Int J Theor Phys (2011) 50: 1305–1318
DOI 10.1007/s10773-010-0603-z

Duality Quantum Computing and Duality Quantum Information Processing

Gui Lu Long

Received: 5 October 2010 / Accepted: 22 November 2010 / Published online: 1 December 2010

Abstract Quantum mechanical systems exhibit wave-particle duality property. This duality property has been exploited for information processing. A duality quantum computer is a quantum computer on the move and passing through a multi-slits. It offers quantum wave divider and quantum wave combiner operations in addition to those allowed in an ordinary quantum computer. It has been shown that all linear bounded operators can be realized in a duality quantum computer, and a duality quantum computer with n qubits and d-slits can be realized in an ordinary quantum computer with n qubits and a qudit in the so-called duality quantum computing mode. In this article, the main structure of duality quantum computing, their mathematical description and applications are reviewed.

Keywords Duality computer · Duality quantum computer · Duality computing mode · Duality mode · Quantum divider · Quantum combiner · Duality parallelism

1 Introduction

The duality computer, or duality quantum computer exploits the wave-particle duality of quantum systems [1]. To exhibit the particle wave duality property, one needs to let a quantum computer move. Of course, it would be very difficult to imagine a huge quantum computer system such as nuclear magnetic resonance facility to move and pass through a double slits. However we do not need to build such a complicated device and it has been proven that a moving n-qubit duality computer passing through a d-slits can be perfectly simulated by an ordinary quantum computer with n-qubit and an additional qudit, where a qudit is similar to a qubit but with d levels [2, 3]. Duality quantum computing in such a way is called

G.L. Long (✉)
Key Laboratory for Atomic and Molecular Nanosciences and Department of Physics,
Tsinghua University, Beijing 100084, China
e-mail: gllong@tsinghua.edu.cn

G.L. Long
Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China

duality quantum computing mode, or duality mode in a quantum computer. Thus we are exempt completely from building a moving quantum computer and can work entirely in an ordinary quantum computer in performing duality quantum computing. Hence, we will treat computing with a true duality quantum computer and with the duality mode of a quantum computer as the same. We will interchangeably use the terminologies in these two pictures in this paper.

The duality quantum computer offers additional capability in information processing in addition to those offered by a quantum computer. This is the duality parallelism. Duality parallelism refers to the capability with which one can perform different gate operations on the sub-wave functions at different slits [1]. This enables the duality computer to perform non-unitary gate operations. After a series of studies [1–4], it is found that the duality quantum gate, or duality gate has the following form

$$L_c = \sum_{i=0}^{d-1} c_i U_i, \tag{1}$$

where c_i is a complex number and U_i is unitary, and the c_i's satisfy

$$\sum_{i=0}^{d-1} |c_i| \leq 1. \tag{2}$$

This form of duality gate is called complex duality gate, or complex generalized quantum gate. In the original paper [1] and in [6], the duality quantum gate is restricted to positive real c_i which is denoted by r_i, and they are constrained by $\sum_i r_i = 1$. In this case, the duality quantum gate is called real duality gate or real generalized quantum gate, and is denoted as L_r, and

$$L_r = \sum_{i=0}^{d-1} r_i U_i. \tag{3}$$

This corresponds to a physical picture of asymmetric d-slits, and r_i is the probability that the duality computer system passes through the i-th slit.

The new operations in duality computing are the quantum wave divider (QWD) operation and quantum wave combiner (QWC) operation [1]. The quantum wave divider operation divides the wave function into many identical parts with reduced amplitudes. The physical picture of this division is that a quantum system passing through a d-slits, and its wave function is divided into d sub-waves, each with the same internal wave function and differs only in the center of mass motion characterized by the slit. The combiner operation adds up all the sub-waves into one wave function. Though the divider operation is analogous to quantum cloning, there is a fundamental difference between them. In quantum divider, one divides the wave function of the same quantum system into many parts, whereas in quantum cloning one copies the state of one quantum system onto another quantum system. The division operation does not violate the non-cloning theorem.

Duality gates are generally non-unitary, it is natural that non-unitary evolutions, such as those in open quantum systems should be simulated in such machines. In a wider context, it is an important issue to study the computing capabilities of duality computing. The recent theorem of Wang, Du and Dou [5] which limits what can not be a duality gate in a Hilbert space with infinite degrees of freedom, is an important step toward this direction.

There have been intensive interests in the theory of duality computer in recent years [1–18]. Here in this review article we will briefly describe the main results. The details of the proof are not given, interested readers can refer to the original papers.

This article is organized as follows. In Sect. 2, we describe the divider and combiner operations. In Sect. 3, we briefly review duality quantum computing. In Sect. 4, we summarize the mathematical theory of duality computer. In Sect. 5, we give a brief review of the algorithms in duality computer and their implications for quantum algorithm design. Finally in Sect. 6, we give a brief summary and present a perspective.

2 Divider, Combiner Operations

The most general form of duality quantum gates have been given [2, 3]. Though the main mathematical properties are essential the same, the notations in previous literatures are not unified. For the convenience of readers, we use the expressions from duality mode in this review article. They are derived according to the duality mode in [2, 3, 11].

The divider structure describes the properties of a quantum wave divider, and it is denoted as $p = (p_0, \dots, p_{d-1})$ where each p_i is a complex number with a module less than 1 and $\sum_{i=0}^{d-1} |p_i|^2 = 1$. Writing $H^{\oplus^d}$ for $\bigoplus_{i=0}^{d-1} H_i$ where $H_i = H$, $i = 0, \dots, d-1$. The divider operator $D_m \colon H \to H^{\oplus^d}$ is defined by

$$D_m\psi = \bigoplus_{i=0}^{d-1} (p_i\psi). \tag{4}$$

This definition of the divider operator in (4) is of the most general form, and it describes a general multi-slits. When there are d identical slits, then $p_i = \sqrt{1/d}$.

Mathematically, the combiner operation C_m can be represented as follows,

$$C_m(\psi_0 \oplus \dots \oplus \psi_{d-1}) = \sum_{i=0}^{d-1} q_i\psi_i, \tag{5}$$

where $q = \{q_0, \dots, q_{d-1}\}$ is the *combiner structure* that describes the properties of a quantum wave combiner. Each q_i is a complex number with a module less than 1, and $\sum_i |q_i|^2 = 1$. If the combiner structure $q_i = 1/\sqrt{d}$, we call it a uniform combiner structure.

In the case of uniform divider and combiner structures, the combined action of divider and combiner leaves the state unchanged, namely

$$D_m\psi = \bigoplus_{i=1}^{d} \sqrt{1/d}\psi, \tag{6}$$

$$C_m \bigoplus_{i=1}^{d} \sqrt{1/d}\psi_i = \sum_i 1/d\psi = \psi. \tag{7}$$

This property also hold when the divider structure and combiner structure satisfy certain relation, which will be given in the next section.

It will be shown later in this article that the divider and combiner structure D_m and C_m each forms a column or a row of elements in a unitary matrix respectively. For duality gates with the form of L_r in (3), the unitary matrices that lead to the structures of C_m and D_m are adjoint to each other.

3 Duality Quantum Computing Mode in a Quantum Computer

A duality computer is a moving quantum computer passing through a d-slits. In Fig. 1, we give an illustration for a duality quantum computer with 3-slits. The quantum wave starts from the 0-th slit in leftmost wall, and then goes to the middle screen with three slits (this is the divider operation). Between the middle screen and the rightmost screen, some unitary operations are performed on the sub-waves from different slits. They are then collected at the 0-slit in the rightmost screen where a detector is placed, and this is the quantum wave combiner operation.

One can imagine that building such a moving quantum computer is extremely hard. However it has been shown that a duality computer can be simulated on an ordinary quantum computer with just a little extra qubit resource [2, 3]. For example, an n-qubit duality quantum computer with d-slits can be simulated by a quantum computer with n qubits and one qudit. Hence, duality quantum computing can be treated as a special working mode of a quantum computer. We are completely exempt from building a moving quantum computer.

The divider operation is simulated by a unitary operation V and the combiner operation is simulated by another unitary operation W on an auxiliary qudit that represents a d-slits. The quantum circuit is shown in Fig. 2, where V and W are two unitary operations on the auxiliary qudit. Between the operations V and W, there are d auxiliary qudit controlled operations. The sub-levels of the qudit simulate the d-slits. At first the initial state of the quantum computer plus the qudit system is $|\Psi\rangle|0\rangle$. Then we perform the unitary operation

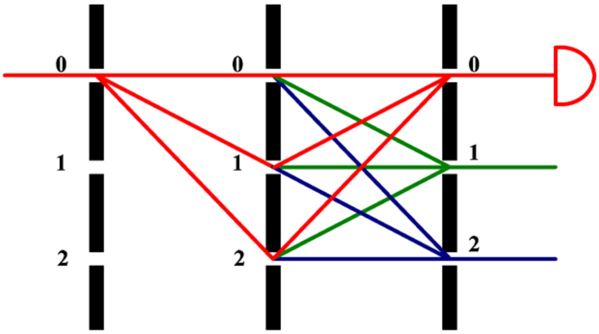

Fig. 1 An illustrated picture for a three-slits duality computer simulated by a quantum computer working in duality mode

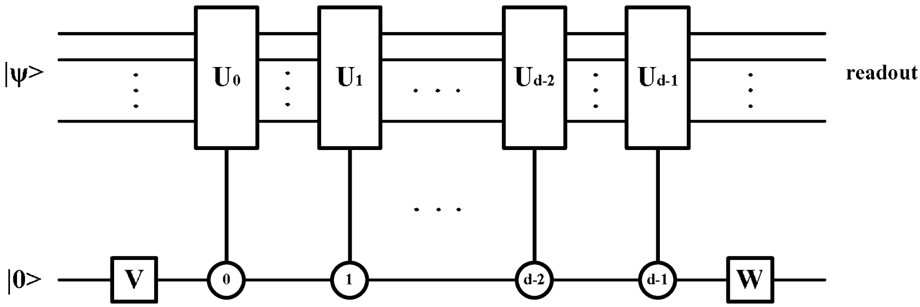

Fig. 2 Duality computing in a quantum computer. $|\Psi\rangle$ is the initial state of duality quantum computer and $|0\rangle$ is the controlling qudit. The circles represent the state of the controlling qudit, the squares represent unitary operations. Unitary operations $U_0, U_1, \ldots, U_{d-1}$ are activated only when the qudit holds the respective values indicated in *circles*

V on the auxiliary qudit, and this transforms the state into

$$|\Psi\rangle|0\rangle \rightarrow |\Psi\rangle V|0\rangle = \sum_{i=0}^{d-1} V_{i0}|\Psi\rangle|i\rangle. \tag{8}$$

Note that the coefficient in each slit is now V_{i0} which is the matrix element of the unitary matrix V. In general, V_{i0} is a complex number. Note that $|V_{i0}| \leq 1$ and $\sum_{i=0}^{d-1} |V_{i0}|^2 = 1$ are the constraint on the coefficients. This V is a generalized quantum division operation, and

$$p_i = V_{i0}, \tag{9}$$

is the divider structure.

Then performing the auxiliary qudit controlled operations on the quantum computer, one has the following state

$$\sum_{i=0}^{d-1} V_{i0} U_i |\Psi\rangle|i\rangle. \tag{10}$$

This simulates the simultaneous operations on the sub-waves at different slits.

To combine the wave functions, one performs the unitary operation W, and the result of this operation is

$$\sum_i V_{i0} U_i |\Psi\rangle W|i\rangle. \tag{11}$$

Because the detector is placed at slit 0, therefore we focus ourselves only on the wave function when the qudit is in state $|0\rangle$. The wave function at the upper slit, namely slit 0, is now

$$\sum_i W_{0i} V_{i0} U_i |\Psi\rangle|0\rangle = \sum_i (W_{0i} V_{i0}) U_i |\Psi\rangle|0\rangle, \tag{12}$$

hence $c_i = W_{0i} V_{i0}$ is the coefficients in the duality gate in (1).

It should be noted that W is a generalized combiner operation and

$$q_i = W_{0i}, \tag{13}$$

is the combiner structure in (5). Physically, this corresponds to a multiple asymmetric slits with some unitary lenses at each slit so that they modify the phases of the wave function at each slit. This is the generalized quantum combiner operation.

For a special case where $W = V^\dagger$, we recover to real generalized quantum gate because $r_i = V_{0i}^\dagger V_{i0} = |V_{i0}|^2$ which is real and positive, and satisfies

$$\sum_i r_i = \sum_i |V_{i0}|^2 = 1, \tag{14}$$

which is the case corresponding to L_r in (2).

In general $c_i = W_{0i} V_{i0}$ is a complex number and is the product of two unitary matrix elements. The sum of c_i's is

$$\sum_i c_i = \sum_i W_{0i} V_{i0} = (WV)_{00}. \tag{15}$$

The value of $(WV)_{00}$ is just that of an element of a unitary matrix, and hence has the constraint $|(WV)_{00}| \leq 1$. Hence the most general form of duality gates allowable by the laws of quantum mechanics is

$$\sum_{i=0}^{d-1} c_i U_i, \tag{16}$$

where c_i are complex numbers with module less or equal to 1, and with the constraint $|\sum_i c_i| \leq 1$ and can be written as the product of elements of two unitary matrices, namely $c_i = W_{0i} V_{i0}$.

It has been shown recently by Cao et al. [10] that it is necessary and sufficient to decompose a generalized quantum gate in the form in (16) in terms of two unitary operators V and W in (15) if the coefficients satisfies

$$\sum_i |c_i| \leq 1. \tag{17}$$

They have given the explicit form of the decomposition, which is crucial in duality quantum algorithm design and related studies.

4 Mathematical Theory of Duality Quantum Computing

The mathematical theory of duality computer has been the subject of many recent studies. The mathematical descriptions can be found in [1–10]. Concise mathematical expressions together with the studies of the properties of divider and combiner, and duality gates are given.

4.1 Properties of Generalized Quantum Gates and Related Operators

Here we briefly summarize the results, and no proof will be given. Interested readers can read the original papers for their proof. In order to keep uniformity, we have used symbols that are different from their original papers. However, the mathematical theory of the divider and combiner operations are restricted to a real structure, namely $p = \{p_0, p_1, \ldots, p_{d-1}\}$ has each p_i real and positive, and the combiner structure is also a special case of the uniform structure. The following results are from [6] and the corresponding operators are labeled with a subscript p.

Lemma 4.1 *The operator D_p is a linear isometry.*

Lemma 4.2 *The operator C_p with identical combiner structure is a linear isometry and $C_p = D_p^\dagger$.*

Note that the combiner with uniform structure is the special case of the general combiner operator.

Theorem 4.3 *The identity I_H is an extreme point of $\mathcal{G}(H)$, where $\mathcal{G}(H)$ is the set of real generalized quantum gates on H.*

Every unitary operator is in $\mathcal{G}(\mathcal{H})$ and $I_{\mathcal{H}} \in \mathcal{G}(\mathcal{H})$. This is to say that $\sum_i p_i U_i = I_{\mathcal{H}}$ if and only if $U_i = I_{\mathcal{H}}$ for all i.

Corollary 4.4 *The extreme points of $\mathcal{G}(\mathcal{H})$ are precisely the unitary operators in $\mathcal{H}$.*

Theorem 4.3 and Corollary 4.4 together tell us that the ordinary quantum computer is included in the duality computer.

Denoting $\mathcal{B}(\mathcal{H})$ by the set of bounded linear operators on $\mathcal{H}$ and let $\mathbb{R}^+\mathcal{G}(\mathcal{H})$ be the positive cone generated by $\mathcal{G}(\mathcal{H})$. That is

$$\mathbb{R}^+\mathcal{G}(\mathcal{H}) = \{\alpha A : A \in \mathcal{G}(\mathcal{H}), \alpha \geq 0\}. \tag{18}$$

Theorem 4.5 *If* $\dim \mathcal{H} < \infty$, *then* $\mathcal{B}(\mathcal{H}) = \mathbb{R}^+\mathcal{G}(\mathcal{H})$.

This theorem tells us that the duality computer is able to perform any operator in a Hilbert spaces $\mathcal{H}$. It will be interesting to study the computability of duality computer in terms of this theorem. However, the theorem by Wang, Du and Dou [5] has given explicitly what can not be a generalized quantum gate when the dimension is infinite. That will be reviewed shortly.

Corollary 4.6 *If* $\dim \mathcal{H} < \infty$, *then $A \in \mathcal{B}(\mathcal{H})$ is normal if and only if $A = \alpha \sum_i p_i U_i$ where $\alpha \geq 0$, $p_i > 0$, $\sum_i p_i = 1$ and U_i are unitary operators that mutually commute.*

Before going further, we briefly introduce some terminology. This part is from [5] of Wang, Du and Dou. Let $\mathcal{H}$ and $\mathcal{K}$ be separable complex Hilbert spaces and let $\mathcal{H}, \mathcal{K}$ denote all the bounded linear operators from $\mathcal{H}$ to $\mathcal{K}$. If $\mathcal{H} = \mathcal{K}$, $\mathcal{B}(\mathcal{H}, \mathcal{H})$ is abbreviated by $\mathcal{B}(\mathcal{H})$. An operator $A \in \mathcal{B}(\mathcal{H}, \mathcal{K})$ is said to be a contraction if $\|A\| \leq 1$. The set of all contractions in $\mathcal{B}(\mathcal{H}, \mathcal{K})$ is denoted by $\mathcal{B}(\mathcal{H}, \mathcal{K})_\infty$. An operator $A \in \mathcal{B}(\mathcal{H})$ is said to be a positive operator if $(Ax, x) \geq 0$ for $x \in \mathcal{H}$. An operator $P \in \mathcal{B}(\mathcal{H})$ is said to be an orthogonal projection if $P = P^\dagger = P^2$. An operator $A \in \mathcal{B}(\mathcal{H})$ is said to be semi-Fredholm if the range $\mathcal{R}(A)$ of A is closed and at least one of $\dim \mathcal{N}(A)$ and $\dim \mathcal{N}(A^\dagger)$ is finite. In this case, the Fredholm index of A is defined by $\operatorname{ind} A = \dim \mathcal{N}(A) - \dim \mathcal{N}(A^\dagger)$, where $\dim \mathcal{N}(K)$ denotes the dimension of the null-space $\mathcal{N}(K)$ of an operator $K \in \mathcal{B}(\mathcal{H})$. An operator E is said to be a partial isometry if E is unitary as an operator from $\mathcal{R}(E^\dagger)$ onto $\mathcal{R}(E)$. The following results are due to Wang, Du and Dou [5].

Theorem 4.7 *If $A \in \mathcal{B}(\mathcal{H})_1$ is a finite-rank perturbation of a semi-Fredholm partial isometry with* $\operatorname{ind} A \neq 0$, *then A is not a generalized quantum gate.*

This is a significant result, since it has told us explicitly that what can not be a generalized quantum gate. It clearly forbids some type of operations that a duality computing admits. This theorem has paved the way for further study on the computability of duality computing. To prove the Wang-Du-Dou theorem, the following lemmas are required.

Theorem 4.8 *Denote $\mathcal{E}_\mathcal{V}(X) = VXV^\dagger$ if $V \in \mathcal{B}(\mathcal{H})$ is an isometry. Then* $\mathcal{E}_\mathcal{V} \in \operatorname{Ext}[\mathcal{Q}(\mathcal{H})]$.

To understand this theorem, some terminology needs be introduced. Denote $\mathcal{A} = (A_1, \ldots, A_d)$, where A_i, $1 \leq i \leq d$, are arbitrary operators in $\mathcal{B}(\mathcal{H})$ satisfying $\sum_{i=1}^d A_i^\dagger A_i = I$. A quantum operation deduced by $\mathcal{A}$ is a bounded linear operator $\mathcal{E}_\mathcal{A}$ defined on $\mathcal{B}(\mathcal{H})$ by

$$\mathcal{E}_\mathcal{A}(X) = \sum_{i=1}^{d} A_i X A_i^\dagger, \quad X \in \mathcal{B}(\mathcal{H}). \tag{19}$$

The set of all quantum operations on $\mathcal{H}$ is denoted by $\mathcal{Q}(\mathcal{H})$. If the A_i, $1 \le i \le d$, are positive operators satisfying $\sum_{i=1}^{d} A_i^2 = I$, then $\mathcal{E}_{\mathcal{A}}$ is called a positive quantum operation, the set of all positive quantum operations is denoted by $\mathcal{Q}_{pos}(\mathcal{H})$. If P_i, $1 \le i \le d$, are orthogonal projections satisfying $\sum_{i=1}^{d} P_i = I$, then $\mathcal{E}_{\mathcal{P}}$ is called a projective quantum operation, the set of all projective quantum operations is denoted by $\mathcal{Q}_{pro}(\mathcal{H})$. If U_i, $1 \le i \le d$, are unitary operators in $\mathcal{B}(\mathcal{H})$ and $\sum_{i=1}^{d} p_i = 1$ with $p_i > 0$, the quantum operation $\mathcal{E}_{\mathcal{U}}(X) = \sum_{i=1}^{d} p_i U_i X U_i^{\dagger}$ is said to be a unitary quantum operation.

Lemma 4.9 *Let $p = (p_1, \dots, p_d)$ be a probability distribution and let A_i, $1 \le i \le d$, be contractions. If $I = \sum_{i=1} p_i A_i$, then $A_i = I$ for $1 \le i \le d$.*

Lemma 4.10 *Let A be a contraction and let A as an operator from $\mathcal{H} = \mathcal{H}_\infty \oplus \mathcal{H}_\in$ into $\mathcal{H} = \mathcal{K}_\infty \oplus \mathcal{H}_\in$ have the operator matrix*

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}. \tag{20}$$

If A_{11} is a unitary from $\mathcal{H}_\infty$ onto $\mathcal{K}_\infty$, then $A_{12} = 0$ and $A_{21} = 0$.

Corollary 4.11 *A non-unitary isometry is not a generalized quantum gate.*

Corollary 4.12 *If* $\dim \mathcal{H} = \infty$, *then* $\mathcal{G}(\mathcal{H}) \neq \mathcal{B}(\mathcal{H})_\infty$.

Lemma 4.13 *If $A \in \mathcal{B}(\mathcal{H})$ with $\|A\| < 1 - \frac{2}{d}$ for some $d > 2$, there are unitary operators $U_1, U_2, \dots, U_d$ such that*

$$A = \frac{1}{n}(U_1 + U_2 + \cdots + U_d). \tag{21}$$

Theorem 4.14 $\mathcal{B}(\mathcal{H})_\infty^\circ \subset \mathcal{G}(\mathcal{H})$.

This theorem tells us that if $A \in \mathcal{B}(\mathcal{H})_\infty$ is not a generalized quantum gate, then A should be in the spherical surface of the unit ball $\mathcal{B}(\mathcal{H})_\infty$.

Let $\mathbb{R}^+\mathcal{G}(\mathcal{H})$ be the positive cone generalized by $\mathcal{G}(\mathcal{H})$. That is

$$\mathbb{R}^+\mathcal{G}(\mathcal{H}) = \{\alpha A : A \in \mathcal{G}(\mathcal{H}), \alpha \ge 0\}. \tag{22}$$

Theorem 4.15 *When* $\dim \mathcal{H} = \infty$, $\mathcal{B}(\mathcal{H}) = \mathbb{R}^+\mathcal{G}(\mathcal{H})$.

Conjecture 4.16 $\mathcal{B}(\mathcal{H})_\infty / \mathcal{G}(\mathcal{H})$ is the set of all finite-rank perturbations of semi-Fredholm partial isometries such that the index does not equal to 0.

Lemma 4.17 *Let $A \in \mathcal{B}(\mathcal{H})$. If, for each vector $x \in \mathcal{H}$, there exists a complex number λ_x such that $Ax = \lambda_x x$, then there exists a complex number λ such that $A = \lambda I$.*

Lemma 4.18 *If $X = \sum_{i=1}^{d} A_i X A_i^{\dagger}$ for each operator $X \in \mathcal{B}(\mathcal{H})$, then $A_i = \lambda_i I$, where $\lambda_i \in \mathbb{C}$ and $1 \le i \le d$.*

Corollary 4.19 *A quantum operation deduced by a unitary is an extreme point of $\mathcal{Q}(\mathcal{H})$.*

Theorem 4.20 *Let $A=(A_1,\dots,A_d)$ and $\mathcal{P}=(P_1,\dots,P_{d'})$, where A_j, $P_i\in\mathcal{B}(\mathcal{H})$, $\sum_{j=1}^{d}A_j^\dagger A_j=I$, $\sum_{i=1}^{d'}P_i^\dagger P_i=I$, $1\le i\le d'$, are orthogonal projections. If $\mathcal{E}_{\mathcal{P}}=\mathcal{E}_{\mathcal{A}}$, then there exists an $d\times d'$ complex matrix $M=(\lambda_{ji})_{d\times d'}$ with $M^\dagger M=I_{d'\times d'}$ and*

$$A_j=\sum_{i=1}^{d'}\lambda_{ji}P_i, \tag{23}$$

where $I_{d'\times d'}$ denotes the $d'\times d'$ identity matrix.

Corollary 4.21 *Under the assumption as in Theorem 4.20, additional $d'=d$, then the matrix M is an $d'\times d'$ unitary.*

4.2 Properties of Complex Generalized Quantum Gates and Related Operators

The properties of complex generalized quantum gates have been extensively studied by Cao et al. and they have extended many of the results for real general quantum gates into complex generalized quantum gates [4, 10]. Here we briefly state their results. The results are from [10].

Let H be a Hilbert space over the field C of all complex numbers, $U(H)$ be the set of all unitary operators on H and $RAGQG(H)$ be the set of all generalized quantum gates $\sum_{k=0}^{d-1}p_kU_k$, where $p_k\in R^+$, $U_k\in U(H)$, $\sum_{k=0}^{d-1}p_k=1$, $d=1,2,\dots$.

Theorem 4.22

(1) *$RAGQG(H)=[0,1]GQG(H)\supset U(H)$;*
(2) *The set $GQG(H)$ and $RAGQG(H)$ are absolutely convex subsets of*

$$B(H)_1=\{T\in B(H):\|T\|\le 1\}. \tag{24}$$

(3) *$GQG(H)\supset\{T\in B(H):T^*=T,\|T\|\le 1\}\cup\{T\in B(H):\|T\|<1\}$.*
(4) *$B(H)=R^+RAGQG(H)=R^+GQG(H)$, and $GQG(H)$ is a multiplicative semigroup.*
(5) *When $\dim H<\infty$, we have*

$$B(H)_1=GQG(H)=RAGQG(H). \tag{25}$$

Remark 4.23 When $\dim H=\infty$, we have

$$RAGQG(H)\ne B(H)_1.$$

Lemma 4.24 *Let*

$$U_k\in U(H),\quad c_k\in C/\{0\}\quad (k=0,1,2,\dots,d-1)$$

and $\sum_{k=0}^{d-1}|c_k|\le 1$. Then $\sum_{k=0}^{d_1}c_kU_k=I_H$ if and only if $\sum_{k=0}^{d-1}|c_k|=1$ and $U_k=e^{-i\arg c_k}I_H$ $(0\le k\le d-1)$.

Theorem 4.25 *The identity I_H is an extreme point of $RAGQG(H)$.*

Remark 4.26 $\sum_{k=0}^{d-1}c_kU_k=I_H$ with $\sum_{k=0}^{d-1}|c_k|=1$ does not imply $U_k=I_H(k=0,1,2,\dots,d-1)$.

Theorem 4.27 *The set* $\mathrm{Ext}(RAGQG(H))$ *of all extreme points of* $RAGQG(H)$ *is* $U(H)$, *i.e.*, $\mathrm{Ext}(RAGQG(H)) = U(H)$.

5 Fixed-Point Duality Quantum Search Algorithms

The unsorted database search problem is a benchmark for computing [19]. To find a marked item from an unsorted database of N items, a classical computer requires $O(N)$ steps. A quantum computer requires $O(\sqrt{N})$ steps using the Grover algorithm [20] or an improved algorithm with 100% successful rate [21]. By introducing classical parallelism, the problem can be further speeded up modestly. Using the Brüschweiler algorithm [22], $O(\ln N)$ steps is required to find the marked state. Using the Xiao-Long algorithm, one needs only a single query to find the marked state [23]. However this speedup is achieved at the cost of more computing resources. Namely now there are $O(N)$ quantum computers working in parallel. In general with N_2 quantum computers working in parallel, the number of queries required to find the marked state is $O(\sqrt{N/N_2})$ in a parallelized quantum computing [24]. Though these algorithms achieve speedup by using more resources, they are still useful in ensemble quantum computers such as liquid nuclear magnetic resonance [25].

Two fixed-point search algorithms, the N1 and N4 algorithms, are presented here. The N1 algorithm was given in [1] and [2]. It finds a marked state from an unsorted database with N items in $O(N)$ steps. This algorithm does not speed up compared to classical algorithms, because it uses the same amount of queries as that in the classical search algorithm. However, it uses much less qubit resource, $\log_2 N$ as compared to $N \log_2 N$ in classical computing. Furthermore, it is faster than the fixed search algorithm given recently by Grover [26] and Li et al. [27]. In these fixed-point search algorithm, the number of queries is $O(3^{\log_2 N})$. The N4 algorithm uses only $N/4$ steps and it is the fastest fixed-point search algorithm up to date.

5.1 The N1 Duality Quantum Search Algorithm

The N1 duality search algorithm [2] is as follows.

(1) Prepare the state of the duality computer in the equally distributed state,

$$|\psi_0\rangle = \sqrt{\frac{1}{N}}(|0\rangle + \cdots + |\tau\rangle + \cdots + |N-1\rangle), \tag{26}$$

where τ is the marked item we are searching for;

(2) Let the duality computer go through QWD, so that it divides the wave into two sub-waves

$$|\psi_u\rangle = \frac{1}{2\sqrt{N}}(|0\rangle + \cdots + |\tau\rangle + \cdots + |N-1\rangle), \tag{27}$$

$$|\psi_d\rangle = \frac{1}{2\sqrt{N}}(|0\rangle + \cdots + |\tau\rangle + \cdots + |N-1\rangle). \tag{28}$$

(3) Apply the query to the lower-path sub-wave, reverse the coefficients of all basis states $|i\rangle$ except the marked state $|\tau\rangle$, the lower sub-wave becomes

$$|\psi_d\rangle' = \frac{1}{2\sqrt{N}}(-|0\rangle + \cdots + |\tau\rangle - \cdots - |N-1\rangle). \tag{29}$$

No operation is applied to the upper-path sub-wave, it remains in state as in (27);

(4) Combine the sub-waves at the QWC, and the wave becomes

$$|\psi_f\rangle = \sqrt{\frac{1}{N}}|\tau\rangle; \tag{30}$$

(5) Make a read-out measurement, with probability $1/N$, a result of the measurement will be obtained, and the measured result is the solution τ. However with probability $(N-1)/N$, there will be no result. If there is no result to the measurement, repeat the process again. After $O(N)$ times, there will be a result to the measurements, and the result is the marked state τ.

The query can be implemented using $O(\log_2 N)$ number of qubits. As the size of the database N increases, the difficulty in constructing the query increases only logarithmically.

5.2 The N4 Duality Quantum Search Algorithm

Recently a novel duality quantum algorithm, the N4 algorithm [18], was designed. It finds a marked state in a fixed manner in $N/4$ steps. This is the fastest fixed-point search algorithm up to date.

The N4-algorithm starts from a direct product state of the database and auxiliary qubit

$$|\psi_{ini}\rangle = |0\rangle \otimes |\psi_0\rangle. \tag{31}$$

Initially, the auxiliary qubit is in $|0\rangle$ state, and the database is prepared in the evenly distributed state

$$|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle = \frac{1}{\sqrt{N}}(|0\rangle + \cdots + |\tau\rangle + \cdots + |N-1\rangle), \tag{32}$$

where $|\tau\rangle$ is the marked state that is being searched.

Here, we analyze one cycle of the search process. It contains five steps, namely

Step 1. Perform the unitary operation of query

$$U_\tau = I - 2|\tau\rangle\langle\tau| \tag{33}$$

on the database to reverse the coefficient of the marked state $|\tau\rangle$, we get state

$$|\psi_\tau\rangle = |\psi_0\rangle - \frac{2}{\sqrt{N}}|\tau\rangle. \tag{34}$$

Step 2. Construct a unitary operation

$$V = \begin{bmatrix} \sqrt{\frac{N}{2N-4}} & \sqrt{\frac{N-4}{2N-4}} \\ \sqrt{\frac{N-4}{2N-4}} & -\sqrt{\frac{N}{2N-4}} \end{bmatrix} \tag{35}$$

for the auxiliary qubit as the QWD gate. Let the duality computer go through QWD, and the whole wave function is divided into two sub-wave functions

$$|\psi\rangle = |\psi_u\rangle + |\psi_d\rangle, \tag{36}$$

where

$$|\psi_u\rangle = \sqrt{\frac{N}{2N-4}}|0\rangle \otimes \left(|\psi_0\rangle - \frac{2}{\sqrt{N}}|\tau\rangle\right), \tag{37}$$

and

$$|\psi_d\rangle = \sqrt{\frac{N-4}{2N-4}}|1\rangle \otimes \left(|\psi_0\rangle - \frac{2}{\sqrt{N}}|\tau\rangle\right). \tag{38}$$

Step 3. Applying the following gate operation on the upper slit, where the auxiliary qubit is in $|0\rangle$ state,

$$U_s = 2|\psi_0\rangle\langle\psi_0| - I, \tag{39}$$

we get

$$|\psi_u'\rangle = \sqrt{\frac{N}{2N-4}}|0\rangle \otimes \left(\frac{N-4}{N}|\psi_0\rangle + \frac{2}{\sqrt{N}}|\tau\rangle\right). \tag{40}$$

By reversing all coefficients of the sub-wave functions on the lower slit which corresponds to the auxiliary qubit in $|1\rangle$ state, we get

$$|\psi_d'\rangle = \sqrt{\frac{N-4}{2N-4}}|1\rangle \otimes \left(-|\psi_0\rangle + \frac{2}{\sqrt{N}}|\tau\rangle\right). \tag{41}$$

Step 4. Perform V^+ on the auxiliary qubit which acts as the QWC gate. Upon this, the whole wave function becomes

$$|\psi_f\rangle = \frac{2}{\sqrt{N}}|0\rangle|\tau\rangle + \sqrt{\frac{N-4}{N}}|1\rangle|\psi_0\rangle. \tag{42}$$

Step 5. Make a read-out measurement to the auxiliary qubit. It is easy to see the marked item $|\tau\rangle$ will be found with certainty when we get $|0\rangle$ state. If the measurement result is $|1\rangle$ state, we can flip the auxiliary qubit to $|0\rangle$ state by a σ_x unitary operation, and then do the search process again until the marked state is obtained. The probability for obtaining the marked state is $4/N$. By detailed calculation, the expectation of the query numbers is found to be $N/4$. It is faster than Grover's fixed-point quantum algorithm [26], and the duality quantum N1-algorithm [1].

Because it allows all linear bounded operators, duality quantum computing may provide a bridge between classical computing and quantum computing. For example, some classical factorization algorithms can be translated into duality computing algorithm [15]. Though some of these "translated" algorithms may not gain speed-up in terms of the number of steps, it is still interesting because they use much less qubit resource as compared to computing in a classical computer. It is anticipated that most of the classical algorithms can be translated into quantum algorithms through the duality mode. This is very important because if quantum computers are constructed in the future, then one can perform both quantum algorithms and classical algorithms simultaneously on the same quantum computer. This is better than having one quantum computer and one classical computer at the same time and switching the working between the two computers constantly.

6 Summary and Perspectives

We have reviewed briefly the duality quantum computing. In a duality computer, quantum wave can be divided and recombined. Different computing gate operations can be performed at the different paths, a property that called the duality parallelism. This enables us to perform computation using not only products of unitary operations, but also linear combinations of unitary operations, which is called the duality gates or the generalized quantum gates. This provides duality parallelism which may outperform quantum parallelism in quantum computer.

The duality computer can be simulated by a quantum computer with just an extra qudit that labels the slits of the duality computer. The divider and combiner operations are two crucial elements of operations in duality computing and they are realized in a quantum computer by controlled operations.

It is likely that the duality computer can be used as a bridge to transform classical algorithms in to quantum computing algorithms. Though they may not gain speedup, they have used much less qubit resource.

Open questions remain in duality computing. One important question is what is the computing power of a duality computer. What can be or can not be done in a duality computer. What is the implication of general quantum gate for the computability in computer science? The simulation of open quantum systems is also an interesting issue.

Acknowledgements This work was supported by the National Natural Science Foundation of China Grant Nos. (10775076, 10874098), the National Basic Research Program of China (2006CB 921106), the Specialized Research Fund for the Doctoral Program of Education Ministry of China.

References

1. Long, G.L.: Commun. Theor. Phys. **45**, 825–844 (2006); Also see arXiv:quant-ph/0512120. It was briefly mentioned in an abstract (5111-53) (Tracking No. FN03-FN02-32) submitted to SPIE conference "Fluctuations and Noise in Photonics and Quantum Optics" in 18 Oct 2002
2. Long, G.L., Liu, Y.: Commun. Theor. Phys. **50**, 1303–1306 (2008)
3. Long, G.L., Liu, Y., Wang, C.: Commun. Theor. Phys. **51**, 65–67 (2009)
4. Cao, H.X., Li, L., Chen, Z.L., et al.: Chin. Sci. Bull. **55**, 2122–2125 (2010). doi:10.1007/s11434-010-3221-5
5. Wang, Y.Q., Du, H.K., Dou, Y.N.: Int. J. Theor. Phys. **47**, 2268–2278 (2008)
6. Gudder, S.: Quantum Inf. Process. **6**, 37 (2007)
7. Long, G.L.: Quantum Inf. Process. **6**(1), 49–54 (2007)
8. Gudder, S.: Int. J. Theor. Phys. **47**, 268–279 (2008). Also http://www.math.du.edu/data/preprints/m0611.pdf
9. Du, H.K., Wang, Y.Q., Xu, J.L.: J. Math. Phys. **49**, 013507 (2008)
10. Zhang, Y., Cao, H.X., Li, L.: Sci. China Phys. Mech. Astron. **53**, 1878–1883 (2010)
11. Long, G.L., Liu, Y.: Front. Comput. Sci. China **2**, 167–178 (2008)
12. Long, G.L., Liu, Y.: Prog. Phys. **28**, 410–431 (2008) (in Chinese)
13. Li, C.Y., Li, Junlin: Commun. Theor. Phys. (Beijing, China) **53**, 75–77 (2010)
14. Liu, Y., Zhang, W.H., Zhang, C.L., Long, G.L.: Commun. Theor. Phys. **49**, 107–110 (2008)
15. Wang, W.Y., Shang, B., Wang, C., Long, G.L.: Commun. Theor. Phys. **47**, 471–473 (2007)
16. Zou, X.F., Qiu, D.W., Wu, L.H., Li, L.J., Li, L.Z.: Quantum Inf. Process. **8**, 37–50 (2009)
17. Chen, Z.L., Cao, H.X.: Int. J. Theor. Phys. **48**, 1669–1671 (2010)
18. Hao, L., Li, D., Long, G.L.: Sci. China Phys. Mech. Astron. **53**, 1765–1768 (2010)
19. Long, G.L., Liu, Y.: Front. Comput. Sci. China **1**, 247–271 (2007) (review article)
20. Grover, L.: A fast quantum mechanical algorithm for database search. In: Proc. 28th Annual ACM Symposium on Theory of Computing, pp. 212–219. ACM, New York (1996)
21. Long, G.L.: Phys. Rev. A **64**, 022307 (2001)

22. Bruüschweiler, R.: Phys. Rev. Lett. **85**, 4815 (2000)
23. Xiao, L., Long, G.L.: Phys. Rev. A **66**, 052320 (2002)
24. Long, G.L., Xiao, L.: Phys. Rev. A **69**, 052303 (2004)
25. Long, G.L., Xiao, L.: J. Chem. Phys. **119**, 8473–8481 (2003)
26. Grover, L.K.: Phys. Rev. Lett. **95**, 150501 (2005)
27. Li, D.F., et al.: Phys. Lett. A **362**, 260–264 (2007)