle_J U'_k...U'_1|\psi_{tu}\rangle$$

because $J \cap ran(h_l) = \emptyset$ for all $l \leq k$. Consequently,

$$\begin{aligned}
&|\psi\rangle \overset{M_I}{\to} \{(|\alpha_t|^2, U'_k...U'_1|\psi_t\rangle) : t \in 2^I\} \\
&\overset{M_J}{\to} \{(|\alpha_t|^2|\beta_{tu}|^2, V'_m...V'_1U'_k...U'_1|\psi_{tu}\rangle) : t \in I \text{ and } u \in 2^J\} \\
&= LHS(|\psi\rangle)
\end{aligned}$$

where M_I and M_J are abbreviations of the first and second primitive actions, respectively, in the left-hand side. □

APPENDIX III
PROOF OF PROPOSITION 5.2

We only prove items 4, 5 and 8, and the others are left to the reader.

4. We proceed by induction on the length of $\mathcal{C}_1$.

- Case 1. $\mathcal{C}_1 = \mathbf{0}$. Trivial.
- Case 2. $\mathcal{C}_1$ is a primitive action. Then we proceed by induction on the length of $\mathcal{C}_2$. The case of $\mathcal{C}_2 = \mathbf{0}$ is trivial, and the case that $\mathcal{C}_2$ is also a primitive action is immediate from Propositions 5.1.4 and 5.1.5. We now consider the following subcases:
  - Subcase 2.1. $\mathcal{C}_2 = \mathcal{C}'_2|\psi\rangle$. Since $dom(|\psi\rangle) \cap D(\mathcal{C}_1), D(\mathcal{C}_1) \cap D(\mathcal{C}'_2) \subseteq D(\mathcal{C}_1) \cap D(\mathcal{C}_2) = \emptyset$, we obtain $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2 = (\mathcal{C}_1 \Rrightarrow \mathcal{C}'_2)|\psi\rangle = (\mathcal{C}'_2 \Rrightarrow \mathcal{C}_1)|\psi\rangle = \mathcal{C}_2 \Rrightarrow \mathcal{C}_1$ by 10, 11(a) and the induction hypothesis on $\mathcal{C}'_2$.
  - Subcase 2.2. $\mathcal{C}_2 = \mathcal{C}'_2[\theta]$. Since $D(\mathcal{C}_1[\theta^{-1}]) \cap D(\mathcal{C}'_2) = \theta^{-1}(D(\mathcal{C}_1) \cap D(\mathcal{C}_2)) = \emptyset$, we obtain $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2 = (\mathcal{C}_1[\theta^{-1}] \Rrightarrow \mathcal{C}'_2)[\theta] = (\mathcal{C}'_2 \Rrightarrow \mathcal{C}_1[\theta^{-1}])[\theta] = \mathcal{C}_2 \Rrightarrow \mathcal{C}_1$ by 8, 11(b), Propositions 5.1.5 and 5.1.6, and the induction hypothesis on $\mathcal{C}'_2$.
  - Subcase 2.3. $\mathcal{C}_2 = \mathcal{C}_{21} \Rrightarrow \mathcal{C}_{22}$. Then $D(\mathcal{C}_1) \cap D(\mathcal{C}_{21}), D(\mathcal{C}_1) \cap D(\mathcal{C}_{22}) \subseteq D(\mathcal{C}_1) \cap D(\mathcal{C}_2) = \emptyset$, and we obtain $\mathcal{C}_1 \Rrightarrow \mathcal{C}_2 = (\mathcal{C}_1 \Rrightarrow \mathcal{C}_{21}) \Rrightarrow \mathcal{C}_{22} = (\mathcal{C}_{21} \Rrightarrow \mathcal{C}_1) \Rrightarrow \mathcal{C}_{22} = \mathcal{C}_{21} \Rrightarrow (\mathcal{C}_1 \Rrightarrow \mathcal{C}_{22}) = \mathcal{C}_{21} \Rrightarrow (\mathcal{C}_{22} \Rrightarrow \mathcal{C}_1) = \mathcal{C}_2 \Rrightarrow \mathcal{C}_1$ by 7, 11(c) and the induction hypothesis on $\mathcal{C}_{21}$ and $\mathcal{C}_{22}$.
- Case 3. $\mathcal{C}_1 = \mathcal{C}'_1|\psi\rangle$. Similar to Subcase 2.1.
- Case 4. $\mathcal{C}_1 = \mathcal{C}'_1[\theta]$. Similar to Subcase 2.2.
- Case 5. $\mathcal{C}_1 = \mathcal{C}_{11} \Rrightarrow \mathcal{C}_{12}$. Similar to Subcase 2.3.

5. By Definition 4.1 we obtain:

$$\begin{aligned}
&dom(\mathcal{C}_1 \Rrightarrow (\mathcal{C}_2 \Rrightarrow \mathcal{C}_3)) \\
&= dom(\mathcal{C}_1) \cup [dom(\mathcal{C}_2 \Rrightarrow \mathcal{C}_3) \setminus codom(\mathcal{C}_1)] \\
&= dom(\mathcal{C}_1) \cup [dom(\mathcal{C}_2) \\
&\qquad \cup (dom(\mathcal{C}_3) \setminus codom(\mathcal{C}_2)) \setminus codom(\mathcal{C}_1)] \\
&= dom(\mathcal{C}_1) \cup [dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_1)] \cup \\
&\qquad [dom(\mathcal{C}_3) \setminus codom(\mathcal{C}_1) \cup codom(\mathcal{C}_2)] \\
&= dom(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) \cup [dom(\mathcal{C}_3) \setminus codom(\mathcal{C}_1) \cup codom(\mathcal{C}_2)], \text{ and}
\end{aligned}$$

$$\begin{aligned}
&dom((\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) \Rrightarrow \mathcal{C}_3) \\
&= dom(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) \cup [dom(\mathcal{C}_3) \setminus codom(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)] \\
&= dom(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) \cup [dom(\mathcal{C}_3) \setminus \\
&\qquad (codom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2)) \cup codom(\mathcal{C}_2)].
\end{aligned}$$

Since $\mathcal{C}_2 \Rrightarrow \mathcal{C}_3$ is well-defined, we have $[dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_2)] \cap dom(\mathcal{C}_3) = \emptyset$, and

$$\begin{aligned}
&dom(\mathcal{C}_3) \setminus (codom(\mathcal{C}_1) \setminus dom(\mathcal{C}_2)) \cup codom(\mathcal{C}_2) \\
&= [dom(\mathcal{C}_3) \setminus codom(\mathcal{C}_1) \cup codom(\mathcal{C}_2)] \\
&\qquad \cup [(dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_2)) \cap dom(\mathcal{C}_3)] \\
&= dom(\mathcal{C}_3) \setminus codom(\mathcal{C}_1) \cup codom(\mathcal{C}_2).
\end{aligned}$$

Therefore, $dom(\mathcal{C}_1 \Rrightarrow (\mathcal{C}_2 \Rrightarrow \mathcal{C}_3)) = dom((\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) \Rrightarrow \mathcal{C}_3)$. Finally, for any $|\psi\rangle$ with $dom(|\psi\rangle) \supseteq dom(\mathcal{C}_1 \Rrightarrow (\mathcal{C}_2 \Rrightarrow \mathcal{C}_3))$, it holds that

$$\begin{aligned}
&(\mathcal{C}_1 \Rrightarrow (\mathcal{C}_2 \Rrightarrow \mathcal{C}_3))(|\psi\rangle) = (\mathcal{C}_2 \Rrightarrow \mathcal{C}_3)(\mathcal{C}_1(|\psi\rangle)) \\
&= \mathcal{C}_3(\mathcal{C}_2(\mathcal{C}_1(|\psi\rangle))) = \mathcal{C}_3((\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)(|\psi\rangle)) \\
&= ((\mathcal{C}_1 \Rrightarrow \mathcal{C}_2) \Rrightarrow \mathcal{C}_3)(|\psi\rangle).
\end{aligned}$$

8. We only prove the second part, and the first part is similar. First, we have:

$$\begin{aligned}
&dom((\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)|\psi\rangle) \\
&= dom(\mathcal{C}_1) \cup [dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_1)] \setminus dom(|\psi\rangle) \\
&= dom(\mathcal{C}_1) \cup [dom(\mathcal{C}_2) \setminus codom(\mathcal{C}_1) \setminus dom(|\psi\rangle)] \\
&= dom(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2|\psi\rangle)
\end{aligned}$$

because $dom(\mathcal{C}_1) \cap dom(|\psi\rangle) = D(\mathcal{C}_1) \cap dom(|\psi\rangle) = \emptyset$.

Second, for any $|\varphi\rangle$ with $dom(|\varphi\rangle) \supseteq dom((\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)|\psi\rangle)$, if $dom(|\varphi\rangle) \cap dom(|\psi\rangle) \neq \emptyset$, then $(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2|\psi\rangle)(|\varphi\rangle) = \mathcal{C}_1(\mathcal{C}_2|\psi\rangle(|\varphi\rangle)) = \mathcal{C}_1(\emptyset) = \emptyset = (\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)|\psi\rangle(|\varphi\rangle)$. For the

case of $dom(|\varphi\rangle) \cap dom(|\psi\rangle) = \emptyset$, we note that $dom(|\psi\rangle) \cap codom(\mathcal{C}_1) \subseteq dom(|\psi\rangle) \cap D(\mathcal{C}_1) = \emptyset$. By Proposition 4.1 we obtain: $dom(\mathcal{C}_1(|\psi\rangle)) = codom(\mathcal{C}_1) \cup [dom(|\varphi\rangle) \setminus dom(\mathcal{C}_1)]$. Then $dom(|\psi\rangle) \cap dom(\mathcal{C}_1(|\varphi\rangle)) = \emptyset$, and it follows from Lemma 4.1.3 that

$$(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2|\psi\rangle)(|\varphi\rangle) = \mathcal{C}_2|\psi\rangle(\mathcal{C}_1(|\varphi\rangle)) = \mathcal{C}_2(|\psi\rangle \otimes \mathcal{C}_1(|\varphi\rangle))$$
$$= \mathcal{C}_2(\mathcal{C}_1(|\psi\rangle \otimes |\varphi\rangle)) = (\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)(|\psi\rangle \otimes |\varphi\rangle) =$$
$$(\mathcal{C}_1 \Rrightarrow \mathcal{C}_2)|\psi\rangle(|\varphi\rangle). \square$$

ACKNOWLEDGMENT

The author is very grateful to the anonymous referees for their invaluable comments and suggestions which helped to improve considerably the presentation of this paper. The authors would like to thank Dr. Zhengfeng Ji for his kind comments and suggestions.

REFERENCES

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. Wootters, Teleporting an unknown quantum state via classical and EPR channels, *Physical Review Letters*, 70(1993)1895-1899.

[2] J. I. Cirac, A. K. Ekert, S. F. Huelga and C. Macchiavello, Distributed quantum computation over noisy channels, *Physical Review A*, 59(1999)4249-4254.

[3] R. Cleve and H. Buhrman, Substituting quantum entanglement for communication, *Physical Review A*, 56(1997)1201-1204.

[4] D. Collins, N. Linden and S. Popescu, Nonlocal content of quantum operations, *Physical Reviews A*, 64(2001) art. no. 032302.

[5] E. D'Hondt and P. Panangaden, The computational power of the W and GHZ states, *Quantum Information and Computation*, 6(2006)173-183.

[6] R. Y. Duan, Y. Feng and M. S. Ying, Entanglement is not necessary for perfect discrimination between unitary operations, *Physical Review Letters*, 98 (2007) art. no. 100503.

[7] J. Eisert, K. Jacobs, P. Papadopoulos and M. B. Plenio, Optimal local implementation of nonlocal quantum gates, *Physical Review A*, 62(2000)052317.

[8] Y. Feng, R. Y. Duan, Z. F. Ji and M. S. Ying, Probabilistic bisimulations for quantum processes, *Information and Computation*, 205(2007)1608-1635.

[9] S. J. Gay and R. Nagarajan, Communicating quantum processes, in: *Proceedings of the 32nd ACM Symposium on Principles of Programming Languages*, ACM Press, 2005.

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

[11] D. Gottesman and I. L. Chuang Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, *Nature*, 402(1999)390C393.

[12] L. K. Grover, Quantum telecomputation, see *arXiv:quant-ph/9704012*.

[13] P. Jorrand and M. Lalire, Toward a quantum process algebra, in: *Proceedings of the 1st ACM Conference on Computing Frontiers*, ACM Press, 2005.

[14] 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.

[15] R. Jozsa and N. Linden, On the role of entanglement in quantum-computational speed-up, *Proceedings of the Royal Society of London, Series A-Mathematical, Physical and Engineering Sciences*, 459(2003)2011-2032.

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

[17] M. Lalire and F. 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.

[18] N. A. Lynch, *Distributed Algorithms*, Morgan Kaufmann, San Francisco, 1996.

[19] A. Serafini, S. Mancini ans S. Bose, Distributed quantum computation via optical fibers, *Physical Review Letters*, 96(2006) art. no. 010503.

[20] S. Tani, H. Kobayashi and K. Matsumoto, Exact quantum algorithms for the leader election problem, in: V. Diekert and B. Durand (Eds.), *Proc. STACS 2005,* LNCS 3404, Springer-Verlag, pp. 581-592, 2005.

[21] R. van Meter, W. J. Munro, K. Nemoto and K. M. Itoh, Arithmetic on a distributed-memory quantum multicomputer, *ACM Journal on Emerging Technologies in Computing Systems*, 3(2008)17:1-23.

[22] R. van Meter, K. Nemoto and W. J. Munro, Communication links for distributed quantum computation, *IEEE Transactions on Computers*, 56(2007)1643-1653.

[23] G. M. Wang and M. S. Ying, Perfect many-to-one teleportation with stabilizer states, *Physical Review A*, 77(2008) art. no. 032324. Also see *arXiv:0711.0462*.

[24] G. M. Wang and M. S. Ying, Deterministic distributed dense coding with stabilizer states, *Physical Review A*, 77(2008) art. no. 032306. Also see *arXiv:0710.4403*.

[25] A. Yimsiriwattana and S. J. Lomonaco Jr., Generalized GHZ states and distributed quantum computing, in: D. Evans, J. J. Holt, C. Jones, K. Klintworth, B. Parshall, O. Pfister, and H. N. Ward (Eds.), *Coding Theory and Quantum Computing*, AMS Contemporary Mathematics 381(2005). Also see *arXiv:quant-ph/0402148v3*.

[26] A. Yimsiriwattana and S. J. Lomonaco Jr., Distributed quantum computing: a distributed Shor algorithm, in: E. Donkor, A. R. Pirich and H. E. Brandt (Eds.), *Quantum Information and Computation II, Proceedings of SPIE*, 5436(2004)360-372. Also see *arXiv:quant-ph/0403146v2*.

[27] M. S. Ying, Y. Feng, R. Y. Duan and Z. F. Ji, An Algebra of Quantum Processes, *ACM Transactions on Computational Logic* (accepted). Also see *arXiv:quant-ph/0707.0330*.

Mingsheng Ying graduated from Fuzhou Teachers College, Jiangxi, China, in 1981. He is Distinguished Professor with the Center of Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology, Sydney, Australia, and Cheung Kong Professor with the State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology, Tsinghua University, Beijing, China. His research interests are quantum computation and quantum information, formal methods and logics in computer science, and foundations of artificial intelligence. He has published more 100 papers in various international journals. He is the author of the book *Topology in Process Calculus: Approximate Correctness and Infinite Evolution of Concurrent Programs* (Springer-Verlag, 2001).

Yuan Feng Yuan Feng received his BS and PhD degrees from Department of Applied Mathematics and Department of Computer Science and Technology, Tsinghua University in 1999 and 2004, respectively. He is now an associate professor at Department of Computer Science and Technology, Tsinghua University, with the research interest mainly in quantum information and quantum computation.