Entangling capacity of global phases and implications for the Deutsch-Jozsa algorithm

H. Azuma[1,*] S. Bose[1,†] and V. Vedral[2,‡]

[1]*Centre for Quantum Computation, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, United Kingdom*
[2]*Optics Section, Blackett Laboratory, Imperial College, London SW7 2BZ, United Kingdom*

We investigate the creation of entanglement by the application of phases whose value depends on the state of a collection of qubits. First we give the necessary and sufficient conditions for a given set of phases to result in the creation of entanglement in a state comprising of an arbitrary number of qubits. Then we consider the maximum entanglement generation by global phases. We analyze the creation of entanglement between any two qubits in three-qubit pure and mixed states. We use our result to prove that entanglement is necessary for the Deutsch-Jozsa algorithm to have an exponential advantage over its classical counterpart.

I. INTRODUCTION

In recent years, entanglement has become an important resource for quantum communications [1]. Quantum computation [2], which is more efficient than the classical computation for certain problems [3–5], could also potentially owe its efficiency to entanglement [6–9]. Though the precise role of entanglement in quantum computation is not yet well understood, entangled states are certainly generated during the course of certain quantum computations. A quantum computation, when halted at an appropriate point, can be regarded as a method of generating entanglement. Typically, a quantum computation is a multiparticle interference experiment with different phases applied to distinct multiparticle states [10]. In general, the phases applied to the multiparticle states during a quantum computation are *global phases* as they depend on the total state of a collection of qubits. In this paper, we will investigate the types of entanglement generated by such global phases and the conditions under which such phases do not generate any entanglement.

The model of quantum computation, which motivates our work is that presented by Cleve, Ekert, Macchiavello and Mosca [10]. This model (with a slight alteration that does not change its principal ingredient) is illustrated in Fig. 1. Each of the qubits, initially in the $|0\rangle$ state, is first transformed according to a Hadamard transformation. This is shown in the figure by the giant Hadamard transformation acting on all the qubits and which converts the total state of the qubits to

$$|\phi\rangle_{1,\ldots,N}=\frac{1}{2^{N/2}}\sum_{j=0}^{2^N-1}|j\rangle, \qquad (1)$$

where N is the total number of qubits and the index j labels the 2^N possible states of the type $|j_1,\ldots,j_N\rangle$ in which each $j_i=0$ or 1. $|\phi\rangle_{1,\ldots,N}$ is a disentangled state. A state-

dependent global phase $f(j)$ is now applied to each state $|j\rangle$. This is shown as the second giant transformation F in the figure. This converts the total state to

$$|\psi\rangle_{1,\ldots,N}=\frac{1}{2^{N/2}}\sum_{j=0}^{2^N-1}e^{if(j)}|j\rangle, \qquad (2)$$

where $\{f(j)\}$ are real and $0\leq f(j)<2\pi$ [$f(j)=2\pi$ is reassigned the value 0]. This state $|\psi\rangle_{1,\ldots,N}$, generated as a result of global phases, can be entangled. We propose to halt the quantum computation at this stage and investigate the amount of entanglement generated. A complete quantum computation, of course, consists of one more step in which another giant Hadamard transformation is applied to all the qubits as shown in Fig. 1. But in this paper we are interested in the entanglement of the state *prior* to this last transformation.

The entanglement of $|\psi\rangle_{1,\ldots,N}$ comes from the global phase factors $f(j)$. First, we study conditions on the phase function $f(j)$ for the state $|\psi\rangle_{1,\ldots,N}$ to be disentangled. Next, we consider the maximum entanglement creation by global phases. Then we derive the entanglement of three-qubit pure states ($N=3$) for the special case in which only one or two of the global phase parameters are nonzero. We study variation of the entanglement as a function of one global phase parameter for a mixed state of three qubits by numerical calculations. Finally, we discuss the implications of this type of entanglement arising in Deutsch-Jozsa algorithm. In particular, we show that for obtaining exponential advantage over its classical counterpart, entangled states must necessarily arise in Deutsch-Jozsa algorithm.

II. NECESSARY AND SUFFICIENT CONDITIONS FOR THE GENERATION OF ENTANGLEMENT BY GLOBAL PHASES

We first derive the conditions on $\{f(j)\}$ for $|\psi\rangle_{1,\ldots,N}$ to be disentangled, i.e.,
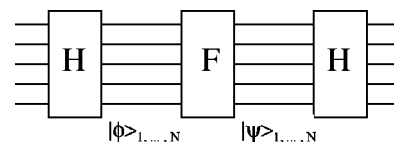
*On leave from Canon Research Center, 5-1, Morinosato-Wakamiya, Atsugi-shi, Kanagawa, 243-0193, Japan. Email address: hiroo.azuma@qubit.org

†Email address: sougato.bose@qubit.org

‡Email address: vlatko.vedral@qubit.org

FIG. 1. A typical quantum computation network.

$$|\psi\rangle_{1,\ldots,N} = |\psi_1\rangle \otimes \cdots \otimes |\psi_N\rangle. \tag{3}$$

In a case of two qubits ($N=2$), we can write the condition as follows:

$$[f(0)-f(1)]-[f(2)-f(3)]=2\pi n, \tag{4}$$

where n is an arbitrary integer.

We now consider the case of three qubits,

$$|\psi_{ABC}\rangle = \frac{1}{2^{3/2}} \sum_{j=0}^{7} e^{if(j)}|j\rangle. \tag{5}$$

First, we derive condition that the qubit C is disentangled from the qubits AB. The density matrix of the qubit C is given by

$$\rho_C = \mathrm{tr}_{AB}(|\psi_{ABC}\rangle\langle\psi_{ABC}|) = \frac{1}{8}\begin{pmatrix} 4 & \gamma \\ \gamma^* & 4 \end{pmatrix}, \tag{6}$$

with taking a basis $\{|0\rangle, |1\rangle\}$ and

$$\gamma = \exp\{i[f(0)-f(1)]\} + \exp\{i[f(2)-f(3)]\}$$
$$+ \exp\{i[f(4)-f(5)]\} + \exp\{i[f(6)-f(7)]\}. \tag{7}$$

(From now on, when we give a matrix representation of a density operator on a 2^N-dimensional space, we always take a logical basis of $\{|x\rangle : x \in \{0,1\}^N\}$.) If and only if $\mathrm{tr}(\rho_C^2)=1$, the qubit C is disentangled from the qubits AB. Hence we obtain the following constraints:

$$[f(0)-f(1)]-[f(2)-f(3)]=2\pi n_1, \tag{8}$$

$$[f(0)-f(1)]-[f(4)-f(5)]=2\pi n_2, \tag{9}$$

$$[f(0)-f(1)]-[f(6)-f(7)]=2\pi n_3. \tag{10}$$

Next, we consider the condition that the qubit B is disentangled from the qubits AC. From similar considerations as before, we obtain another constraint

$$[f(0)-f(2)]-[f(4)-f(6)]=2\pi n_4. \tag{11}$$

From these results, we obtain four constraints, Eqs. (8)–(11), where $n_1, \ldots, n_4$ are arbitrary integers, so that $|\psi_{ABC}\rangle$ is disentangled perfectly.

Next consider the general case of N qubits. Before deriving the condition for $|\psi\rangle_{1,\ldots,N}$ to be disentangled, we think how many constraints of $\{f(j)\}$ do we need to disentangle $|\psi\rangle_{1,\ldots,N}$ completely. In Eq. (2), the number of real parameters is equal to 2^N. On the other hand, if $|\psi\rangle_{1,\ldots,N}$ is disentangled, we can describe it as

$$|\psi\rangle_{1,\ldots,N} = e^{i\theta_0}(|0\rangle + e^{i\theta_1}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{i\theta_N}|1\rangle), \tag{12}$$

where $0 \leq \theta_i < 2\pi$ for $0 \leq \forall i \leq N$ and the number of real parameters is equal to $(N+1)$. Therefore, to disentangle $|\psi\rangle_{1,\ldots,N}$ to an N-qubit product state, we need $[2^N-(N+1)]$ constraints. The constraints are given as follows;

$$[f(0)-f(1)]-[f(2)-f(3)]=2\pi n_1,$$
$$[f(0)-f(1)]-[f(4)-f(5)]=2\pi n_2,$$
$$\vdots$$
$$[f(0)-f(1)]-[f(2^N-2)-f(2^N-1)]$$
$$= 2\pi n_{2^{N-1}-1},$$
$$[f(0)-f(2)]-[f(4)-f(6)]=2\pi m_1,$$
$$\vdots$$
$$[f(0)-f(2)]-[f(2^N-4)-f(2^N-2)]$$
$$= 2\pi m_{2^{N-2}-1},$$
$$\vdots$$
$$[f(0)-f(2^{N-2})]-[f(2^{N-1})-f(3\times 2^{N-2})]$$
$$= 2\pi l, \tag{13}$$

and we can confirm that the number of the above constraints is

$$\sum_{k=1}^{N} (2^{N-k}-1) = 2^N-(N+1). \tag{14}$$

As $|\psi\rangle_{1,\ldots,N}$ being disentangled automatically implies that *all* the above constraints hold, if any of them fails, $|\psi\rangle_{1,\ldots,N}$ is necessarily entangled. A *sufficient* condition for global phase functions $f(j)$ to produce entanglement is thus the violation of any of the above constraints.

In a compact form the above expression can be rewritten as

$$f(j) = \vec{\theta}\cdot\vec{j} + \theta_0 \qquad (\mathrm{mod}\, 2\pi), \tag{15}$$

where $\vec{\theta}=(\theta_1, \ldots, \theta_N)$, $\vec{j}=(j_1, \ldots, j_N)$, and the components j_i are obtained from the binary expression of j as $j_1, \ldots, j_N$, and "$\cdot$" means the inner product of N-component vectors. An easy argument now proves that the violation of Eq. (15) is also a necessary condition for the generation of entanglement by global phases. Consider a phase function $f(j)$ expressible in the form of Eq. (15). Then the whole state, after application of the global phases, can be rewritten in the form of Eq. (12). This is a disentangled state. This means that the ability to express $f(j)$ in the form of Eq. (15) implies no generation of entanglement. In other words, to generate entanglement it is necessary to have a violation of Eq. (15). We have thus found that the necessary and sufficient condition for the generation of entanglement by global phases is the impossibility of the expansion given by Eq. (15) of the global phase function. In the subsequent sections,

we proceed to study the degree and type of entanglement generated by some global phase functions that generate entanglement.

III. GLOBAL PHASES AND THE MAXIMUM ENTANGLEMENT GENERATION

In this section, we discuss the maximum entanglement generation by global phases and show some examples of it. As we are handling $N(\geq 2)$-qubit states and a quantitative definition of entanglement for three or more qubits has not defined in general, we have to clarify the meaning of the maximum entanglement at first. We use this terminology as follows. Let us consider an arbitrary $N(\geq 2)$-qubit pure state. If we regard it as a bipartite pure state of one arbitrary qubit and the others, we can consider its von Neumann entropy as entanglement [11]. As we are thinking about N qubits, we can obtain N different von Neumann entropies. If all of them take the maximum value of unity, we regard the state to be maximally entangled.

Here, we derive some examples of the maximally entangled states. An arbitrary state with global phases is given by Eq. (2). We separate it into the first qubit and the others as

$$\frac{1}{\sqrt{2}}[|0\rangle|\varphi_0\rangle + |1\rangle|\varphi_1\rangle], \qquad (16)$$

where

$$|\varphi_j\rangle = \frac{1}{\sqrt{2^{N-1}}} \sum_{z \in \{0,1\}^{N-1}} e^{if(j,z)}|z\rangle \qquad \text{for } j=0,1. \qquad (17)$$

If $\langle \varphi_0 | \varphi_1 \rangle = 0$, the von Neumann entropy of the reduced density matrix of the first qubit reaches unity. (This condition serves special cases that take the maximized von Neumann entropy. It is only just a sufficient condition.) As we can give a similar discussion for every qubit, we find that

$$\sum_{z \in \{0,1\}^{N-1}} \exp[if(z_1, \ldots, z_{j-1}, 0, z_{j+1}, \ldots, z_N)]$$

$$- if(z_1, \ldots, z_{j-1}, 1, z_{j+1}, \ldots, z_N)] = 0$$

$$\text{for } j=1, \ldots, N, \quad (18)$$

is a sufficient condition for the maximally entangled states. Let us show examples of $f(x)$, which satisfy Eq. (18). In the case of $N=3$, the following global phase satisfies Eq. (18),

$$f_3(x) = \begin{cases} 0, & x=000,001,010,110 \\ \pi, & x=100,101,011,111. \end{cases} \qquad (19)$$

If we carry out the following procedure, we can obtain an example for $N \geq 4$. Suppose we have $\{f_N(x)\}$ that satisfy Eq. (18) for N-qubit case already. We construct $f_{N+1}(x)$ as follows:

$$f_{N+1}(0,z) = f_{N+1}(1,z) = 0$$

$$\text{for half of } \{z : z \in \{0,1\}^N, f_N(z) = 0\},$$

$$f_{N+1}(0,z) = 0, \quad f_{N+1}(1,z) = \pi$$

$$\text{for the other half of } \{z : z \in \{0,1\}^N, f_N(z) = 0\},$$

$$f_{N+1}(0,z) = f_{N+1}(1,z) = \pi$$

$$\text{for half of } \{z : z \in \{0,1\}^N, f_N(z) = \pi\},$$

$$f_{N+1}(0,z) = \pi, \quad f_{N+1}(1,z) = 0$$

$$\text{for the other half of } \{z : z \in \{0,1\}^N, f_N(z) = \pi\}. \qquad (20)$$

Applying this procedure in iteration, we can obtain the maximally entangled states for arbitrary number of qubits. For $N=4$, we obtain

$$f_4(x) = \begin{cases} 0, & x=0000,1000,0001,1001, \\ & \quad 0010,0110,1011,1111 \\ \pi, & x=0100,1100,0101,1101, \\ & \quad 1010,1110,0011,0111. \end{cases} \qquad (21)$$

IV. ENTANGLEMENT BETWEEN TWO QUBITS ON THREE-QUBIT PURE STATES

The general problem of entanglement generation by global phase functions for N qubits is very complicated as it involves 2^N phase parameters. We will consider the simpler case of three-qubit pure states that have just one or two nonzero phase parameters. We first derive how the entanglement between two qubits of a three-qubit pure state varies as a function of global phase functions. For this, we evaluate the complete three-qubit pure state after application of the global phases, compute the reduced density matrix for any two qubits, and obtain the entanglement between these two qubits using the formula for entanglement of formation by Wootters and coworker [12]. We estimate values of phase parameters that give the maximum entanglement.

First, we consider the following pure state with only one global phase parameter θ,

$$|\psi_{ABC}\rangle = \frac{1}{2\sqrt{2}}(e^{i\theta}|000\rangle + |001\rangle + \cdots + |111\rangle). \qquad (22)$$

Defining $\rho_{BC} = \text{tr}_A |\psi_{ABC}\rangle \langle \psi_{ABC}|$, we obtain $\rho_{AB} = \rho_{BC} = \rho_{CA}$ and we get $E(\rho_{AB}) = E(\rho_{BC}) = E(\rho_{CA})$. If we decided

to apply the phase factor $e^{i\theta}$ to $|001\rangle$, instead of $|000\rangle$, and calculated the entanglement between any two qubits, we would obtain the same amount of entanglement as before. To understand this, we apply $\mathbf{I}^{(A)} \otimes \mathbf{I}^{(B)} \otimes \sigma_x^{(C)}$ to Eq. (22), and we obtain

$$|\psi'_{ABC}\rangle = (\mathbf{I}^{(A)} \otimes \mathbf{I}^{(B)} \otimes \sigma_x^{(C)})|\psi\rangle_{ABC}$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle + e^{i\theta}|001\rangle + |010\rangle + \cdots + |111\rangle).$$
$$(23)$$

In general, due to local convertibility, applying a phase factor $e^{i\theta}$ to any of the kets $|x\rangle$ ($\forall x \in \{0,1\}^3$) is equivalent in terms of entanglement as long as it is the *only* phase that is applied.

Here, we evaluate the entanglement between the qubits B and C for the state given by Eq. (22). The reduced density matrix for ρ_{BC} for the qubits B and C is given by

$$\rho_{BC} = \frac{1}{8} \begin{bmatrix} 2 & 1+\tau & 1+\tau & 1+\tau \\ 1+\bar{\tau} & 2 & 2 & 2 \\ 1+\bar{\tau} & 2 & 2 & 2 \\ 1+\bar{\tau} & 2 & 2 & 2 \end{bmatrix}, \quad (24)$$

where $\tau = e^{i\theta}$. Before computing the entanglement, we have to compute another density matrix $\tilde{\rho}$ from ρ following the prescription given in Ref. [12]. We get

$$\rho_{BC}\tilde{\rho}_{BC} = \frac{1}{64} \begin{bmatrix} X & -X & -X & Z \\ Y & -Y & -Y & X \\ Y & -Y & -Y & X \\ Y & -Y & -Y & X \end{bmatrix}, \quad (25)$$

where

$$X = -4\tau + |1+\tau|^2, \quad Y = 4(-1+\bar{\tau}),$$

$$Z = 2(1-\tau^2). \quad (26)$$

Defining an eigenvalue of $\rho_{BC}\tilde{\rho}_{BC}$ as $(\lambda/64)$, we can write an equation for λ as

$$\det\left|\rho_{BC}\tilde{\rho}_{BC} - \frac{\lambda}{64}\mathbf{I}\right| = 0, \quad (27)$$

and finally we obtain the following equation:

$$\lambda^2[\lambda^2 + 2\lambda(Y-X) + X^2 - YZ] = 0. \quad (28)$$

Solutions of this equation are $\lambda = 0$ for a double root and

$$\lambda_\pm = 2(\sqrt{2} \pm 1)^2(1-\cos\theta)(\geq 0). \quad (29)$$

Therefore, because of $\lambda_+ \geq \lambda_-$, the concurrence [12] is given by

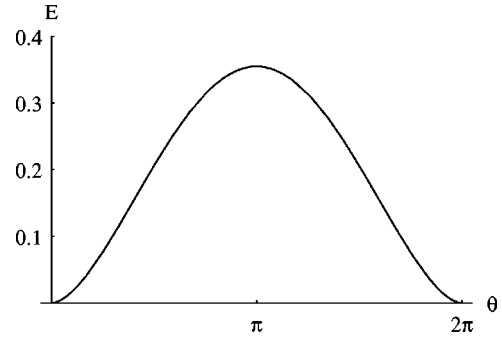FIG. 2. Entanglement E against phase parameter θ for Eq. (24).

$$C = \frac{1}{8}(\sqrt{\lambda_+} - \sqrt{\lambda_-}) = \frac{1}{2\sqrt{2}}\sqrt{1-\cos\theta}(\geq 0), \quad (30)$$

and entanglement can be written as $\mathcal{E}(C) = H(p)$, where

$$p = \frac{1}{2}\left[1 + \sqrt{1 - \frac{1}{8}(1-\cos\theta)}\right]. \quad (31)$$

From Eqs. (30) and (31), we find

$$0 \leq C \leq \frac{1}{2}, \quad \frac{1}{2}\left(1 + \frac{\sqrt{3}}{2}\right) \leq p \leq 1, \quad (32)$$

where p gets maximum at $\theta = 0$ ($C = 0$) and gets minimum at $\theta = \pi$ ($C = 1/2$). (In this range, $H(p)$ decreases monotonously.) $H(p)$ gets the maximum value of $H((1/2)[1 + (\sqrt{3}/2)]) \approx 0.36$ at $\theta = \pi$ and gets the minimum one of $H(1) = 0$ at $\theta = 0$. In Fig. 2, we show a variation of the entanglement E as a function of θ.

The physical reason for the entanglement peaking at $\theta = \pi$ can be understood if $|\psi_{ABC}\rangle$ is rewritten in the following manner

$$|\psi_{ABC}\rangle \propto |0\rangle_A \otimes (e^{i\theta}|00\rangle + |01\rangle + |10\rangle + |11\rangle)_{BC}$$

$$+ |1\rangle_A \otimes (|00\rangle + |01\rangle + |10\rangle + |11\rangle)_{BC}. \quad (33)$$

The state ρ_{BC} is essentially a mixture of the state $e^{i\theta}|00\rangle + |01\rangle + |10\rangle + |11\rangle$, which is maximally entangled for
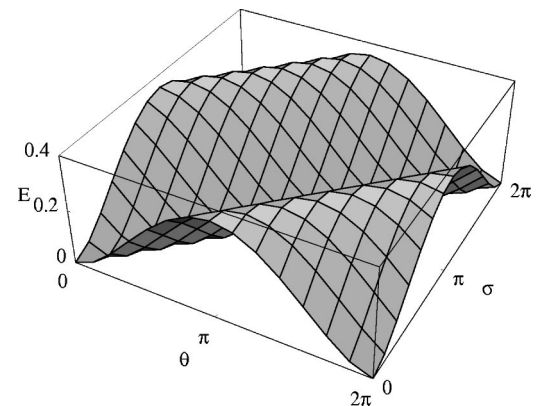
FIG. 3. Entanglement E against phase parameters θ and σ for Eq. (35).

$\theta = \pi$, and $|00\rangle + |01\rangle + |10\rangle + |11\rangle$, which is always disentangled. (If we apply Hadamard transformation to the first qubit of the Bell singlet, we obtain $-|00\rangle + |01\rangle + |10\rangle + |11\rangle$.) Hence it is only expected that the entanglement of the mixture will be maximum at $\theta = \pi$. It is also clear that the entanglement can never be maximal in magnitude because the entangled and the disentangled states are always mixed in equal proportions in ρ_{BC}.

Next, we consider pure states with two phase parameters θ and σ. For example, consider the following state:

$$|\psi_{ABC}\rangle = \frac{1}{2\sqrt{2}}(e^{i\theta}|000\rangle + e^{i\sigma}|001\rangle + |010\rangle + \cdots + |111\rangle),$$

(34)

we trace out the qubit A and get

$$\rho_{BC} = \frac{1}{8}[(e^{i\theta}|00\rangle + e^{i\sigma}|01\rangle + |10\rangle + |11\rangle)$$

$$\times (e^{-i\theta}\langle 00| + e^{-i\sigma}\langle 01| + \langle 10| + \langle 11|)$$

$$+ (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$\times (\langle 00| + \langle 01| + \langle 10| + \langle 11|)]$$

$$= \frac{1}{8}\begin{bmatrix} 2 & \bar{\zeta}\tau + 1 & \tau + 1 & \tau + 1 \\ \zeta\bar{\tau} + 1 & 2 & \zeta + 1 & \zeta + 1 \\ \bar{\tau} + 1 & \bar{\zeta} + 1 & 2 & 2 \\ \bar{\tau} + 1 & \bar{\zeta} + 1 & 2 & 2 \end{bmatrix},$$

(35)

where $\tau = e^{i\theta}$ and $\zeta = e^{i\sigma}$. Writing an eigenvalue of $\rho_{BC}\tilde{\rho}_{BC}$ as $(\lambda/64)$, we obtain $\lambda = 0$ and

$$\lambda_{\pm} = 2(\sqrt{2} \pm 1)^2 [1 - \cos(\theta - \sigma)] (\geq 0).$$

(36)

Hence, the concurrence is

$$C = \frac{1}{2\sqrt{2}}\sqrt{1 - \cos(\theta - \sigma)} (\geq 0),$$

(37)

and the entanglement can be written as $\mathcal{E}(C) = H(p)$, where

$$p = \frac{1}{2}\left\{1 + \sqrt{1 - \frac{1}{8}[1 - \cos(\theta - \sigma)]}\right\}.$$

(38)

From Eqs. (37) and (38), we find that C and p can take values in the ranges of Eq. (32). Because p gets maximum at $\theta = \sigma$ ($C = 0$) and gets minimum at $\theta = \sigma \pm \pi$ ($C = 1/2$), $H(p)$ gets the maximum value at $\theta = \sigma \pm \pi$ and gets the minimum one at $\theta = \sigma$. In Fig. 3, we show a variation of entanglement E as a function of θ and σ.

Again, in this case it is easy to see why the entanglement is minimum for $\theta = \sigma$. The whole state can be rewritten as

$$|\psi_{ABC}\rangle \propto |0\rangle_A \otimes [e^{i\theta}|0\rangle(|0\rangle + e^{i(\sigma - \theta)}|1\rangle) + |1\rangle(|0\rangle + |1\rangle)]_{BC}$$

$$+ |1\rangle_A \otimes (|0\rangle + |1\rangle)_B(|0\rangle + |1\rangle)_C.$$

(39)

This makes it clear that the state ρ_{BC} is a mixture of the state $[e^{i\theta}|0\rangle(|0\rangle + e^{i(\sigma - \theta)}|1\rangle) + |1\rangle(|0\rangle + |1\rangle)]_{BC}$, which is entangled for $\sigma \neq \theta$, and the always disentangled state $(|0\rangle + |1\rangle)_B(|0\rangle + |1\rangle)_C$. The entanglement of ρ_{BC} will thus depend entirely on the entanglement of $[e^{i\theta}|0\rangle(|0\rangle + e^{i(\sigma - \theta)}|1\rangle) + |1\rangle(|0\rangle + |1\rangle)]_{BC}$, whose entanglement will be zero when $\theta = \sigma$ and maximum when $\theta - \sigma = \pi$.

The entanglement between the qubits B and C will depend on the choice of the two kets from the set $\{|x\rangle : x \in \{0,1\}^3\}$ to which we decide to apply the global phases ($e^{i\theta}$ and $e^{i\sigma}$). [It is different from the one-parameter case of Eq. (22)]. Imagine that we had applied the phases to $|000\rangle$ and $|011\rangle$. Then the reduced density matrix for ρ'_{BC} would be

$$\rho'_{BC} = \frac{1}{8}[(e^{i\theta}|00\rangle + |01\rangle + |10\rangle + e^{i\sigma}|11\rangle)$$

$$\times (e^{-i\theta}\langle 00| + \langle 01| + \langle 10| + e^{-i\sigma}\langle 11|)$$

$$+ (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$\times (\langle 00| + \langle 01| + \langle 10| + \langle 11|)].$$

(40)

Because we cannot transform the density matrix ρ of Eq. (40) to that of Eq. (35) by local unitary transformations $U^{(A)} \otimes U^{(B)} \otimes U^{(C)}$, the entanglement of Eq. (35) need not be equal to that of Eq. (40) in general.

Writing ρ'_{BC} as

$$\rho'_{BC} = \frac{1}{8}\begin{bmatrix} 2 & \tau + 1 & \tau + 1 & \tau\bar{\zeta} + 1 \\ \bar{\tau} + 1 & 2 & 2 & \bar{\zeta} + 1 \\ \bar{\tau} + 1 & 2 & 2 & \bar{\zeta} + 1 \\ \bar{\tau}\zeta + 1 & \zeta + 1 & \zeta + 1 & 2 \end{bmatrix},$$

(41)

and an eigenvalue of $\rho'_{BC}\tilde{\rho}'_{BC}$ as $(\lambda/64)$, we obtain $\lambda = 0$ and

$$\lambda_{\pm} = 2\{3r + 2ts \pm 2[2r(r + ts)]^{1/2}\},$$

(42)

where $t = 1 - \cos\theta$, $s = 1 - \cos\sigma$, and $r = 1 - \cos(\theta + \sigma)$. The concurrence is given by $C = (1/8)(\sqrt{\lambda_+} - \sqrt{\lambda_-})$ and $0 \leq C \leq 1/2$. At $\theta + \sigma = 0$ (mod 2π), $C = 0$ and the entanglement E gets minimum. At $\theta + \sigma = \pi$ (mod 2π), $C = 1/2$ and E gets maximum. In Fig. 4, we show a variation of entanglement E as a function of θ and σ. As in the previous cases, the entanglement is entirely due to the entanglement of the first part $e^{i\theta}|00\rangle + |01\rangle + |10\rangle + e^{i\sigma}|11\rangle$ of the density matrix ρ'_{BC}.

Note that in both the cases of Eqs. (35) and (40) maximal entanglement between B and C can never be reached by varying θ and σ. However, one could get maximal entanglement if one applied the two phase parameters to two different global states. This is equivalent to applying same sets of phases as before, but examining the entanglement between the pair of qubits A and C or A and B. Let us consider the three-qubit pure state of Eq. (34) again and trace out the qubit C (in contrast to A) to get
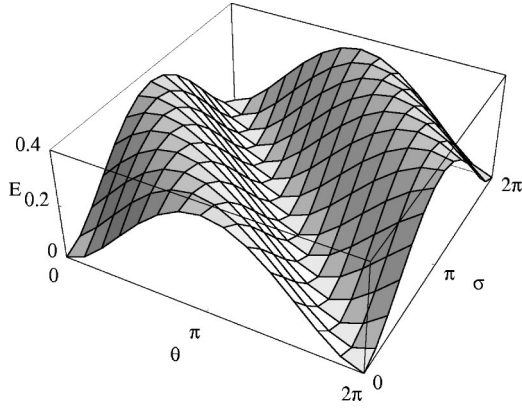
FIG. 4. Entanglement E against phase parameters θ and σ for Eq. (40).

$$\rho_{AB} = \frac{1}{8}[(e^{i\theta}|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$\times (e^{-i\theta}\langle 00| + \langle 01| + \langle 10| + \langle 11|)$$

$$+ (e^{i\sigma}|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$\times (e^{i\sigma}\langle 00| + \langle 01| + \langle 10| + \langle 11|)]$$

$$= \frac{1}{8}\begin{bmatrix} 2 & \zeta + \tau & \zeta + \tau & \zeta + \tau \\ \bar{\zeta} + \bar{\tau} & 2 & 2 & 2 \\ \bar{\zeta} + \bar{\tau} & 2 & 2 & 2 \\ \bar{\zeta} + \bar{\tau} & 2 & 2 & 2 \end{bmatrix}. \qquad (43)$$

If we write an eigenvalue of $\rho_{AB}\widetilde{\rho}_{AB}$ as $(\lambda/64)$, we obtain $\lambda = 0$ and

$$\lambda_{\pm} = 2[4(t+s) - u \pm 2\{2(t+s)[2(t+s) - u]\}^{1/2}], \qquad (44)$$

where t and s are defined before and $u = 1 - \cos(\theta - \sigma)$. In Fig. 5, we show a variation of entanglement of ρ_{AB} as a function of θ and σ.

We now compare the entanglement of ρ_{AB} for Eq. (43) and ρ_{BC} for Eq. (35) with fixed θ. In Fig. 6, we show the
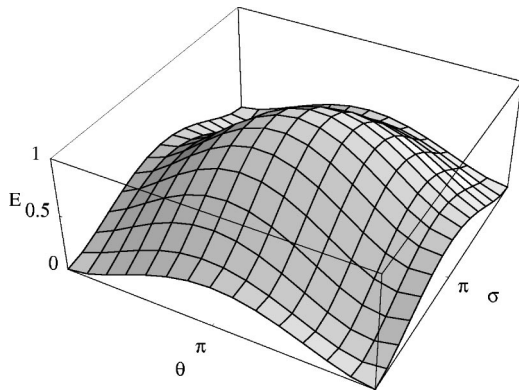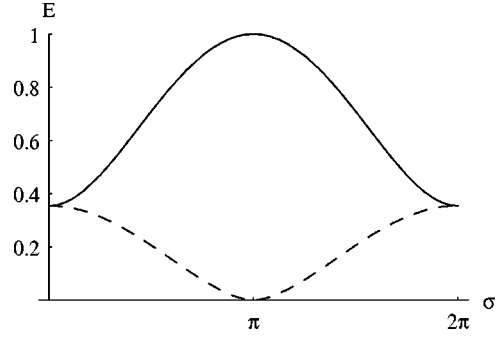

FIG. 5. Entanglement E against phase parameters θ and σ for Eq. (43).

FIG. 6. Entanglement E of ρ_{AB} for Eq. (43) and ρ_{BC} for Eq. (35) against σ with fixed $\theta(=\pi)$. A solid line represents E of ρ_{AB} and a dashed line represents E of ρ_{BC}.

variation of entanglement of ρ_{AB} and ρ_{BC} with $\theta = \pi$. From Fig. 6, we notice the following facts. When the entanglement E of ρ_{BC} decreases, E of ρ_{AB} increases. ρ_{AB} becomes the maximally entangled state at $\theta = \sigma = \pi$. To understand this, we rewrite ρ_{AB} with $\theta = \pi$ as follows:

$$\rho_{AB} = \frac{1}{4}[(|0\rangle|-\rangle + |1\rangle|+\rangle)(\langle 0|\langle -| + \langle 1|\langle +|)$$

$$+ (|0\rangle|\phi_\sigma\rangle + |1\rangle|+\rangle)(\langle 0|\langle \phi_\sigma| + \langle 1|\langle +|)], \quad (45)$$

where

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

$$|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle),$$

$$|\phi_\sigma\rangle = (1/\sqrt{2})(e^{i\sigma}|0\rangle + |1\rangle). \qquad (46)$$

Note that $(|0\rangle|-\rangle + |1\rangle|+\rangle)$ is the maximally entangled state and the phase parameter σ controls the entanglement of the second term in Eq. (45). As $|\phi_{\sigma=\pi}\rangle = |-\rangle$, A and B are maximally entangled in the state $(|0\rangle|-\rangle + |1\rangle|+\rangle)$ (with C being completely disentangled from them) for $\sigma = \pi$.

V. ENTANGLEMENT BETWEEN TWO QUBITS ON THREE-QUBIT MIXED STATES

In previous sections, we have studied the entanglement between two qubits on pure states with phase factors. The pure state of Eq. (22) is prepared by taking a three-qubit state $(|+\rangle\langle +|)^{\otimes 3}$, and giving a phase $e^{i\theta}$ on the ket vector $|000\rangle$. (In this section, we will often use the basis $\{|\pm\rangle = (1/\sqrt{2})(|0\rangle \pm |1\rangle)\}$.)

Here, instead of the pure state $(|+\rangle\langle +|)^{\otimes 3}$, we take a mixed state

$$[(1-q)|+\rangle\langle +| + q|-\rangle\langle -|]^{\otimes 3}, \qquad (47)$$

where $0 \leq q \leq 1/2$. Then, we consider the application of a single phase factor as follows:

$$|000\rangle \rightarrow e^{i\theta}|000\rangle. \qquad (48)$$

Tracing out any qubit out of the three qubits, we obtain the density matrix in the form of

$$
\rho = \frac{1}{4}
\begin{bmatrix}
1 & (1+\tau)\alpha & (1+\tau)\alpha & 2(1+\tau)\alpha^2 \\
(1+\bar{\tau})\alpha & 1 & 4\alpha^2 & 2\alpha \\
(1+\bar{\tau})\alpha & 4\alpha^2 & 1 & 2\alpha \\
2(1+\bar{\tau})\alpha^2 & 2\alpha & 2\alpha & 1
\end{bmatrix},
$$
(49)

where $\tau = e^{i\theta}$ and $\alpha = (1/2) - q$. Now we proceed to derive the entanglement $E(\rho)$ as a function of θ and q.

We already know that entanglement takes the maximum value at $\theta = \pi$ when we fix $q = 0$. The interesting question is whether that peak of entanglement remains in the same place for a nonzero q. Before evaluating $E(\rho)$ explicitly, we show that it gets a local stationary value at $\theta = \pi$ for arbitrary fixed p $(0 \leq \forall q \leq 1/2)$. (It remains stationary locally along θ axis at any fixed q.)

We first show that an infinitesimal variation of θ from $\theta = \pi$ does not affect an equation of eigenvalues of $\rho\tilde{\rho}$. The equation of eigenvalues of $\rho\tilde{\rho}$ with $\theta = \pi + \delta$ and $|\delta| \ll 1$ is given by

$$
\det|\rho\tilde{\rho} - \lambda \mathbf{I}|\big|_{\theta = \pi + \delta}
$$

$$
= \det|\rho\tilde{\rho} - \lambda \mathbf{I}|\Big|_{\theta = \pi} + \delta \frac{\partial}{\partial\theta}[\det|\rho\tilde{\rho} - \lambda\mathbf{I}|]\big|_{\theta=\pi} + O(\delta^2)
$$

$$
= 0.
$$
(50)

Hence, if $\partial_\theta[\det|\rho\tilde{\rho} - \lambda\mathbf{I}|]\big|_{\theta=\pi} = 0$, the equation is not affected by δ and the eigenvalues of $\rho\tilde{\rho}$ get stationary around a neighborhood of $\theta = \pi$ for fixed q.

Writing

$$
\rho\tilde{\rho} - \lambda\mathbf{I} =
\begin{bmatrix}
X+L & V & V & W \\
Y & -Z+L & -Z & -V \\
Y & -Z & -Z+L & -V \\
Z & -Y & -Y & X+L
\end{bmatrix},
$$
(51)

where

$$
X = -(1/16)(1-\bar{\tau})\alpha^2[(1-\tau)\alpha^2 + \tau],
$$

$$
Y = -(1/16)(1-\bar{\tau})\alpha(1+4\alpha^2),
$$

$$
Z = -(1/4)(1-\bar{\tau})\alpha^2,
$$

$$
V = (1/16)(1-\bar{\tau})\alpha[2\alpha^2 + \tau(1+2\alpha^2)],
$$

$$
W = (1/8)(1-\tau^2)\alpha^2,
$$

$$
L = -\lambda + (1/16)(1+2\alpha)^2(1-2\alpha)^2,
$$
(52)

we can obtain the following result with some calculations [13]:

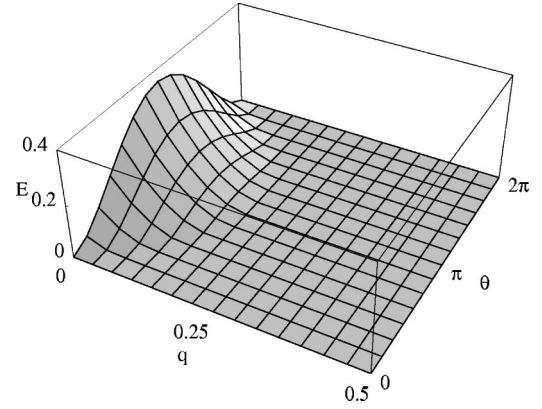

FIG. 7. Entanglement E against phase parameter θ and probability q for the mixed state of Eq. (49).

$$
\frac{\partial}{\partial\theta}[\det|\rho\tilde{\rho} - \lambda\mathbf{I}|]\big|_{\theta=\pi}
$$

$$
=
\begin{bmatrix}
\begin{vmatrix}
\partial_\theta X & \partial_\theta V & \partial_\theta V & \partial_\theta W \\
Y & -Z+L & -Z & -V \\
Y & -Z & -Z+L & -V \\
Z & -Y & -Y & X+L
\end{vmatrix}
\\
+2
\begin{vmatrix}
X+L & V & V & W \\
\partial_\theta Y & -\partial_\theta Z & -\partial_\theta Z & -\partial_\theta V \\
Y & -Z & -Z+L & -V \\
Z & -Y & -Y & X+L
\end{vmatrix}
\\
+
\begin{vmatrix}
X+L & V & V & W \\
Y & -Z+L & -Z & -V \\
Y & -Z & -Z+L & -V \\
\partial_\theta Z & -\partial_\theta Y & -\partial_\theta Y & \partial_\theta X
\end{vmatrix}
\end{bmatrix}_{\theta=\pi} = 0.
$$
(53)

Therefore, $E(\rho)$ remains stationary at $\theta = \pi$ for any fixed q and we can expect that it gets maximum there along θ axis.

By numerical calculations, we get Fig. 7. It is clear from this figure that the basic behavior of entanglement with variation of a single phase parameter θ does not change for a mixed initial state and it is still maximum at $\theta = \pi$. Figure 8 shows variation of E as a function of q for $\theta = \pi$. This figure illustrates that the entanglement is lost rapidly as q gets larger. This is also an expected result: the more mixed the initial state is, the harder it is to entangle it by global phase functions.

VI. NECESSITY OF ENTANGLEMENT FOR EXPONENTIAL SPEEDUP IN THE DEUTSCH-JOZSA ALGORITHM

We now present an application of our results on entangling by global phases to the question of necessity of en-
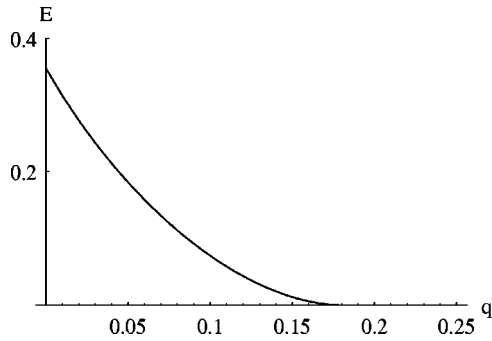
FIG. 8. Entanglement E against probability q for $\theta = \pi$ for the mixed state of Eq. (49).

tanglement in quantum computation. In the Deutsch-Jozsa algorithm, the following state appears [3]:

$$|\Psi\rangle = 2^{-n/2} \sum_{j \in \{0,1\}^n} e^{if(j)} |j\rangle, \qquad (54)$$

where $0 \leq f(j) \leq 2\pi \ \forall j$. If $f(j)$ is constant $\forall j$, $|\Psi\rangle$ is a uniform superposition, and we get $|0 \cdots 0\rangle$ by applying the quantum Fourier transformation (QFT) to $|\Psi\rangle$. On the other hand, if $\{f(j)\}$ takes on values 0 or π randomly but in a balanced manner (i.e., equal occurrences of 0 and π), $|\Psi\rangle$ is orthogonal to the uniform superposition and we get a state orthogonal to $|0 \cdots 0\rangle$ after QFT. Therefore, we can investigate whether f is constant or balanced by a single application of the global phase function using a quantum computer. On the other hand, in the worst case scenario using a classical algorithm, one may have to evaluate this function for at least half the number of possible arguments j. This implies $2^n/2$ (exponential) function evaluations. This is why the Deutsch-Jozsa algorithm is regarded as having an exponential advantage over its classical counterpart.

To see that entanglement is necessary for the exponential advantage of this algorithm, consider the following scenario. It is given that the global phase functions, apart from being constant or balanced and taking values 0 or π, are also restricted in such a manner that they never produce an entangled state in the course of the entire computation. This implies (according to the conditions obtained in Sec. II)

$$f(j) = \vec{\theta} \cdot \vec{j} + \theta_0 \qquad (\text{mod } 2\pi). \qquad (55)$$

If we know beforehand that f can be written as Eq. (55), we can estimate f completely with $O(n)$ steps of classical algorithm, even in the worst case. We supply $(0 \cdots 0)$ and strings where only one digit is 1 and the others are 0, $(10 \cdots 0)$, ..., $(0 \cdots 01)$, as j of inputs for f, and we get θ_0 and $\bar{\theta}$ as outputs. Hence, when we restrict the possible set of functions

to those which are *nonentanglement producing*, a polynomial time classical algorithm exists. In other words, there is only a polynomial advantage of quantum computation over classical computation. To make the quantum algorithm have an exponential advantage over its classical counterpart, we must remove the restriction of Eq. (55) on the global phase functions $f(j)$, which implies that entanglement cannot be prevented from arising any more during the course of the quantum computation. As no entanglement implies only polynomial advantage, to get exponential advantage, entanglement is necessary.

VII. CONCLUSIONS

In this paper, we have investigated the generation of entanglement through global phase functions. We have obtained the necessary and sufficient conditions for the application of global phases to the pure product state $|0 \cdots 00\rangle + |0 \cdots 01\rangle + \cdots + |1 \cdots 11\rangle$ to result in entanglement. We have considered the maximum entanglement creation by global phases and shown examples of it. Though we have obtained a sufficient condition, this is a very general (in the sense of all global phases being present) statement. We have then investigated the amount of two-qubit entanglement that can be generated in three-qubit pure states when only one or two of the global phase parameters are nonzero. An interesting, though potentially difficult, future direction will be the investigation of the quantity of entanglement when all phase parameters are present for an arbitrary number of qubits. While we have obtained the conditions for *presence* or *absence* of entanglement in the general case, it would be interesting to classify functions according to the *degree* of entanglement they can generate. We have also examined entanglement generation through a single global phase parameter for mixed initial states. The general problem of finding necessary and sufficient conditions for entanglement by global phases for mixed states remains open. One could expect counterintuitive results in that case as the same global phase function might entangle one pure component and disentangle another pure component of a mixture of two pure states. Finally, we have applied our conditions to prove the necessity of entanglement in the Deutsch-Jozsa algorithm for the algorithm to have an exponential advantage over its classical counterpart. It would be interesting to apply similar techniques to the investigation of the role of entanglement in other quantum algorithms.

[1] C.H. Bennett and D.P. DiVincenzo, Nature (London) **404**, 247 (2000).
[2] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).
[3] D. Deutsch and R. Jozsa, Proc. R. Soc. London, Ser. A **439**, 553 (1992).
[4] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (FOCS)* (IEEE Computer Society, Los Alamitos, 1994), pp. 124–134; P.W. Shor,

SIAM J. Comput. **26**, 1484 (1997).

[5] L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (*STOC*) (ACM Press, New York, 1996), pp. 212–219; L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[6] R. Jozsa, in *The Geometric Universe: Science, Geometry, and the Work of Roger Penrose,* edited by S. A. Huggett *et al.* (Oxford University Press, London, 1998), pp. 369–379.

[7] A. Ekert and R. Jozsa, Philos. Trans. R. Soc. London, Ser. A **356**, 1769 (1998).

[8] N. Linden and S. Popescu, Phys. Rev. Lett. **87**, 047901 (2001).

[9] K. Dorai, Arvind, and A. Kumar, Phys. Rev. A **63**, 034101 (2001).

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

[11] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996); C.H. Bennett and P.W. Shor, IEEE Trans. Inf. Theory **44**, 2724 (1998).

[12] S. Hill and W.K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997); W.K. Wootters, *ibid.* **80**, 2245 (1998).

[13] S. Barnett, *Matrices: Methods and Applications* (Clarendon Press, Oxford, 1990), Chap. 4.