CHIN.PHYS.LETT. Vol. 18, No. 2 (2001) 166

A Universal Quantum Network—Quantum Central Processing Unit *

WANG An-Min(王安民)[1,2]
[1]Laboratory of Quantum Communication and Quantum Computing
[2]Department of Modern Physics, University of Science and Technology of China, Hefei 230027

(Received 16 October 2000)

A new construction scheme of a universal quantum network which is compatible with the known quantum gate-assembly schemes is proposed. Our quantum network is standard, easy-assemble, reusable, scalable and even potentially programmable. Moreover, we can construct a whole quantum network to implement the general quantum algorithm and quantum simulation procedure. In the above senses, it is a realization of the quantum central processing unit.

PACS: 03. 67. Lx, 89. 80. +h, 03. 65. Bz

The quantum computer[1,2] has attracted considerable attention because it can speed up computation greatly, and even exponentially, as compared with a classical computer, for example, in factorization of a large number[3] and search for unstructured data.[4] A central part of the quantum computer is the quantum network. As is well known, a universal quantum network can be constructed by a set of elementary gates[5] in principle. However, at present, knowledge of the whole quantum networks for the main known quantum algorithms is not complete, and the quantum network for simulating Schrödinger equation has not been found. This is because, from the scheme of Barenco and co-workers, one does not know clearly how to assemble and scale up the quantum networks for a product of a series of quantum computing steps and a summation for a set of quantum computing parts. Therefore, knowing how to construct a whole quantum network in a practical situation is still extremely important. In order to solve this problem, we propose a new construction scheme for a universal quantum network in this letter. Our universal quantum network can carry out a general quantum computing task just like a quantum central processing unit (QCPU). Moreover, it is standard, easy-assemble, reusable and scalable, even programmable.[6] Consequently, it is a realization of QCPU. In fact, as long as it is indeed so, one can indeed truly make, at least in theory, a quantum computer.

To arrive at the above goals, we first introduce an auxiliary qubit A prepared in $|0\rangle_A$ and define the universal quantum network for a transformation U acting on k qubits as

$$Q(U) = \prod_{m,n=0}^{2^k-1} \exp\{(U_{mn}|m\rangle\langle n| \otimes I_A) \cdot C^\dagger\}, \quad (1)$$

where I_R and I_A are the identity matrices in the register space and the auxiliary qubit space respectively, and

$$C^\dagger = I_R \otimes c_A^\dagger = I_R \otimes |1\rangle_{AA}\langle 0| \quad (2)$$

is the so-called "Jointer" whose action is to put all of the factors such as $\exp[U_{mn}|m\rangle\langle n|]$ into a product form. These factors are called the elements of quantum circuit. If the graphics rules for these are given out, the picture of the quantum network $Q(U)$ can be easily drawn. It is worth emphasizing that there is an essential difference between the classical gate and the quantum gate. This is just that the classical gate is always to carry out a determined operation, but the quantum gate can carry out a kind of operations. For example, the quantum rotation gate can rotate a state to any angle and then it needs one parameter ϕ or $e^{i\phi}$ to determine its operation. So are the elements of quantum circuit.

Compared with the known schemes, the most important two new features of $Q(U)$ are

$$Q(U_1 + U_2 + \cdots + U_r) = Q(U_1)Q(U_2)\cdots Q(U_r), \quad (3)$$

$$Q(U_1U_2\cdots U_r) = I + C^\dagger \left(\prod_{j=1}^{r} CQ(U_j)\right) CC^\dagger, \quad (4)$$

where $I = I_R \otimes I_A$, and

$$C = I_R \otimes c_A = I_R \otimes |0\rangle_{AA}\langle 1| \quad (5)$$

is the so-called "Connector" that is used to prepare a transformed state so that this prepared state can be used in the next successive transformation. Furthermore, note that there are the relations $c_A^2 = c_A^{\dagger 2} = 0$ and $c_A c_A^\dagger + c_A^\dagger c_A = I_A$. Thus c_A and $c_A^\dagger$ can be thought of as the fermionic annihilate and create operators, respectively, in the auxiliary qubit. From this, the auxiliary system might be extended to a larger system beyond a qubit if one can easily implement a nilpotent transiting operator by it. Obviously, Eq.(3) is a quantum network for a summation of a set of quantum computing parts. In order to put the quantum network for a product of a series of quantum computing steps into a form of full multiplication, we use two registers respectively to the input state space and

*Supported by the National Natural Science Foundation of China under Grant No. 69773052, and the Fellowship of Chinese Academy of Sciences.
©2001 Chinese Physical Society and IOP Publishing Ltd

the output state space including one auxiliary qubit. Then we define

$$\overline{Q}(U_1U_2\cdots U_r)=(I_R)_{\rm in}\otimes\left[C^\dagger\left(\prod_{j=1}^{r}CQ(U_j)\right)CC^\dagger\right]_{\rm out}, \tag{6}$$

while the initial state is now prepared into $(|\Psi(t)\rangle)_{\rm in}\otimes(|\Psi(t)\rangle\otimes|0\rangle_A)_{\rm out}$. Therefore, in our scheme, a whole quantum network is constructed *via* the so-called "motherboard" with many "slots". A slot is an interspace between a pair of connectors and so a motherboard is made of some connectors. The quantum networks for a series of quantum computing steps, just like some "plug-in boards", are inserted into these slots, and the quantum networks for a set of quantum computing parts, even like some "building blocks", are put together directly. All of them are very easily assembled and scaled as a whole quantum network.

Obviously, $Q(U)$ is universal and Eq.(1) is an alternative for the formula of Reck *et al.*[7] since it keeps the advantages such as the product form, only involving two states (not qubit) and a close relation with the elementary gates etc. For example, the simplest is a quantum network for a transformation S of a single quantum state: $|n\rangle\longrightarrow {\rm e}^{{\rm i}\alpha_n}|n\rangle, |m\rangle(m\neq n)\longrightarrow|m\rangle$

$$Q(S)=\exp\{C^\dagger\}\exp\{[({\rm e}^{{\rm i}\alpha_n}-1)|n\rangle\langle n|\otimes I_A]\cdot C^\dagger\}, \tag{7}$$

where $\exp\{C^\dagger\}=Q(I_R)$ is a quantum subnetwork for an identity gate and we construct $Q(S)$ by decomposing this transformation into $I+({\rm e}^{{\rm i}\alpha_n}-1)|n\rangle\langle n|$. In particular, when $\alpha_n=\pi$, this transformation is a reflection of $|n\rangle$, which can be used in Grover's algorithm. Another example is a quantum subnetwork for $U(i)=I_1\otimes I_2\otimes\cdots\otimes U_i\otimes\cdots\otimes I_k$

$$Q(U(i))=\exp\{(U(i)\otimes I_A)\cdot C^\dagger\}. \tag{8}$$

For a controlled gate $U_{\rm control}=|0\rangle\langle0|\otimes I_2+|1\rangle\langle1|\otimes U$, we have

$$\begin{aligned}Q(U_{\rm control}) &= \exp\{(|0\rangle\langle0|\otimes I_2\otimes I_A)C^\dagger\}\\ &\quad\cdot\exp\{(|1\rangle\langle1|\otimes U\otimes I_A)C^\dagger\}.\end{aligned} \tag{9}$$

When U is a NOT gate, it is a quantum network for the controlled NOT. Likewise, we can write down a quantum network for the Toffoli gate (controlled–controlled–NOT), in which the third qubit experiences NOT if and only if the others are in the state $|1\rangle$:

$$\begin{aligned}Q({\rm Toffoli}) &= \exp\{C^\dagger\}\exp\{-(|1\rangle\langle1|\otimes|1\rangle\langle1|\otimes I\\ &\quad\otimes I_A)C^\dagger\}\exp\{(|1\rangle\langle1|\otimes|1\rangle\langle1|\\ &\quad\otimes N\otimes I_A)C^\dagger\},\end{aligned} \tag{10}$$

since we can decompose $U_{\rm Toffoli}=I-|1\rangle\langle1|\otimes|1\rangle\langle1|\otimes I+|1\rangle\langle1|\otimes|1\rangle\langle1|\otimes N$, where N is a NOT gate. Therefore, all the elementary quantum gates can be written down by our quantum networks. This implies that our construction scheme is compatible with the known quantum gate-assembly schemes because as soon as we have obtained an expression of a quantum computation in terms of a set of the elementary quantum gates, we can first construct the quantum subnetworks for these elementary quantum gates and then easily assemble them into a whole quantum network by virtue of the properties of our quantum network.

Furthermore, every factor in $Q(U)$ is an exponential form which may be easy to implement in experiment. Even our scheme can be applied to an irreversible and/or non-unitary transformation.

It is easy to see that $Q(U)$ acting on $|\Psi\rangle\otimes|0\rangle_A$ just carries out a general quantum computation:

$$Q(U)|\Psi\rangle\otimes|0\rangle_A=|\Psi\rangle\otimes|0\rangle_A+|\Psi\rangle'\otimes|1\rangle_A, \tag{11}$$

and its reversible operation reads

$$Q^{-1}(U)=\prod_{m,n=0}^{k-1}\exp\{-(U_{mn}|m\rangle\langle n|\otimes I_A)C^\dagger\}. \tag{12}$$

Thus, two project measurements,

$$D = C^\dagger C=I_R\otimes|1\rangle_{A\,A}\langle1|, \tag{13}$$

$$P = CC^\dagger=I_R\otimes|0\rangle_{A\,A}\langle0|, \tag{14}$$

result in an output state $|\Psi\rangle'\otimes|1\rangle_A$ and an input state $|\Psi\rangle\otimes|0\rangle_A$, respectively.

In mathematics, every element of quantum circuit is directly related to a natural basis $|m\rangle\langle n|$ of the operator in Hilbert space and a matrix element U_{mn} of the transformation matrix for a quantum computation. This implies that the parameters of the elements of the quantum circuit can be reset; that is, our quantum network is potentially programmable.[6] On the other hand, this feature also makes it possible for them be constructed by the elementary quantum gates.[8] In fact, it is easy to prove that $|m\rangle\langle n|$ can be written as a product of a general exchange transformation and a measurement $|n\rangle\langle n|$ from left or a measurement $|m\rangle\langle m|$ from right

$$|m\rangle\langle n|=E(m,n)|n\rangle\langle n|=|m\rangle\langle m|E(m,n), \tag{15}$$

where

$$E(m,n)=\begin{cases}\prod_{j=n}^{m-1}E(j+1,j), & (n<m)\\ \prod_{j=0}^{n-m-1}E(n-j-1,n-j), & (n>m)\\ I_R. & (n=m).\end{cases} \tag{16}$$

$$\begin{aligned}&E(m,m+1)=E(m+1,m)\\ &=\sum_{j=0;j\neq m,m+1}^{2^k-1}|j\rangle\langle j|+|m\rangle\langle m+1|+|m+1\rangle\langle m|.\end{aligned} \tag{17}$$

The order of product in Eq.(16) is arranged as left multiplication with index j increasing. It is clear

that the generalized exchange gate $E(m, m+1)$ for two neighbour basic states $|m\rangle$ and $|m+1\rangle$ is Hermian and unitary. It is easy to see that its action on $|m\rangle$ or $|m+1\rangle$ leads to their exchange and keeps the other basic states invariant. Note that for two qubits, $E(2,3)$ is a CNOT gate and $E(1,2)$ is a swapping gate.[9] While $E(m,n)$ is just an exchange transformation of arbitrary two states $|m\rangle$ and $|n\rangle$; that is, $E(m,n)|n\rangle = |m\rangle$ and $\langle m|E(m,n) = \langle n|$. Thus the universal quantum network for U is just defined by

$$Q(U) = \prod_{m,n=0}^{2^k-1} \exp\{(U_{mn}E(m,n)|n\rangle\langle n| \otimes I_A) \cdot C^\dagger\}. \tag{18}$$

The key point is the efficiency of a universal quantum network. It seems that a universal quantum network consisting of $2^k \times 2^k$ basic elements is the same as a classical computer in the use of computing resources. In fact, this is the price to be paid for universality. Because the basic elements of the quantum circuit only act on a branch (path) of the quantum data flow from its definition, $Q(U)$ needs $2^k \times 2^k$ basic elements in general. However, in practice, our construction is obtained in terms of the symmetries and physical features in a quantum computation. Therefore, many elements of the quantum circuit do not really appear. Quantum Fourier transformation[10] is an example.[11] Generally speaking, the number of elements of a realization of QCPU for the transformation U is at least equal to the number of the inequality matrix elements in U, except for zero.

Our universal quantum network proposed in this letter leads to a general design principle for a quantum algorithm and quantum simulation. That is, we ought to find such a suitable and optimized decomposition that the quantum subnetworks for its components can be as effectively and easily constructed as possible. The process of decomposition can continue until our aim is served. In principle, this is possible if a quantum computation can be effectively carried out. In order to do so, we need to use the fundamental laws of physics, especially the principles and features of quantum mechanics, for example, the coordinate system choice, representation transformation, picture scheme and quantum measurement theory, if we think that a quantum computing task is a physical process. Moreover, we have to use the symmetry properties of every computing part and/or step U^i as far as possible, such as the direct product decomposition, the transposing invariance $U^i_{nm} = U^i_{mn}$ or the row equality $U^i_{mn} = U^i_{m0}$ for all n or the line equality $U^i_{mn} = U^i_{0n}$ for all m as well as make U_i with zero elements and equal elements as many as possible. In general, we can always find some symmetries through decomposing U into a summation $U_1 + U_2 + \cdots + U_n$ and/or a product $U_1 U_2 \cdots U_n$. In this letter, we have obtained the whole quantum networks for Shor's algorithm, Grover's algorithm and simulating Schrödinger equation in general. This means that our universal quantum network can generally describe the known main results in quantum computation.

In the above sense, we have designed a universal quantum network which can carry out general quantum computing; that is, a realization of QCPU is given out. Obviously, our construction scheme can keep the advantages in the known schemes. More importantly, our method simplifies the construction for a universal quantum network in terms of the elementary quantum gates and standardizes the process of construction as a procedure; that is, from the elementary quantum gates to the elements of quantum circuit, again to the quantum subnetworks for the quantum computing parts U_i ($U = U_1 + U_2 + \cdots + U_r$) and/or the quantum computing steps U_i ($V = V_1 V_2 \cdots V_r$), and finally to a whole quantum network. Moreover, each step in this procedure is facile and can be determined. The significance of simplification and standardization is to provide not only the facility in engineering, but also the realizability in an effective construction. Furthermore, our construction provides a way to reuse and update a quantum subnetwork as well as the potential possibility to program a quantum network.

I would like to thank Artur Ekert for his great help and for his hosting my visit to Centre of Quantum Computing in Oxford University. I also thank Markus Grassl for his helpful comments.

References

[1] Feynman R P 1982 *Int. J. Theor. Phys.* **21** 467
[2] Deutsch D 1985 *Proc. Roy. Soc. Lond. A* **400** 97
[3] Shor P W 1994 in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser, (Los Alamitos, CA: IEEE Computer Society Press) p 20
Shor P W 1997 *SIAM Journal of Computation*, **26** 1484
[4] Grover L K 1997 *Phys. Rev. Lett.* **79** 325; quant-ph/9605034
[5] Barenco A et al *Elementary gates for quantum computing*, quant-ph/9503016
[6] Nielsen M A and Chuang I L 1997 *Phys. Rev. Lett.*, **79** 321
[7] Reck M, Zeilinger A, Bernstein H J and Bertani P 1994 *Phys. Rev. Lett.* **73** 58
[8] Shor P W 1996 in *Proceedings of the 37th Annual Symposium on the Foundations of Computer Science* (Los Alamitos, CA: IEEE Computer Society Press) p 15
[9] Loss D and DiVincenzo D P 1998 *Phys. Rev. A* **57** 120
[10] Ekert A 1998 *Phys. Scripta* **T76** 218; Cleve R, Ekert A, Macchiavello C and Mosca M 1998 *Proc. Roy. Soc. London. A* **454** 339
[11] Wang A M *New Construction of a Universal Quantum Network and Its Applications*, preprint quant-ph/0006122