Distributed implementation of standard oracle operators

Anthony Chefles[*]
Quantum Information Processing Group, Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS34 8QZ, United Kingdom

(Received 7 July 2007; revised manuscript received 24 August 2008; published 3 December 2008)

The standard oracle operator corresponding to a function f is a unitary operator that computes this function coherently, i.e., it maintains superpositions. This operator acts on a bipartite system, where the subsystems are the input and output registers. In distributed quantum computation, these subsystems may be spatially separated, in which case we will be interested in its classical and entangling capacities. For an arbitrary function f, we show that the unidirectional classical and entangling capacities of this operator are $\log_2(n_f)$ bits (ebits) where n_f is the number of different values this function can take. An optimal procedure for bidirectional classical communication with a standard oracle operator corresponding to a permutation on $\mathbb{Z}_M$ is given. The bidirectional classical capacity of such an operator is found to be $2\log_2(M)$ bits. The proofs of these capacities are facilitated by an optimal distributed protocol for the implementation of an arbitrary standard oracle operator.

DOI: 10.1103/PhysRevA.78.062304 PACS number(s): 03.67.Lx, 03.67.Dd, 03.67.Hk, 03.67.Mn

I. INTRODUCTION

The rapidly developing field of quantum information science has yielded many new concepts in communications and computation, which have led to major applications such as quantum cryptography and fast quantum algorithms [1]. In quantum as in classical information processing, situations involving spatially separated parties are of particular interest. It is therefore necessary to develop the theory of distributed quantum information processing [2–9]. Here, we consider quantum systems whose component subsystems are possessed by a number of spatially separated parties. These subsystems cannot interact directly, so the effect of an interaction must be brought about using only local quantum operations and nonlocal resources. The nonlocal resources needed to implement an arbitrary quantum operation in this manner are classical communication channels and shared entangled states.

One particularly important quantum operation within the context of quantum information processing is the standard oracle operator. This operator is a key building block for quantum algorithms. Generally speaking, an oracle operator is a unitary operator that computes a function. The key difference between oracle operators and classical methods of computation is that the former, being linear quantum-mechanical operators, maintain superpositions. A superposition of different values of the independent variable, which we denote by x, will then evolve into a superposition of the corresponding values of $f(x)$, giving rise to the well-known and important phenomenon of quantum parallelism. The standard oracle operator is a convenient oracle operator which can be used to compute an arbitrary function [10,11]. However, it has different registers for x and $f(x)$ and in a distributed setting it is natural to consider these to be spatially separated.

In this paper, we investigate numerous aspects of the distributed implementation of standard oracle operators. We consider both the minimum entanglement and classical communication resources, in both directions, required for this implementation and also the corresponding capacities, which relate to the fact that it is possible to use such an operator to send classical information and create entangled states. It is important to determine the values of these quantities for the following reasons. Regarding the minimal resources necessary for the distributed implementation of the standard oracle operator, it is highly desirable to use classical communication and, even more so, shared entanglement, as efficiently as possible when implementing distributed quantum operations. Concerning the capacities, it is important to have knowledge of these quantities in circumstances where we are able to perform this operation and wish to use it to create entangled states or transmit classical information.

The main result of this article is that for an arbitrary function f, all six minimum implementation resources and capacities are equal to $\log_2(n_f)$ bits/ebits, where n_f is the number of different values this function can take. In the course of this investigation, we provide optimal protocols for entanglement creation and classical communication using an arbitrary standard oracle operator, indeed also for bidirectional classical communication when the function f is a permutation. We also give an optimal protocol for the distributed implementation of an arbitrary standard oracle operator.

Let us set the scene by reviewing the main properties of standard oracle operators. Let M,N be arbitrary finite integers $\geqslant 1$. Consider $\mathcal{F}_{MN}$, the set of functions from $\mathbb{Z}_M \mapsto \mathbb{Z}_N$. Let A and B be quantum systems with M- and N-dimensional Hilbert spaces $\mathcal{H}_M$ and $\mathcal{H}_N$. These systems are taken to be spatially separated and in the possession of corresponding parties Alice and Bob. To each $f \in \mathcal{F}_{MN}$ there corresponds a unitary standard oracle operator on $\mathcal{H}_M \otimes \mathcal{H}_N$:

$$U_f|x\rangle_A \otimes |y\rangle_B = |x\rangle_A \otimes |y \oplus f(x)\rangle_B. \tag{1.1}$$

A and B may be referred to as the control and target systems, respectively. In Eq. (1.1), $\oplus$ denotes addition modulo N. Also, $x \in \mathbb{Z}_M, y \in \mathbb{Z}_N$ and $\{|x\rangle\}$ is an orthonormal basis set for $\mathcal{H}_M$, likewise with $\{|y\rangle\}$ and $\mathcal{H}_N$. These are the computational

[*] anthony.chefles@btinternet.com

basis sets for both systems. There are N^M functions in $\mathcal{F}_{MN}$, so there are N^M associated standard oracle operators U_f.

To proceed, let us partition $\mathbb{Z}_M$ into subsets corresponding to different values of $f(x)$. Let n_f be the number of different values that $f(x)$ can take. Clearly, $n_f \leqslant M,N$. Let f_j, where $j\in\{0,\ldots,n_f-1\}$, be the possible values of $f(x)$. We also define $S_j \subset \mathbb{Z}_M$ to be the set of values of x for which $f(x) = f_j$ and denote by $P_j = \Sigma_{x\in S_j}|x\rangle\langle x|$ the projector onto the subspace spanned by the states $|x\rangle$ for $x\in S_j$. Finally, let K_j be the cardinality of S_j. Clearly, K_j is the rank of P_j. It is a simple matter to prove that U_f can be written in the form [11]

$$U_f = \sum_{j=0}^{n_f-1} P_{jA} \otimes (e^{-if_j\Phi_N})_B, \tag{1.2}$$

where we use the N-dimensional Pegg-Barnett phase operator

$$\Phi_N = \sum_{n\in\mathbb{Z}_N} \frac{2\pi n}{N} |\phi_{Nn}\rangle\langle\phi_{Nn}|, \tag{1.3}$$

whose eigenstates are the N-dimensional Pegg-Barnett phase states $|\varphi_{Nn}\rangle = N^{-1/2}\Sigma_{y\in\mathbb{Z}_N} e^{2\pi i n y/N}|y\rangle$ [12]. These states form an orthonormal basis for $\mathcal{H}_N$ which is conjugate to the computational basis $\{|y\rangle\}$. One can readily verify that

$$e^{-i\Phi_N}|y\rangle = |y \oplus 1\rangle \;\; \forall \;\; y \in \mathbb{Z}_N. \tag{1.4}$$

We note that Eq. (1.2) gives an operator Schmidt decomposition of U_f, where the related Schmidt operator sets are $\{P_j/\sqrt{K_j}\}$ and $\{e^{-if_j\Phi_N}/\sqrt{N}\}$. These are orthonormal sets with respect to the Hilbert-Schmidt inner product $\langle A,B\rangle = \mathrm{Tr}(A^\dagger B)$. The Schmidt coefficients are $\sqrt{NK_j}$ and the Schmidt rank of U_f, denoted by $\mathrm{Sch}(U_f)$, is equal to n_f.

II. LOWER BOUNDS ON THE ENTANGLING AND CLASSICAL CAPACITIES

In a distributed setting, any type of nonlocal resource that can be created by a quantum operation must also be consumed in order to perform the operation. For a bipartite quantum operation, there are three such resources: shared entanglement E and classical communication in the Alice → Bob and Bob → Alice directions, which we shall denote by $C_{\rightarrow}$ and $C_{\leftarrow}$, respectively. We shall use the subscripts R and C to denote, respectively, the minimum of the corresponding resource required to perform a quantum operation and the capacity of the operation corresponding to this resource. The entangling capacity is the maximum amount of entanglement that the operation can create. The classical capacity, in a given direction, is the maximum amount of classical information that the operation can be used to send in that direction.

A fundamental result in quantum information theory is that, for any bipartite unitary operator U, each capacity cannot exceed the amount of the corresponding resource that must be consumed [4]. We therefore have the following inequalities:

$$E_R(U) \geqslant E_C(U), \tag{2.1}$$

$$C_{R\rightarrow}(U) \geqslant C_{C\rightarrow}(U), \tag{2.2}$$

$$C_{R\leftarrow}(U) \geqslant C_{C\leftarrow}(U). \tag{2.3}$$

There is a further capacity to consider, the bidirectional classical capacity $C_{C\leftrightarrow}(U)$. This is the maximum total amount of classical information that Alice and Bob can send to each other with one use of the quantum operation. Since the unidirectional classical capacities are optimized for transmission in their associated directions, we have

$$C_{C\leftrightarrow}(U) \leqslant C_{C\rightarrow}(U) + C_{C\leftarrow}(U). \tag{2.4}$$

It should be said at this point that we shall be considering the true capacities of the operation, rather than those obtained following the imposition of constraints. For example, when considering the entangling capacity, we shall assume limitless auxiliary resources such as classical communication. Similarly, when considering classical capacities, we shall assume limitless auxiliary resources including shared entanglement.

We shall now obtain, for an arbitrary standard oracle operator U_f, lower bounds on the entangling and unidirectional classical capacities $E_C(U_f)$, $C_{C\rightarrow}(U_f)$, and $C_{C\leftarrow}(U_f)$. We begin by examining entanglement creation. Consider some arbitrary but fixed $x_j \in S_j$, for each $j\in\{0,\ldots,n_f-1\}$. Suppose that A and B are initially prepared in the product state

$$|\chi\rangle = \left(\frac{1}{\sqrt{n_f}}\sum_{j=0}^{n_f-1}|x_j\rangle_A\right)\otimes|0\rangle_B, \tag{2.5}$$

where $|0\rangle$ is the zeroth computational basis state in $\mathcal{H}_N$. Acting upon this state with U_f gives

$$U_f|\chi\rangle = \frac{1}{\sqrt{n_f}}\sum_{j=0}^{n_f-1}|x_j\rangle_A \otimes |f_j\rangle_B. \tag{2.6}$$

This is a maximally entangled state with Schmidt rank n_f, having $\log_2(n_f)$ ebits of entanglement. We conclude that

$$E_C(U_f) \geqslant \log_2(n_f). \tag{2.7}$$

Let us now show that Alice and Bob can send each other $\log_2(n_f)$ classical bits using U_f. That Alice can send Bob $\log_2(n_f)$ bits is almost trivially demonstrated. Let $r \in \{0,\ldots,n_f-1\}$ be the classical message she wishes to send to Bob. She prepares A in the state $|x_r\rangle$. Meanwhile, Bob prepares B in the state $|0\rangle$. The oracle operator U_f then acts on these systems, giving rise to the state $|x_r\rangle_A \otimes |f_r\rangle_B$. Bob can subsequently perform a computational basis measurement to reveal f_r and hence r, Alice's $\log_2(n_f)$ bit message.

For Bob to send the same amount of classical information to Alice, the two parties can use the following entangled state:

$$|\psi\rangle = \frac{1}{\sqrt{n_f}}\sum_{j=0}^{n_f-1}|x_j\rangle_A \otimes |N \ominus f_j\rangle_B, \tag{2.8}$$

where $\ominus$ denotes subtraction modulo N. Bob wishes to send the value of $s\in\{0,\ldots,n_f-1\}$ to Alice. To encode his chosen value of s in the above state, he makes use of a unitary phase shift operator G acting on $\mathcal{H}_N$ which is defined through

$$G|N\ominus f_j\rangle = e^{2\pi i j/n_f}|N\ominus f_j\rangle. \tag{2.9}$$

His encoding of s is performed through the transformation $|\psi\rangle \mapsto |\psi_s\rangle = (\mathbb{1}_A \otimes G_B^s)|\psi\rangle$, giving

$$|\psi_s\rangle = \frac{1}{\sqrt{n_f}}\sum_{j=0}^{n_f-1} e^{2\pi i j s/n_f}|x_j\rangle_A \otimes |N\ominus f_j\rangle_B. \tag{2.10}$$

The oracle operator U_f is then applied, resulting in the state

$$U_f|\psi_s\rangle = \left(\frac{1}{\sqrt{n_f}}\sum_{j=0}^{n_f-1} e^{2\pi i j s/n_f}|x_j\rangle_A\right) \otimes |N\rangle_B. \tag{2.11}$$

The states inside the parentheses, indexed by s, are orthonormal and can be perfectly discriminated by Alice. Doing so enables her to read Bob's $\log_2(n_f)$ bit message s. The existence of these classical communication protocols implies that

$$C_{C\rightarrow}(U_f), C_{C\leftarrow}(U_f) \geqslant \log_2(n_f). \tag{2.12}$$

Let us now consider simultaneous, bidirectional classical communication. Here we will see that, when f is permutation from $\mathbb{Z}_M \mapsto \mathbb{Z}_M$, the above protocol can be modified to enable Alice and Bob to send to each other $\log_2(n_f) = \log_2(M)$ classical bits simultaneously. Let $f:\mathbb{Z}_M \mapsto \mathbb{Z}_M$ be a permutation of degree M. We begin with the state

$$|\Psi\rangle = \frac{1}{\sqrt{M}}\sum_{x\in\mathbb{Z}_M} |x\rangle_A \otimes |M\ominus x\rangle_B, \tag{2.13}$$

which resembles the state $|\psi\rangle$ in Eq. (2.8). Here, $\oplus/\ominus$ denotes addition/subtraction modulo M. Alice encodes her message $r \in \mathbb{Z}_M$ with the unitary transformation $|x\rangle \mapsto |f^{-1}(x \oplus r)\rangle$ on A. Again, Bob encodes his message s with a unitary phase shift on B; here $|M\ominus x\rangle \mapsto e^{2\pi i s x/M}|M\ominus x\rangle$ where $s \in \mathbb{Z}_M$. The total state transformation is $|\Psi\rangle \mapsto |\Psi_{rs}\rangle$, where

$$|\Psi_{rs}\rangle = \frac{1}{\sqrt{M}}\sum_{x\in\mathbb{Z}_M} e^{2\pi i s x/M}|f^{-1}(x\oplus r)\rangle_A \otimes |M\ominus x\rangle_B. \tag{2.14}$$

The corresponding standard oracle operator U_f is then applied, which results in the transformation

$$U_f|\Psi_{rs}\rangle = \frac{1}{\sqrt{M}}\sum_{x\in\mathbb{Z}_M} e^{2\pi i s x/M}|f^{-1}(x\oplus r)\rangle_A \otimes |M\oplus r\rangle_B. \tag{2.15}$$

Alice and Bob are now able to read each other's messages. For the sake of clarity, let Alice now invert her earlier unitary transformation on A and Bob perform the unitary transformation $\Sigma_{r'\in\mathbb{Z}_M}|r'\rangle\langle M\oplus r'|$ on B. This results in the state

$$\left(\frac{1}{\sqrt{M}}\sum_{x\in\mathbb{Z}_M} e^{2\pi i s x/M}|x\rangle_A\right) \otimes |r\rangle_B. \tag{2.16}$$

The states of A are the orthonormal eigenstates of Φ_M indexed by s. These states are perfectly distinguishable by Alice, as are the states $|r\rangle$ by Bob. Discrimination among these states enables Alice and Bob to read each other's $\log_2(M)$ bit messages. We therefore conclude, for a standard oracle operator corresponding to a permutation of degree M, that the bidirectional classical capacity satisfies

$$C_{C\leftrightarrow}(U_f) \geqslant 2\log_2(M). \tag{2.17}$$

III. AN OPTIMAL DISTRIBUTED IMPLEMENTATION PROTOCOL

Having obtained lower bounds on the entangling and classical capacities for a standard oracle operator, we now obtain upper bounds on the corresponding minimum resources for its distributed implementation. We will now show that

$$E_R(U_f), C_{R\rightarrow}(U_f), C_{R\leftarrow}(U_f) \leqslant \log_2(n_f), \tag{3.1}$$

by describing an explicit protocol that uses $\log_2(n_f)$ ebits of entanglement and the same number of classical bits in each direction to perform the distributed implementation of a standard oracle operator. We begin with an arbitrary initial state of systems A and B, which may be written in the form

$$|\Phi\rangle = \sum_{\substack{m\in\mathbb{Z}_M\\ n\in\mathbb{Z}_N}} c_{mn}|m\rangle_A \otimes |n\rangle_B. \tag{3.2}$$

In addition to A and B, Alice and Bob have respective ancillas a and b. Their Hilbert spaces can be described in the following way. Let us define $\mathcal{H}_f$ as the n_f-dimensional subspace of $\mathcal{H}_M$ spanned by the states $|x_j\rangle$ for $j \in \{0,\ldots,n_f-1\}$. Then the Hilbert spaces of a and b are copies of $\mathcal{H}_f$. The two ancillas are initially prepared in the maximally entangled state $n_f^{-1/2}\Sigma_{j=0}^{n_f-1}|x_j\rangle_a \otimes |x_j\rangle_b$, which has $\log_2(n_f)$ ebits of entanglement. The total initial state is therefore

$$|\Phi_0\rangle = \frac{1}{\sqrt{n_f}}\sum_{j=0}^{n_f-1}\sum_{\substack{m\in\mathbb{Z}_M\\ n\in\mathbb{Z}_N}} c_{mn}|m\rangle_A \otimes |x_j\rangle_a \otimes |n\rangle_B \otimes |x_j\rangle_b. \tag{3.3}$$

Our protocol can be described in the following way.

Step 1. Alice applies the following unitary operator to Aa:

$$\Omega = \sum_{k=0}^{n_f-1} P_{kA} \otimes V_{ka}. \tag{3.4}$$

Here, V_k is a unitary operator on $\mathcal{H}_f$ which acts as $V_k|x_j\rangle = |x_{j\bar{\oplus}k}\rangle$, where throughout, $\bar{\oplus}$ ($\bar{\ominus}$) denotes addition (subtraction) modulo n_f. The state transformation effected by this operator is $|\Phi_0\rangle \mapsto |\Phi_1\rangle$, where

$$|\Phi_1\rangle = \frac{1}{\sqrt{n_f}}\sum_{j,k=0}^{n_f-1}\sum_{\substack{m\in S_k\\ n\in\mathbb{Z}_N}} c_{mn}|m\rangle_A \otimes |x_{j\bar{\oplus}k}\rangle_a \otimes |n\rangle_B \otimes |x_j\rangle_b. \tag{3.5}$$

Step 2. Alice performs a computational basis measurement on a, getting result x_r for some $r \in \{0,\ldots,n_f-1\}$. This results in the state transformation $|\Phi_1\rangle \mapsto |\Phi_{2r}\rangle$, where

$$|\Phi_{2r}\rangle = \sum_{k=0}^{n_f-1} \sum_{\substack{m\in S_k \\ n\in\mathbb{Z}_N}} c_{mn}|m\rangle_A \otimes |x_r\rangle_a \otimes |n\rangle_B \otimes |x_{r\bar{\ominus}k}\rangle_b . \tag{3.6}$$

Step 3. Alice communicates the value of r to Bob, thus sending him $\log_2(n_f)$ classical bits. With his knowledge of r, Bob performs the unitary transformation $|x_{r\bar{\ominus}k}\rangle \mapsto |x_k\rangle$ on b, resulting in the total state transformation $|\Phi_{2r}\rangle \mapsto |\Phi_{3r}\rangle$, where

$$|\Phi_{3r}\rangle = \sum_{k=0}^{n_f-1} \sum_{\substack{m\in S_k \\ n\in\mathbb{Z}_N}} c_{mn}|m\rangle_A \otimes |x_r\rangle_a \otimes |n\rangle_B \otimes |x_k\rangle_b . \tag{3.7}$$

Step 4. Bob now performs the unitary transformation

$$|n\rangle_B \otimes |x_k\rangle_b \mapsto |n \oplus f_k\rangle_B \otimes |x_k\rangle_b, \tag{3.8}$$

where $\oplus$ denotes addition modulo N. This transformation is effectively the oracle operator U_f, with b and B being the control and target systems, respectively, and the state of the control system is restricted to the subspace $\mathcal{H}_f$ of $\mathcal{H}_M$. This gives $|\Phi_{3r}\rangle \mapsto |\Phi_{4r}\rangle$ where

$$|\Phi_{4r}\rangle = \sum_{k=0}^{n_f-1} \sum_{\substack{m\in S_k \\ n\in\mathbb{Z}_N}} c_{mn}|m\rangle_A \otimes |x_r\rangle_a \otimes |n \oplus f_k\rangle_B \otimes |x_k\rangle_b . \tag{3.9}$$

Step 5. Bob performs a discrete Fourier transform on the b system whose effect is $|x_k\rangle \mapsto n_f^{-1/2}\Sigma_{s=0}^{n_f-1} e^{2\pi iks/n_f}|x_s\rangle$, resulting in the total state transformation $|\Phi_{4r}\rangle \mapsto |\Phi_{5r}\rangle$, where

$$|\Phi_{5r}\rangle = \frac{1}{\sqrt{n_f}} \sum_{k,s=0}^{n_f-1} \sum_{\substack{m\in S_k \\ n\in\mathbb{Z}_N}} c_{mn} e^{2\pi iks/n_f}|m\rangle_A \otimes |x_r\rangle_a \otimes |n \oplus f_k\rangle_B \otimes |x_s\rangle_b . \tag{3.10}$$

Step 6. Bob now performs a computational basis measurement on b. On obtaining the result x_s, where $s \in \{0, \ldots, n_f - 1\}$, the total state is transformed as

$$|\Phi_{5r}\rangle \mapsto |\Phi_{6rs}\rangle = \sum_{k=0}^{n_f-1} \sum_{\substack{m\in S_k \\ n\in\mathbb{Z}_N}} c_{mn} e^{2\pi iks/n_f}|m\rangle_A \otimes |x_r\rangle_a \otimes |n \oplus f_k\rangle_B \otimes |x_s\rangle_b \tag{3.11}$$

and he communicates the value of s to Alice. This requires him to send her $\log_2(n_f)$ bits of classical information.

Step 7. Alice now uses the, in general degenerate, unitary phase shift operator $T = \Sigma_{k=0}^{n_f-1} e^{-2\pi ik/n_f} P_k$. Knowing s, she applies the operator T^s to A. This results in the transformation $|\Phi_{6rs}\rangle \mapsto |\Phi_{7rs}\rangle$, where

$$\begin{aligned} |\Phi_{7rs}\rangle &= \sum_{k=0}^{n_f-1} \sum_{\substack{m\in S_k \\ n\in\mathbb{Z}_N}} c_{mn}|m\rangle_A \otimes |x_r\rangle_a \otimes |n \oplus f_k\rangle_B \otimes |x_s\rangle_b \\ &= (U_f|\Phi\rangle)_{AB} \otimes |x_r\rangle_a \otimes |x_s\rangle_b, \end{aligned} \tag{3.12}$$

which is the desired transformation of the state of AB. The existence of this protocol for the distributed implementation of the standard oracle operator U_f, with the specified resources together with the lower capacity bounds in Eqs. (2.7) and (2.12) and inequalities (2.1)–(2.3), establishes that all six quantities in these latter inequalities are equal to $\log_2(n_f)$ [13]. We also see from Eq. (2.4) that when f is a permutation of degree M, the bidirectional classical capacity $C_{C\leftrightarrow}(U_f)$ is equal to $2\log_2(n_f)$ bits and that the bidirectional classical communication protocol we described is optimal.

IV. DISCUSSION

There are several points to be made about this distributed protocol. First, it generalizes earlier work on the distributed implementation of the controlled-NOT (CNOT) gate [2,4,5]. In fact, this unitary gate is the standard oracle operator corresponding to the one-bit identity function. Our protocol has interesting security properties. The actual classical data that Alice and Bob send to each other consists of random measurement results. It follows that if they wish to use U_f to send classical information to each other, this will be concealed from an eavesdropper listening to their classical transmissions. Also, we see that in step 4, Bob effectively implements the oracle locally. Only this step makes reference to the details of the function f, which even Alice doesn't have to know for the successful implementation of U_f. The details of f will also be concealed from a potential eavesdropper on the classical transmissions.

It is also worth mentioning that this implementation protocol is always at least twice as efficient, with respect to the consumption of all resources, as the bidirectional teleportation protocol which can be used for the distributed implementation of any bipartite operation, and is optimal for some of them, for example, the SWAP and double CNOT operations [3–5]. This protocol operates by having one party, say Alice, teleport the state of her system to the other, Bob, upon which Bob is able to perform any global operation locally. The procedure concludes with Bob teleporting back to Alice the transformed state of her system. From the well-known properties of quantum teleportation, we easily see that for two quantum systems, the smallest of which (assumed here to be Alice's) has Hilbert space dimension D, this protocol consumes $2\log_2(D)$ ebits of entanglement and $2\log_2(D)$ bits of classical capacity in each direction.

To implement a standard oracle operator this way, we note that n_f is no greater than the dimensionalities of either Alice's or Bob's Hilbert spaces. Hence, $n_f \leqslant D$ and we can easily see by comparing the above resources for bidirectional teleportation with those required to implement the protocol of the preceding section that the latter is always at least twice as efficient as the former with respect to each of these resources.

We also point out that this protocol simplifies when f is a permutation on $\mathbb{Z}_M$. When this is so, $M=N=n_f$ and all four quantum systems have identical Hilbert spaces. The projectors P_k have rank-one and project onto all of the computational basis states in $\mathcal{H}_M$. One further curious property of permutations is the ease with which their standard oracle operators can be seen to be locally equivalent. Kashefi *et al.* [10] noted that for any permutation f on $\mathbb{Z}_M$, one can define the unitary minimal oracle operator $Q_f=\Sigma_{x\in\mathbb{Z}_M}|f(x)\rangle\langle x|$, which is related to U_f through $U_f=(Q_f^{\dagger}\otimes 1_M)U_{\mathrm{ID}}(Q_f\otimes 1_M)$. Here, U_{ID} is the standard oracle operator corresponding to the $\mathbb{Z}_M \mapsto \mathbb{Z}_M$ identity function. All standard oracle operators for permutations of degree M are therefore interconvertible with local unitary operations. It follows that the minimum nonlocal resources to implement these operators and their corresponding capacities are equal.

To conclude, we have studied numerous aspects of the distributed implementation of standard oracle operators. These arise frequently in the context of quantum algorithms and the results presented here will be useful in relation to distributed quantum computation. It is also to be expected that the methods used to establish the minimum nonlocal implementation resources and capacities of standard oracle operators will be useful in a more general context. In particular, the optimal distributed protocol for standard oracle operators has the potential to be modified for more general unitary operators.

ACKNOWLEDGMENTS

I would like to thank Timothy Spiller and Bill Munro for helpful discussions and comments on the manuscript and also Martin Plenio for many enjoyable conversations about this topic. Part of this work was carried out at NICT, Tokyo and I would like to thank Masahide Sasaki and his group for their hospitality. This work was supported by the EU project QAP.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[2] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).

[3] A. Chefles, C. R. Gilson, and S. M. Barnett, Phys. Rev. A **63**, 032314 (2001).

[4] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000).

[5] D. Collins, N. Linden, and S. Popescu, Phys. Rev. A **64**, 032302 (2001).

[6] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).

[7] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin, IEEE Trans. Inf. Theory **49**, 1895 (2003).

[8] M. S. Leifer, L. Henderson, and N. Linden, Phys. Rev. A **67**, 012306 (2003).

[9] R. Van Meter, K. Nemoto, and W. J. Munro, IEEE Trans. Comput. **56**, 1643 (2007).

[10] E. Kashefi, A. Kent, V. Vedral, and K. Banaszek, Phys. Rev. A **65**, 050304(R) (2002).

[11] A. Chefles, A. Kitagawa, M. Takeoka, M. Sasaki, and J. Twamley, J. Phys. A **40**, 10183 (2007).

[12] D. T. Pegg and S. M. Barnett, Phys. Rev. A **39**, 1665 (1989).

[13] It is noteworthy that the entangling capacity $E_C(U_f)$ can also be deduced from the general inequality $E_C(U)\leqslant\log_2[\mathrm{Sch}(U)]$ obtained by Bennett *et al.*, [7] for an arbitrary bipartite unitary operator U, together with our entanglement creation protocol and our observation that $\mathrm{Sch}(U_f)=n_f$.