TITLE:

Phase-creation algorithm to solve and extended Deutsch problem with an implementation on an NMR quantum computer (Analytical Study of Quantum Information and Related Fields)

AUTHOR(S):

Ozawa, Hiroshi

CITATION:

Ozawa, Hiroshi. Phase-creation algorithm to solve and extended Deutsch problem with an implementation on an NMR quantum computer (Analytical Study of Quantum Information and Related Fields). 数理解析研究所講究録 2002, 1266: 114-124

ISSUE DATE:

2002-05

URL:

http://hdl.handle.net/2433/42102

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録 1266 巻 2002 年 114-124

Phase-creation algorithm to solve an extended Deutsch problem with an implementation on an NMR quantum computer

Hiroshi Ozawa

Information Technology Center, The University of Tokyo, Tokyo 113-0033, Japan

(小澤 宏 東京大学情報基盤センター)

The Deutsch-Jozsa algorithm to implement an f-controlled-NOT transformation on a quantum computer was generalized to create arbitrary phases. This phase-creation algorithm was applied to solve an extended Deutsch problem for a function that maps $\{0,1\}^n$ to $\{0,1\}^m$. Implementation of the algorithm on an NMR quantum computer is discussed.

1 Introduction

Quantum computation [1] is a rapidly growing field of research. A quantum computer [2] uses a set of two-state systems as quantum bits (qubits), and executes a computation by a sequence of unitary transformations on them; the desired useful information is extracted by measuring the final state of the qubits (or a subset of the qubits). After simple quantum logic gates have been tested successfully using cold trapped ions [3], several groups proposed the use of nuclear magnetic resonance (NMR) of bulk quantity molecules [4,5]. The first quantum algorithm that was implemented on any quantum computer was Deutsch-Jozsa algorithm [6] to solve Deutsch problem [2], and these implementations employed NMR.

Deutsch problem, generalized by Deutsch and Jozsa [6], in its simplest form, is stated as follows: "For an unknown given Boolean function $f(x)$,

$$f(x): \quad \{0,1\}^n \mapsto \{0,1\}\,, \tag{1}$$

determine whether it is constant or balanced by evaluating it only once," where balanced means equal number of variables for all function values. The original Deutsch problem corresponds to the case of $n = 1$.

To evaluate $f(x)$ on a quantum computer, some unitary transformation $U_{f(x)}$ is necessary, and the Deutsch-Jozsa algorithm [Eq. (3)] uses an f-controlled-NOT transformation, which is defined by

$$\begin{aligned} &|x\rangle\,|y\rangle \xrightarrow{U_{f(x)}} |x\rangle\,|y \oplus f(x)\rangle\,, \\ &\qquad x \in \{0,1\}^n = 0,1,\ldots,2^n-1\,, \\ &\qquad y,\, f(x) \in \{0,1\}^m = 0,1,\ldots,2^m-1\,, \end{aligned} \tag{2}$$

where the first qubits (quantum register) are the control and the second qubits are the target. If we set the target qubit to a one-qubit superposition state, $(|0\rangle - |1\rangle)/\sqrt{2}$, we have

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{U_{f(x)}} (-1)^{f(x)}\,|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}\,. \tag{3}$$

Using this Deutsch-Jozsa algorithm and the Hadamard transformation H defined by

$$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,, \qquad |1\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}}\,, \tag{4}$$

we obtain

$$|0\rangle\,|1\rangle \xrightarrow{H^2} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}\,, \tag{5}$$

$$\xrightarrow{U_{f(x)}} \frac{(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}\,, \tag{6}$$

$$= (-1)^{f(0)} \frac{|0\rangle + (-1)^{f(0)\oplus f(1)}\,|1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}\,, \tag{7}$$

$$\xrightarrow{H^2} (-1)^{f(0)}\,|f(0) \oplus f(1)\rangle\,|1\rangle\,. \tag{8}$$

Equations (5)−(8) show that, stating from the state $|0\rangle|1\rangle$, only one function evaluation suffices to obtain the state $|f(0) \oplus f(1)\rangle$ for the control, which is $|0\rangle$ ($|1\rangle$) when $f(x)$ is constant (balanced), solving the $n = 1$ Deutsch problem. This may be the simplest example of quantum parallelism [2], an important aspect of the power of quantum computers.

Recently, Collins, Kim, and Holton (CKH) [7] showed for the f-controlled-NOT transformation that, if the target register in the input is restricted to the subspace spanned by $(|0\rangle - |1\rangle)/\sqrt{2}$, then there is no entanglement between the control and the target registers in the output, the state of the target does not change; therefore, the target can be redundant. In this refined CKH algorithm, the transformation $U_{f(x)}$ is simply given by

$$|x\rangle \xrightarrow{U_{f(x)}} (-1)^{f(x)} |x\rangle \,. \tag{9}$$

Of course, this algorithm is experimentally applicable when we can directly create the phase $(-1)^{f(x)} = \pm 1$ for the state $|x\rangle$.

In this work we will give an algorithm to create arbitrary phases $e^{i\pi\phi(x)}$, rather than only ± 1 [Eqs. (3) and (9)], and apply this algorithm to solve an extended Deutsch problem where the function maps $\{0,1\}^n$ to $\{0,1\}^m$.

2 Phase-creation algorithm

Recalling that the input state for the target qubit of the Deutsch-Jozsa algorithm is the Hadamard transform of $|1\rangle$ [Eqs. (3)−(5)], and that the Hadamard transformation is the simplest (modulo 2) case of a quantum Fourier transformation [8], we will replace this qubit (the target) by an m-qubit quantum register, $|u\rangle$, which is the quantum Fourier transform modulo 2^m of $|00\ldots01\rangle$:

$$|\overbrace{00\ldots01}^{m}\rangle \xrightarrow{F_{2^m}} |u\rangle = \frac{1}{\sqrt{2^m}} \sum_{y\in\{0,1\}^m} e^{i2\pi y/2^m} |y\rangle \,. \tag{10}$$

Note that $|u\rangle$ is in fact unentangled [8], and is given by

$$|u\rangle = \frac{1}{\sqrt{2^m}} (|0\rangle + e^{i2\pi/2} |1\rangle) \otimes (|0\rangle + e^{i2\pi/2^2} |1\rangle) \otimes \cdots \otimes (|0\rangle + e^{i2\pi/2^m} |1\rangle) \,. \tag{11}$$

Next, extending the definition of f-controlled-NOT transformation [Eq. (2)], we will define a unitary transformation $U_{\phi(x)}$ by a state-shift operation on each state $|y\rangle$ of the target register $|u\rangle$; y is shifted by an integer value $2^{m-1}\phi(x)$, which is determined by the state $|x\rangle$ of the control register:

$$|x\rangle\,|y\rangle \xrightarrow{U_{\phi(x)}} |x\rangle\,|y - 2^{m-1}\phi(x) \bmod 2^m\rangle\,,$$

$$x \in \{0,1\}^n\,, \qquad y \in \{0,1\}^m\,, \tag{12}$$

$$\phi(x) \in \frac{1}{2^{m-1}}\{0,1\}^m = 0, \frac{1}{2^{m-1}}, \frac{2}{2^{m-1}}, \cdots, \frac{2^m-1}{2^{m-1}}\,.$$

Using Eqs. (10) and (12), we obtain

$$|x\rangle\,|u\rangle = \frac{1}{\sqrt{2^m}}\,|x\rangle \sum_{y\in\{0,1\}^m} e^{i2\pi y/2^m}\,|y\rangle\,, \tag{13}$$

$$\xrightarrow{U_{\phi(x)}} \frac{1}{\sqrt{2^m}}\,|x\rangle \sum_{y\in\{0,1\}^m} e^{i2\pi y/2^m}\,|y - 2^{m-1}\phi(x) \bmod 2^m\rangle\,, \tag{14}$$

$$= \frac{1}{\sqrt{2^m}}\,e^{i\pi\phi(x)}\,|x\rangle \sum_{y\in\{0,1\}^m} e^{i2\pi[y/2^m - \phi(x)/2]} \times |y - 2^{m-1}\phi(x) \bmod 2^m\rangle\,, \tag{15}$$

$$= e^{i\pi\phi(x)}\,|x\rangle\,|u\rangle\,, \tag{16}$$

which shows that state-shift operations on states $|y\rangle$ of the target register $|u\rangle$ result in the creation of a phase $e^{i\pi\phi(x)}$ for the control register $|x\rangle$, because of the property of the Fourier-transformed state of the target. (When we use a target register which is the Fourier transform of $|a\rangle = |a_{m-1}a_{m-2}\ldots a_0\rangle$ where $a_i \in \{0,1\}$ and $a = 2^{m-1}a_{m-1} + 2^{m-2}a_{m-2} + \cdots + 2^0 a_0$, we obtain a phase $e^{i\pi a\phi(x)}$ for the control register $|x\rangle$.) This is an explicit expression of what Cleve *et al.* [9] proposed for the creation of arbitrary interference patterns. If we put $m = 1$ in Eqs. (10)–(16), we obtain the Deutsch-Jozsa algorithm [Eq. (3)], and if we put $n \geq 2$ and $m = 2$, we obtain four phases, 1, i, -1, and $-i$, for $|x\rangle$, corresponding to $\phi(x) = 0$, $\frac{1}{2}$, 1, and $\frac{3}{2}$, respectively. Note that since $2^{m-1}\phi(x)$ is an integer, the smallest phase created is $e^{i\pi/2^{m-1}}$.

We see in Eqs. (13)–(16) that in the output the target register $|u\rangle$ does not entangle with the control register $|x\rangle$, and that the state of the target register does not change by the transformation $U_{\phi(x)}$. Therefore, just as in

the CKH algorithm, the target register can also be redundant in this phase-creation algorithm. If we can experimentally create the phase $e^{i\pi\phi(x)}$ for the state $|x\rangle$, this algorithm is simply described as

$$|x\rangle \xrightarrow{U_{\phi(x)}} e^{i\pi\phi(x)}|x\rangle . \tag{17}$$

3 An extended Deutsch problem

Here we give an extension of the Deutsch problem: "For an unknown given 2^m-valued function $\phi(x)$,

$$\phi(x): \quad \{0,1\}^n \mapsto \frac{1}{2^{m-1}}\{0,1\}^m , \qquad n \geq m , \tag{18}$$

determine whether it is constant or balanced by evaluating it only once." In this problem, the numbers of constant and balanced functions are 2^m and $2^n!/(2^{n-m}!)^{2^m}$, respectively.

Following the procedure given by Deutsch and Jozsa [6] to solve the Deutsch problem, where $n \geq 2$ [Eq. (1)], we can prove that this extended problem, where $n \geq m \geq 2$, can also be solved if we use the phase-creation algorithm, as follows.

Walsh transformation W for an n-qubit state $|v\rangle$ is given by

$$|v\rangle \xrightarrow{W} \frac{1}{\sqrt{2^n}} \sum_{w\in\{0,1\}^n} (-1)^{\vec{v}\cdot\vec{w}}|w\rangle , \qquad v, w \in \{0,1\}^n , \tag{19}$$

where $\vec{v}\cdot\vec{w}$ is the sum modulo 2 of the bitwise products of v and w. This transformation is equivalent to performing a one-qubit Hadamard transformation on each of the n qubits individually. When we apply the phase-creation transformation to an equally weighted superposition state $\sum|x\rangle$, which is produced by the Walsh transformation of an n-qubit state $|00\ldots0\rangle$, and apply another Walsh transformation, we obtain

$$|\overbrace{00\ldots0}^{n}\rangle \xrightarrow{W} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle , \tag{20}$$

$$\xrightarrow{U_{\phi(x)}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} e^{i\pi\phi(x)} |x\rangle \,, \tag{21}$$

$$\xrightarrow{W} \frac{1}{2^n} \sum_{x,w\in\{0,1\}^n} e^{i\pi[\phi(x)+\vec{x}\cdot\vec{w}]} |w\rangle \,. \tag{22}$$

The amplitude of the state $|00\ldots0\rangle$ in the output is

$$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} e^{i\pi\phi(x)} \,, \tag{23}$$

which is nonzero (e.g., either 1, i, -1, or $-i$ for the case of $m = 2$) if $\phi(x)$ is constant, whereas it is zero if $\phi(x)$ is balanced.

4 Discussion

When we solve the extended Deutsch problem, we create phases $e^{i\pi\phi(x)}$ for equally weighted superposition states $|x\rangle$ [Eqs. (20) and (21)]. Experimentally this process can be carried out either indirectly using an additional register $|u\rangle$ [Eqs. (13)–(16)], or, if possible, directly without using it [Eq. (17)]. The former method corresponds to what was used in the NMR quantum computer experiments to solve the $n = 1$ [10,11] and 2 [12] Deutsch problems using the Deutsch-Jozsa algorithm, while the latter corresponds to what was used to solve the $n = 2$ [13] and 3 [14–16] problems using the CKH algorithm. In these experiments where the phases to be created are 1 or -1, the CKH algorithm is experimentally applicable in NMR [13–16], and this algorithm allows the size of a quantum computer to be reduced by one spin than when using the Deutsch-Jozsa algorithm. (The experiments of Refs. [12] and [14–16] were carried out on three-spin systems.)

To see that this also holds for the extended Deutsch problem where the phases are arbitrary, let us consider the simplest case of $n = m = 2$, where four functions are constant and 24 functions are balanced. Two typical examples of the balanced functions are

$$\phi_1(00) = 0\,, \quad \phi_1(01) = \tfrac{1}{2}\,, \quad \phi_1(10) = 1\,, \quad \phi_1(11) = \tfrac{3}{2}\,, \tag{24}$$

$$\phi_2(00) = 0\,, \quad \phi_2(01) = \tfrac{1}{2}\,, \quad \phi_2(10) = \tfrac{3}{2}\,, \quad \phi_2(11) = 1\,. \tag{25}$$

When we apply the transformation $U_{\phi(x)}$ of these functions to the superposition state which is the Walsh transform of $|00\rangle$ [Eqs. (20) and (21)], we obtain either an unentangled state or a superposition state:

$$(|0\rangle - |1\rangle) \otimes (|0\rangle + i\,|1\rangle) \quad \text{for } U_{\phi_1}\,, \tag{26}$$

$$|00\rangle + i\,|01\rangle - i\,|10\rangle - |11\rangle \quad \text{for } U_{\phi_2}\,. \tag{27}$$

The matrices for these transformations are given by

$$U_{\phi_1} = \begin{bmatrix} 1 & & & \\ & i & & \\ & & -1 & \\ & & & -i \end{bmatrix} = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & \\ & i \end{bmatrix}, \tag{28}$$

$$U_{\phi_2} = \begin{bmatrix} 1 & & & \\ & i & & \\ & & -i & \\ & & & -1 \end{bmatrix} = \begin{bmatrix} 1 & & & \\ & i & & \\ & & i & \\ & & & 1 \end{bmatrix} \cdot \left(\begin{bmatrix} 1 & \\ & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \right) . \tag{29}$$

If we note [17] that the single-spin operators in the Cartesian basis are defined by

$$I_x = \frac{1}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad I_y = \frac{1}{2}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad I_z = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{30}$$

and that the following expressions hold for their exponential operators with the second spin denoted by S,

$$e^{i\theta I_\alpha} = \cos\frac{\theta}{2}\,\mathbf{1} + i\,2\,\sin\frac{\theta}{2}\,I_\alpha\,, \qquad \alpha = x, y, z\,, \tag{31}$$

$$e^{i\theta I_z S_z} = \cos\frac{\theta}{4}\,\mathbf{1} + i\,4\,\sin\frac{\theta}{4}\,I_z\,S_z\,, \tag{32}$$

we obtain

$$\begin{bmatrix} 1 & \\ & -1 \end{bmatrix} = i\,e^{-i\pi I_z} = i\,e^{-i\pi I_x}\,e^{-i\pi I_y}\,, \tag{33}$$

$$\begin{bmatrix} 1 & \\ & i \end{bmatrix} = \frac{1+i}{\sqrt{2}}\,e^{-i(\pi/2)I_z} = \frac{1+i}{\sqrt{2}}\,e^{-i(\pi/2)I_x}\,e^{-i(\pi/2)I_y}\,e^{i(\pi/2)I_x}\,, \tag{34}$$

$$\begin{bmatrix} 1 & & & \\ & i & & \\ & & i & \\ & & & 1 \end{bmatrix} = \frac{1+i}{\sqrt{2}}\,e^{-i\pi I_z S_z}\,. \tag{35}$$

These equations show that the transformations U_{ϕ_1} and U_{ϕ_2} (and also all other transformations) consist of terms of the forms $e^{\pm i\pi I_\beta}$, $e^{\pm i(\pi/2)I_\beta}$ $(\beta = x, y)$, and $e^{\pm i\pi I_z S_z}$ (up to the overall phases). This can be compared to the case of the Deutsch problem $(n = 2,\ m = 1)$, where transformations $U_{f(x)}$ consist of terms of the forms $e^{\pm i\pi I_\beta}$ and $e^{\pm i2\pi I_z S_z}$. In the case of $n = 3$, if we denote the third spin by K, the terms of $U_{f(x)}$ are of the forms $e^{\pm i\pi I_z}$, $e^{\pm i(\pi/2)I_z}$, $e^{\pm i\pi I_z S_z}$, and $e^{-i2\pi I_z S_z K_z}$ [13], where the last one is equivalent to

$$e^{-i(\pi/2)I_x}\,e^{-i\pi I_z K_z}\,e^{-i(\pi/2)I_y}\,e^{-i\pi I_z S_z}\,e^{i(\pi/2)I_y}\,e^{i\pi I_z K_z}\,e^{i(\pi/2)I_x}\,, \tag{36}$$

and, consequently, the terms of $U_{\phi(x)}$ are of the forms as small as $e^{\pm i(\pi/2^m)I_\beta}$ and $e^{\pm i(\pi/2^{m-1})I_z S_z}$.

In NMR, we can implement $e^{\pm i(\pi/2^k)I_\beta}$ $(k = 0, 1, \ldots)$ by an rf pulse $(\pm\pi/2^k)_\beta(I)$, i.e., an rf pulse to rotate spin I by an angle $\pm\pi/2^k$ around the β axis, where I is arbitrary. To implement $e^{-i(\pi/2^{k-1})I_z S_z}$ $(k = 0, 1, \ldots)$ where I and S are arbitrary, we make use of time evolution due to the spin-spin coupling between spins I and S, with the effects of all other spin-spin couplings and all Zeeman evolutions negated. For this implementation we use [18] the following property of the sequence of the type

$$(\pi)_x(I) - t - (\pi)_x(I)\,, \tag{37}$$

where t is the evolution time. Its effect on the Zeeman evolution of spin I is given by

$$e^{i\pi I_x}\, e^{i\omega_i t I_z}\, e^{i\pi I_x} = e^{-i\omega_i t I_z}\ . \tag{38}$$

This equation shows that the direction of time evolution is now reversed from plus to minus. Therefore, this sequence, when preceded by an evolution of the same time length, causes the cancellation of the Zeeman evolution of spin I during the first period. Likewise, the effect of the sequence of Eq. (37) on an evolution due to the spin-spin coupling between spins I and S is given by

$$e^{i\pi I_x}\, e^{-i2\pi J_{IS} t I_z S_z}\, e^{i\pi I_x} = e^{i2\pi J_{IS} t I_z S_z}\ , \tag{39}$$

which shows a similar effect of time inversion on spin-spin coupling evolutions. Using these properties, we see that $e^{-i(\pi/2^{k-1})I_z S_z}$ can be implemented by the the sequences

$$\tau/2 - (\pi)_x(I,S) - \tau/2 - (\pi)_x(I,S) \quad \text{when } n=2\ , \tag{40}$$

$$\begin{aligned}\tau/4 - (\pi)_x(I,S) - \tau/4 - (\pi)_x(I,S,K) - \tau/4 \\ -(\pi)_x(I,S) - \tau/4 - (\pi)_x(I,S,K) \quad \text{when } n=3\ ,\end{aligned} \tag{41}$$

$$\begin{aligned}&\tau/8 - (\pi)_x(I,S) - \tau/8 - (\pi)_x(I,S,K) - \tau/8 - (\pi)_x(I,S) - \tau/8 \\ &\quad -(\pi)_x(I,S,K,L) - \tau/8 - (\pi)_x(I,S) - \tau/8 - (\pi)_x(I,S,K) \\ &\quad -\tau/8 - (\pi)_x(I,S) - \tau/8 - (\pi)_x(I,S,K,L) \quad \text{when } n=4\ ,\end{aligned} \tag{42}$$

etc., where τ is the free precession period of length such that $2\pi J_{IS}\tau = \pi/2^{k-1}$, i.e., $\tau = 1/(2^k J_{IS})$, J_{IS} is the spin-spin coupling constant between spins I and S, and K and L denote the third and forth spins, respectively. Therefore, in NMR, we can directly create the phases $e^{i\pi\phi(x)}$ for the states $|x\rangle$ which are in equally weighted superpositions [Eqs. (20) and (21)]. This means that indirect phase creation to use an additional target register $|u\rangle$ [Eqs. (13)–(16)] is in practice unnecessary.

It should be noted, however, that when we do use the additional register for phase creation, the state-shift operations for the 2^m superposition states $|y\rangle$ of $|u\rangle$ [Eqs. (10) and (12)] can be implemented by a sequence of NOT and controlled-NOT operations on the qubits of $|u\rangle$ [19], and these operations are also executable in NMR for any number of spins [18]. To prepare the initial state $|00\ldots0\rangle$ from thermal equilibrium, a systematic procedure described in Ref. [20] can be used, and an experimental study of quantum Fourier transformation was given in Ref. [21].

In this work we described an explicit procedure to generalize the phases ± 1 which frequently appear in quantum computation to arbitrary phases $e^{i\pi\phi(x)}$, and showed that in NMR these phases can be directly created to equally weighted superposition states $\sum |x\rangle$ without using an additional register. This algorithm of phase creation can be applied to solve an extended Deutsch problem for a function that maps $\{0,1\}^n$ to $\{0,1\}^m$, rather than to $\{0,1\}$. Finding other problems to use arbitrary phases may expand the field of quantum computation.

References

[1] For a review, see *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, edited by D. Bouwmeester, A. Ekert, and A. Zeilinger (Springer-Verlag, Berlin, 2000).

[2] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).

[3] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995). Also see J. I. Cirac and P. Zoller, *ibid.* **74**, 4091 (1995).

[4] N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).

[5] D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Natl. Acad. Sci. U.S.A. **94**, 1634 (1997).

[6] D. Deutsch and R. Jozsa, Proc. R. Soc. London, Ser. A **439**, 553 (1992).

[7] D. Collins, K. W. Kim, and W. C. Holton, Phys. Rev. A **58**, R1633 (1998).

[8] D. Coppersmith, IBM Research Report No. RC19642 (1994).

[9] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. London, Ser. A **454**, 339 (1998).

[10] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung, and S. Lloyd, Nature (London) **393**, 143 (1998).

[11] J. A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).

[12] N. Linden, H. Barjat, and R. Freeman, Chem. Phys. Lett. **296**, 61 (1998).

[13] U. Sakaguchi, H. Ozawa, C. Amano, T. Fukumi, and W. S. Price, in *Mathematical Aspects of Quantum Information and Quantum Chaos*, Proceedings of the Workshop 17-19 February 1999, edited by M. Ohya, RIMS Kokyuroku No. 1142 (Research Institute for Mathematical Sciences, Kyoto University, Kyoto, 2000), pp. 36-52.

[14] Arvind, K. Dorai, and A. Kumar, LANL e-print quant-ph/9909067.

[15] D. Collins, K. W. Kim, W. C. Holton, H. Sierzputowska-Gracz, and E. O. Stejskal, Phys. Rev. A **62**, 022304 (2000).

[16] J. Kim, J.-S. Lee, S. Lee, and C. Cheong, Phys. Rev. A **62**, 022312 (2000).

[17] J. J. Sakurai, *Modern Quantum Mechanics* (Benjamin/Cummings, Menlo Park, CA, 1985), Chap. 3.

[18] U. Sakaguchi, H. Ozawa, C. Amano, and T. Fukumi, Phys. Rev. A **60**, 1906 (1999).

[19] For example, for the case of $m = 3$ and $\phi(x) = \frac{1}{2}$ $(\frac{3}{2})$, $U_{\phi(x)}$ transforms $|y\rangle$ to $|y-2\rangle$ $(|y+2\rangle)$ where $y = 0, 1, \ldots, 7$, and this transformation is implemented by a sequence of two steps: (i) NOT operation on the second qubit of $|u\rangle$, and (ii) NOT operation on the first qubit conditional the second qubit turned to 1 (0).

[20] U. Sakaguchi, H. Ozawa, and T. Fukumi, Phys. Rev. A **61**, 042313 (2000).

[21] Y. S. Weinstein, M. A. Pravia, E. M. Fortunato, S. Lloyd, and D. G. Cory, Phys. Rev. Lett. **86**, 1889 (2001).