Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity

Hoi-Kwong Lo
MagiQ Technologies Incorporated, 275 Seventh Avenue, 26th Floor, New York, New York 10001
(Received 28 January 2000; published 16 June 2000)

We study the amount of classical communication needed for distributed quantum-information processing. In particular, we introduce the concept of ''remote preparation'' of a quantum state. Given an ensemble of states, Alice's task is to help Bob in a distant laboratory to prepare a state of her choice. We find several examples of an ensemble with an entropy S where the remote preparation can be done with a communication cost lower than the amount $(2S)$ required by standard teleportation. We conjecture that, for an *arbitrary* N-dimensional *pure* state, its remote preparation requires $2\log_2 N$ bits of classical communication, as in standard teleportation.

PACS number(s): 03.67.Hk

I. INTRODUCTION AND MOTIVATION

There are two main motivations for studying the classical-communication cost in quantum-information processing (CCCIQIP). The first motivation is to better understand the fundamental laws of quantum-information processing. The second is the fact that CCCIQIP can be regarded as a natural generalization of quantum-communication complexity, a subject of much recent interest.

A. First motivation

Quantum-information theory—the synthesis of quantum mechanics with information theory—has been a subject of much recent interest. It is now known that novel phenomena including teleportation [1] and dense coding [2] can occur when the laws of quantum mechanics are invoked in information processing. To better understand these diverse exotic phenomena, it is important to derive the fundamental laws of quantum-information processing.

Until recently, it was customary to ignore the classical-communication cost in quantum-information processing. The motivation was that classical communication is ''cheap'' whereas quantum communication and entanglement are expensive. However, as emphasized in [3], in applications such as dense coding [2], classical-communication cost is of primary interest and it would be totally inconsistent to ignore it. In summary, it is important to take full consideration of classical-communication cost in the study of quantum-information processing.

Some examples of CCCIQIP (for example, ''remote preparation'' to be introduced in this paper) can also be regarded as a refinement of Schumacher's coding theorem [4] in which information is decomposed into two parts: (a) a quantum piece (prior entanglement) and (b) a classical piece (subsequent classical communication). In contrast, in the standard Schumacher coding theorem, quantum information is transmitted directly via quantum bits (qubits).

B. Second motivation

In contrast to the lack of interest in classical-communication cost shown in the quantum community, classical-communication cost is an important subject in theoretical computer science. It is given the name ''communication complexity.'' For example, two or more parties with distributed private inputs $i_1, i_2, \ldots, i_N$ would like to cooperate to compute a function $f(i_1, i_2, \ldots, i_N)$. (For instance, in an appointment scheduling problem, two distant parties would like to find a date when both are free.) They do so by sending classical bits to each other. The goal of communication complexity is to study the number of classical bits of communication needed. Of particular interest is the limiting case when the problem ''size'' is big. (For instance, in the appointment scheduling problem, the number of dates under consideration is large.) Classical-communication complexity can be regarded as the study of classical-communication resource (classical bits) in a classical problem.

Recently, there has been much interest in using *quantum* resources, namely, prior entanglement, to reduce the communication complexity of a classical function. While for some problems this is now known to allow a huge reduction, problems such as the inner product function have been shown to forbid any saving. Quantum-communication complexity [5] can, therefore, be regarded as the study of entanglement-enhanced communication complexity of a *classical* function.

In quantum-information processing, a new complication arises: the input and output states may be nonclassical. The simplest example is an entangled state. (A more subtle form of nonlocality without entanglement also exists [6].) The study of classical-communication cost in quantum-information processing can, thus, be regarded as a natural generalization of quantum-communication complexity by allowing the inputs and outputs to be (possibly nonseparable) quantum states, rather than classical ones.

C. Prior work

There are a number of prior works. The first paper on the subject of CCCIQIP is probably the seminal teleportation paper [1], in which it is shown that an arbitrary unknown state (possibly entangled with an external system) in an N-dimensional Hilbert space can be transmitted by the dual

usage of prior entanglement and $2\log_2 N$ classical bits of communication.[1]

Notice that, in the classical case, if the value of the input (i,j) and the deterministic output $f(i,j)$ are fixed and given beforehand, the classical-communication complexity is trivially zero. The quantum case (CCCIQIP) is strikingly different. Even if Alice and Bob know exactly their fixed input Ψ and output Φ states, the manipulation of a bipartite state Ψ into another bipartite Φ state may still require a nontrivial amount of classical communication.[2] The intuitive reason behind this result is that a quantum state is generally entangled. Since it cannot be written as a direct product of pure states, it cannot be prepared by bilocal operations. See also [6].

Interestingly, in some situations the classical-communication cost can be made to vanish in the asymptotic limit [3]. Consider the situation of entanglement dilution [8]: two distance observers Alice and Bob who share a large number NS of singlets (i.e., maximally entangled states) would like to dilute them into N pairs of the nonmaximally entangled state $a|00\rangle+b|11\rangle$ whose entropy of entanglement, $-|a|^2\log_2|a|^2-|b|^2\log_2|b|^2$, is equal to S. The standard scheme [8] involves a teleportation step and, thus, has a classical communication cost proportional to N. Nevertheless, it was subsequently shown in [3] that entanglement dilution can be done in the asymptotic limit with a vanishing amount of classical communication. As a consequence, entanglement is, indeed, a fungible resource. That is to say that the same amount of two-party pure state entanglement in different forms or concentrations can truly be regarded as equivalent because they are interconvertible into each other [8], with a negligible amount of classical-communication cost between the two parties [3]. A key point of their argument is that there is a huge degree of degeneracy in the Schmidt coefficients [9] of the relevant bipartite state.

Recently, important discussions on the classical communication cost of entanglement manipulations has also been presented by Nielsen [10,11].

D. Related work

CCCIQIP is also related to other subjects. For instance, Brassard, Cleve, and Tapp [12] have studied the issue of simulating entanglement with classical communication. Another related subject is quantum nonlocality without entanglement [6]. This concerns the opposite question, namely, the crucial role of quantum entanglement in a rather novel context. CCCIQIP and many other studies can be regarded as the investigations of limiting cases of quantum-information processing, in which the cost of one type of resource (entanglement or classical communication) is often ignored.

E. Main result

Our main results are as follows. First of all, as first pointed out by Gottesman [13], the usual teleportation [1] can be decomposed into a two-stage process. Starting with a pure state $a|0\rangle+b|1\rangle$ on Alice's side and an Einstein-Podolsky-Rosen (EPR) pair shared between Alice and Bob, the first stage will lead to an entangled state $a|00\rangle+b|11\rangle$ shared between Alice and Bob. The second stage will lead to a state $a|0\rangle+b|1\rangle$ fully in Bob's hand. Moreover, each stage requires a single bit of classical communication. (This works not only for a pure initial state, but also for a qubit that is entangled with an ancilla.)

Second, we give a simple procedure that halves the amount of classical-communication cost in entanglement dilution compared to even the improved scheme in [3]. This is done by noting that only the first stage of teleportation is needed for entanglement dilution. (The second step can simply be skipped.)

Third, we move on to consider the following general problem, which we shall call ''remote preparation,'' following Popescu [14]. Suppose Alice and Bob initially share some entanglement. We only allow Alice to send classical bits to Bob. Alice's goal is to help Bob to prepare some pure state chosen from some specific preagreed distribution. The key difference between remote preparation and the usual teleporation is that, unlike teleportation, we assume in remote preparation that Alice knows the precise state of the object that she is trying to help Bob to prepare. (Putting it differently, Alice is given an infinite number of copies of the pure state and is required to transmit only one to Bob.) In addition, the preagreed distribution may not be totally random. We have some theorems and a conjecture. With some appropriate constraints on the distribution, one can use our theorems to reduce the classical communication cost below what is required in teleportation even in the asymptotic case. In other words, remote preparation of constrained states in some cases offers a discount rate compared to full-blown teleportation of an ensemble with the same amount of entropy. This is *a priori* a surprising result. We conjecture that such a reduction in classical-communication cost is impossible for an unconstrained state.

II. TWO-STAGE TELEPORTATION

Suppose Alice would like to transmit an unknown qubit $a|0\rangle_q+b|1\rangle_q$ to Bob. Instead of sending it directly to Bob via a quantum-communication channel, Alice can achieve the same goal by using a classical channel, provided that Alice and Bob initially share some entanglement. This process is called teleportation [1]. Transmission of each qubit requires two classical bits of communication. (It can be shown that teleportation works not only for pure states, but also for states that are entangled with ancillas.) In what follows, the well-known teleportation process will be decomposed into two steps. The following result was pointed out by Gottesman [13].

[1]The amount of classical communication, $2\log_2 N$ bits, needed is optimal. This follows from dense coding [2]. If transmission of an arbitrary (possibly entangled) N-dimensional state could be done with fewer than $2\log_2 N$ bits of classical communication, then causality would be violated.

[2]This result is not difficult to prove, using the idea of the proof in [7] that entanglement manipulation strategies with one-way communication are generally more powerful than those with no communication.

Theorem 1: Two-stage teleportation. Suppose Alice and Bob share an EPR pair and that Alice is given an unknown qubit $a|0\rangle_q+b|1\rangle_q$ in her hand. There exists a two-stage process for transmitting the unknown qubit to Bob such that, on completion of the first step, Alice shares with Bob an entangled state $a|00\rangle_{AB}+b|11\rangle_{AB}$ and, on completion of the second step, the state $a|0\rangle_B+b|1\rangle_B$ is fully in Bob's hand. Furthermore, each step requires a single bit of classical communication.

Remark A. Essentially the same procedure works for an initial state that is entangled with an ancilla.

Remark B. An analogous procedure works for an N-dimensional state with $\log_2 N$ classical bits of communication needed for each step.

Proof. Step 1. Alice applies an exclusive OR (XOR) between the unknown qubit q and her member A of the EPR pair that she shares with Bob, with the unknown qubit as the target qubit. Since

$$\begin{aligned} |x\rangle_q|0\rangle_A &\rightarrow |x\rangle_q|0\rangle_A, \\ |x\rangle_q|1\rangle_A &\rightarrow |x+1\rangle_q|1\rangle_A, \end{aligned} \tag{1}$$

one gets

$$\begin{aligned} a|0\rangle_q+b|1\rangle_q(|00\rangle_{AB}+|11\rangle_{AB}) \rightarrow |0\rangle_q(a|00\rangle_{AB}+b|11\rangle_{AB}) \\ +|1\rangle_q(b|00\rangle_{AB} \\ +a|11\rangle_{AB}). \end{aligned} \tag{2}$$

Now, Alice measures the qubit q and sends the outcome, a single bit, via a classical-communication channel to Bob. If the outcome is 0, Alice and Bob share $a|00\rangle_{AB}+b|11\rangle_{AB}$ as required. If the outcome is 1, they share $b|00\rangle_{AB}+a|11\rangle_{AB}$. Alice and Bob can now apply a bilocal unitary transformation $|0\rangle\rightarrow|1\rangle$ to obtain the desired state $a|00\rangle_{AB}+b|11\rangle_{AB}$.

Step 2. Alice applies a Hadamard transformation on her member of the shared pair. She then measures it and sends the outcome to Bob. On receiving Alice's outcome, Bob applies a unitary transformation on his member of the shared pair to recover the unknown qubit. Mathematically, the Hadamard transform is, up to an overall normalization,

$$\begin{aligned} |0\rangle_A &\rightarrow |0\rangle_A+|1\rangle_A, \\ |1\rangle_A &\rightarrow |0\rangle_A-|1\rangle_A. \end{aligned} \tag{3}$$

Therefore,

$$\begin{aligned} a|00\rangle_{AB}+b|11\rangle_{AB} &\rightarrow a(|0\rangle_A+|1\rangle_A)|0\rangle_B \\ &\quad +b(|0\rangle_A-|1\rangle_A)|1\rangle_B \\ &= |0\rangle_A(a|0\rangle_B+b|1\rangle_B) \\ &\quad +|1\rangle_A(a|0\rangle_B-b|1\rangle_B). \end{aligned} \tag{4}$$

Now Alice measures A. If she obtains 0 as the outcome, then Bob has $a|0\rangle_B+b|1\rangle_B$ as required. Similarly, if Alice obtains 1 as the outcome, Bob then has $a|0\rangle_B-b|1\rangle_B$ which can now be converted to $a|0\rangle_B+b|1\rangle_B$ by applying the Pauli operator σ_z. Q.E.D.

For experts in stabilizer codes, the above result is rather trivial. However, theorem 1 has a simple application on entanglement dilution.

Corollary. One can halve the amount of classical communication needed for entanglement dilution.

Proof. For entanglement dilution, the desired output state of Bob is entangled with Alice. Therefore, all that is required is the first step of the two-step teleportation procedure. By skipping the second step, one saves half of the classical-communication cost.

Remark C. The above corollary 2 applies not only to a naive entanglement dilution scheme, but also to the advanced scheme proposed in [3], which requires a vanishing amount of classical communication in the asymptotic limit.

III. REMOTE PREPARATION OF CONSTRAINED STATES

So far our discussion has been restricted to teleportation. It turns out that the idea of decomposing the transmission process of quantum information into two parts, as employed in Theorem 1, is useful in a more general context. In this section, we illustrate this point by considering a similar but more general procedure for transmitting quantum information, which has been called ''remote preparation'' by Popescu [14]. Suppose Alice and Bob initially share some entanglement and subsequently Alice can send only classical bits to Bob. The goal of remote preparation is for Alice to help Bob to prepare some pure state chosen from some specific preagreed distribution. The big difference between remote preparation and the usual teleporation is that, unlike teleportation, in remote preparation, Alice knows the precise pure state of the object that she is trying to help Bob to prepare. (Equivalently, Alice is given an infinite number of copies of the pure state and is required to transmit only one to Bob.) Another difference is that, in general, the preagreed distribution does not need to be random. We have the following asymptotic (large-N) result.

Theorem 2. Suppose Alice and Bob are given the values of a and b and that they satisfy $|a|^2+|b|^2=1$. Suppose further that Alice and Bob share NS e-bits of entanglement (defined in [15]), where $S=-|a|^2\log_2|a|^2-|b|^2\log_2|b|^2$ for large N. Alice would like to help Bob to remotely prepare N objects, each of the form $a|0\rangle+be^{i\theta_i}|1\rangle$. Here the θ_i's are known to Alice only. We claim that NS bits of classical communication is sufficient.

Proof. By entanglement (concentration and) dilution [8,3], Alice and Bob can convert the NS e-bits of entanglement into N pairs of $a|00\rangle+b|11\rangle$ with a very high fidelity (and with an asymptotically vanishing amount of classical communication [3]). Now, consider a two-stage remote preparation process in complete analogy with two-stage teleporation (i.e., from $a|0\rangle_a+be^{i\theta_i}|1\rangle_a$ to $a|00\rangle_{AB}+be^{i\theta_i}|11\rangle_{AB}$ and then $a|0\rangle_B+be^{i\theta_i}|1\rangle_B$). Since Alice and Bob already share $a|00\rangle+b|11\rangle$, they now have a short-cut to step 1. Indeed, they can convert $a|00\rangle+b|11\rangle$ into

$a|00\rangle+be^{i\theta_i}|11\rangle$, for each i, with no communication at all: Using her knowledge of θ_i, this can be done by Alice's rotating the phase of $|1\rangle$ under her control, i.e., $|1\rangle \rightarrow e^{i\theta_i}|1\rangle$. Now each of Alice and Bob then performs quantum data compression [4] on his/her system, compressing it into NS qubits. (Notice that S is the von Neumann entropy of Alice/Bob's system.) Alice and Bob then perform the second step of the two-step teleportation process—more precisely, its higher dimensional generalization as noted in Remark B—on the typical space, which has a dimension $2^{O(NS)}$. This requires NS classical bits and zero e-bits. Bob can now perform quantum date dilution to recover the system. Q.E.D.

Remark D. As far as classical-communication cost is concerned, our result is optimal. That is to say that NS bits are necessary for the remote preparation of the above ensemble. The reason is the following. S is the von Neumann entropy of Alice's ensemble (i.e., a random ensemble of pure states of the form $a|0\rangle_B+be^{i\theta_i}|1\rangle_B$). By Holevo's theorem [16], the quantum signals can be used to transmit NS classical bits to Bob. So, if there were a way to transmit the quantum signals to Bob with fewer than NS classical bits, causality would be violated.

Remark E. The special case where $|a|=|b|$ has also been proved by various people including Popescu [17].

So far, our discussion has focused on the classical-communication cost. What about the amount of quantum resource (entanglement) for remote preparation? We have the following conjecture.

Conjecture 1. For any remote preparation procedure that uses only NS bits, NS e-bits is the minimal amount of entanglement needed for any remote preparation procedure for the N signals of the form $a|0\rangle+be^{i\theta_i}|1\rangle$ where a and b are known to Alice and Bob and the θ_i's are known to Alice only, and $S=-|a|^2\log_2|a|^2-|b|^2\log_2|b|^2$.

We remark that the proviso—that uses only NS bits—is necessary. Without such a proviso, fewer e-bits can be used at the expense of a large number of bits. For example, Alice can divide the latitude into two semicircular segments, $0 \leqslant \theta \leqslant \pi$ and $\pi \leqslant \theta \leqslant 2\pi$. Now, she encodes a state by two pieces, one classical and one quantum. For a state in the first segment, she encodes it by a classical bit 0, together with the state as it is. For a state in the second segment, she encodes it by a classical bit 1 together with the rotated $a|0\rangle+be^{i(\theta_i-\pi)}|1\rangle$, which is a state in the first segment. Notice that the quantum states, now all being in the same segment, have a smaller entropy than NS e-bits. A similar reasoning can be used to reduce the e-bit cost in remote preparation even further at the expense of increasing classical bit cost.

IV. FURTHER EXAMPLES OF REMOTE PREPARATION

In Theorem 2, the moduli a and b of the coefficients of each state are independent of i. One might wonder if this is a necessary condition for the reduction in classical-communication cost. The answer is no. Indeed, in the following theorem, Theorem 3, we give an example in which reduction of classical-communication cost happens even when the moduli of the coefficients vary for the states in the ensemble. What is actually needed is some constraint on those coefficients.

Theorem 3. Suppose Alice and Bob initially share entanglement and only a classical communication channel. Alice would like to help Bob to prepare a set of N normalized states, where each state, say the ith one, is of the form $a_i|0\rangle+b_i|1\rangle+c_i|2\rangle+d_i|3\rangle$ with

$$|a_i|^2+|b_i|^2=2e^2 \tag{5}$$

for all i's. Here, e is known in advance to both Alice and Bob whereas only Alice knows the individual coefficients a_i, b_i, c_i, and d_i of each state. We claim that only $N(1+S)$ bits of classical communication will be sufficient for such remote preparation, where $S=-2\{e^2\log_2 e^2+(0.5-e^2)[\log_2(0.5-e^2)]\}=1+H(2e^2)\geqslant 1$ [here, we define $H(d)=-d\log_2 d-(1-d)\log_2(1-d)$] is the entropy of the ensemble.

Remark F. Note that the standard teleportation scheme would require $2NS$ bits of classical communication. Since $S>1$ (except for $e^2=0$ or 1/2), remote preparation always provides some saving in classical-communication cost over standard teleportation.

Proof. Our proof is analogous to that of Theorem 2. Let us divide the remote preparation process into two steps. Starting from $a_i|0\rangle+b_i|1\rangle+c_i|2\rangle+d_i|3\rangle$ in Alice's hand, the goal of the first step is to obtain an entangled state shared between Alice and Bob, $a_i|00\rangle+b_i|11\rangle+c_i|22\rangle+d_i|33\rangle$. The goal of the second step is to obtain $a_i|0\rangle+b_i|1\rangle+c_i|2\rangle+d_i|3\rangle$ in Bob's hand.

Step 1. Starting with their NS ebits, by using entanglement (concentration and) dilution and their common knowledge of e, Alice and Bob can, with a high fidelity, share N objects of the form

$$\psi=e|00\rangle_{AB}+e|11\rangle_{AB}+f|22\rangle_{AB}+f|33\rangle_{AB}, \tag{6}$$

where $f^2+e^2=0.5$, with an asymptotically vanishing amount of classical communication [3,8]. In what follows, we describe a procedure that allows Alice and Bob to manipulate ψ into $a_i|00\rangle_{AB}+b_i|11\rangle_{AB}+c_i|22\rangle_{AB}+d_i|33\rangle_{AB}$ using only a single classical bit of communication.

First of all, Alice prepares a two-state ancilla in the initial state $|0\rangle_a$. She then couples it with her system A and evolves it with a unitary transformation:

$$\begin{aligned} e|0\rangle_a|0\rangle_A &\rightarrow (a_i|0\rangle_a+b_i|1\rangle_a)|0\rangle_A, \\ e|0\rangle_a|1\rangle_A &\rightarrow (b_i|0\rangle_a+a_i|1\rangle_a)|1\rangle_A, \\ f|0\rangle_a|2\rangle_A &\rightarrow (c_i|0\rangle_a+d_i|1\rangle_a)|2\rangle_A, \\ f|0\rangle_a|3\rangle_A &\rightarrow (d_i|0\rangle_a+c_i|1\rangle_a)|3\rangle_A. \end{aligned} \tag{7}$$

(It is easy to check that the transformation can be made unitary. Also, with her knowledge of a_i, b_i, c_i, and d_i, Alice can indeed implement such a unitary transformation.)

Now, starting with

$$|0\rangle_a(e|00\rangle_{AB}+e|11\rangle_{AB}+f|22\rangle_{AB}+f|33\rangle_{AB}), \tag{8}$$

the unitary transformation gives

$$|0\rangle_a(a_i|00\rangle_{AB}+b_i|11\rangle_{AB}+c_i|22\rangle_{AB}+d_i|33\rangle_{AB}) + |1\rangle_a(b_i|00\rangle_{AB}+a_i|11\rangle_{AB}+d_i|22\rangle_{AB}+c_i|33\rangle_{AB}). \tag{9}$$

Now Alice measures the state of the ancilla a and sends the one-bit outcome to Bob. If the outcome is 0, the first step of remote preparation is already done. If the outcome is 1 instead, Alice and Bob can simply apply a bilocal unitary transformation to obtain what is desired. Since each of the N signals requires one classical bit, N classical bits are sent in the first step.

Step 2. As in Theorem 2, Alice applies quantum data compression to the N quantum signals, compressing them into NS qubits. She can then proceed with the second step of the remote preparation in the same way as the second step of the two-stage teleportation, thus sending Bob NS classical bits. Adding the classical communication cost in the two steps, we get $N+NS=N(1+S)$ bits. Q.E.D.

In Theorem 3, the four coefficients a_i, b_i, c_i, and d_i are partitioned into two sets with *equal* numbers of elements, $\{a_i,b_i\}$ and $\{c_i,d_i\}$ and the constraint Eq. (5) lies in the sum of moduli squared of each set. [Compare the degeneracy in Schmidt decomposition of $\psi=e|00\rangle_{AB}+e|11\rangle_{AB}+f|22\rangle_{AB}+f|33\rangle_{AB}$ in Eq. (6).] One might wonder if a partition into sets with equal numbers of elements is a necessary condition for reducing classical communication cost. The answer is no, thanks to the following lemma.

Lemma 1. Suppose that Alice and Bob share initial entanglement and a classical communication channel. Let the $|l\rangle$'s be an orthonormal basis of some Hilbert space $\mathcal{H}$. Let $I=I_1\cup I_2\cup\cdots\cup I_M$ be a partition of the set of indices, i.e., l's. Suppose Alice would like to help Bob to prepare N objects, each of which, say the ith one,

$$\psi_i=\sum_l a_{li}|l\rangle, \tag{10}$$

is a pure state in $\mathcal{H}$ and that, for each set $m\in\{1,2,\cdots,M\}$, the sum of moduli squared of its elements satisfies

$$\sum_{k\in I_m}|a_{ki}|^2=c_m \tag{11}$$

for all the states i in the ensemble. Here, the sets I_m and the values c_m are known to Alice and Bob in advance while only Alice knows the individual coefficients a_{li}. We claim that the remote preparation can be done with $N[(\log_2 d)+S]$ bits of classical communication, where $d=\mathrm{lcm}(|I_1|,|I_2|,\ldots,|I_M|)$ and S is the maximal entropy of the ensemble consisting of states satisfying the form Eq. (11).

Proof. To illustrate the idea of the proof, it suffices to consider a simple example where $I=I_1\cup I_2$, $|I_1|=2$, and $|I_2|=3$. (In this particular example, the scheme requires a larger amount of classical-comunication cost than direct teleportation and is, therefore, not very useful.)

Step 1. By entanglement (concentration and) dilution, Alice and Bob can manipulate their initially shared entanglement into N copies of the form

$$\alpha|00\rangle+\alpha|11\rangle+\beta|22\rangle+\beta|33\rangle+\beta|44\rangle, \tag{12}$$

where $2|\alpha|^2=c_1$ and $3|\beta|^2=c_2$. For each quantum signal, Alice now prepares an ancilla of dimension $d=\mathrm{lcm}(|I_1|,|I_2|,\ldots,|I_M|)$ in the state $|0\rangle_a$. In the current special case, $d=\mathrm{lcm}(2,3)=6$. She now couples the ancilla with each (say the ith) quantum signal. In the current special case, she now evolves her combined system of ancilla and the ith quantum signal with the following unitary transformation:

$$\begin{aligned}
|0\rangle_a|0\rangle_A&\rightarrow(|0\rangle+|1\rangle+|2\rangle)(a_{0i}|0\rangle+a_{1i}|1\rangle)|0\rangle_A,\\
|0\rangle_a|1\rangle_A&\rightarrow(|0\rangle+|1\rangle+|2\rangle)(a_{1i}|0\rangle+a_{0i}|1\rangle)|1\rangle_A,\\
|0\rangle_a|2\rangle_A&\rightarrow(a_{2i}|0\rangle+a_{3i}|1\rangle+a_{4i}|2\rangle)(|0\rangle+|1\rangle)|2\rangle_A,\\
|0\rangle_a|3\rangle_A&\rightarrow(a_{3i}|0\rangle+a_{4i}|1\rangle+a_{2i}|2\rangle)(|0\rangle+|1\rangle)|3\rangle_A,\\
|0\rangle_a|4\rangle_A&\rightarrow(a_{4i}|0\rangle+a_{2i}|1\rangle+a_{3i}|2\rangle)(|0\rangle+|1\rangle)|4\rangle_A.
\end{aligned} \tag{13}$$

Here, the ancilla is further divided into two subsystems, on the right hand side of the equations. From the proof of Theorem 3, it is not too hard to see that, by (i) Alice measuring the ancilla and sending the outcomes to Bob, and (ii) Alice and Bob performing a bilocal unitary transformation, Alice and Bob can achieve the first step of remote preparation, i.e., prepare an entangled state of the form $a_{0i}|00\rangle_{AB}+a_{1i}|11\rangle_{AB}+a_{2i}|22\rangle_{AB}+a_{3i}|22\rangle_{AB}+a_{4i}|44\rangle_{AB}$. For each signal, the first step requires $\log_2 d$ bits of classical communication.

Here we sketch the proof for the general case. Since, for each m, $|I_m|$ divides d, the dimension of the ancilla that Alice has prepared, she can divide the ancilla into two subsystems of dimensions $|I_m|$ and $d/|I_m|$, respectively. Call them systems anc_1^m and anc_2^m, respectively. Equivalently, for each m, she can label her ancilla basis vectors by a double index. We emphasize that, *unlike the simple case presented above*, in the general case, this double index is a *local* labeling depending on m. Denote $|I_m|$ by R and $d/|I_m|$ by T. Let us use the double index $\{s,t\}$ to label a basis for the decomposition locally. Let also $I_m=\{k_1,k_2,\ldots,k_R\}$. For $1\leqslant r\leqslant R$, the unitary transformation maps the initial state

$$|0\rangle_a|k_r\rangle_A \tag{14}$$

into

$$\left(\sum_s a_{k_{r+s \bmod R}}|s\rangle_{\mathrm{anc}_1^m}\right)\left(\sum_t\frac{1}{\sqrt{T}}|t\rangle_{\mathrm{anc}_2^m}\right)|k_r\rangle_A, \tag{15}$$

where the ancilla is locally decomposed into two subsystems anc_1^m and anc_2^m and its state is labeled by a double index (s,t). Suppose Alice measures the ancilla and sends her outcome to Bob. The outcome can be written, locally for each

m, as a pair s and t. s contains the information needed for the completion of the first step of remote preparation because it tells Alice and Bob which bilocal unitary transformation to apply to their states in the subspace spanned by $\{|k_r\rangle_A | k_r \in I_m\}$. On the other hand, t is unimportant.

Step 2. As in the proof of Theorem 3, Alice applies quantum data compression to her N signals, compressing them into NS qubits. She then performs the second step of teleportation, thus sending NS classical bits to Bob. By combining the two steps, a total of $N[(\log_2 d)+S]$ classical bits are used. Q.E.D.

Theorem 4. Suppose that Alice and Bob share initial entanglement and a classical-communication channel. Alice would like to help Bob to prepare N_{tot} objects, each of which, say the ith one, is of the form $a_i|0\rangle+b_i|1\rangle+ce^{i\theta_i}|2\rangle$, where c is known to Alice and Bob in advance, but a_i, b_i, and θ_i are known to Alice only. We claim that $N_{tot}(S+1-|c|^2)$ classical bits will be sufficient for such remote preparation. Here, $S=-[2d^2\log_2 d^2+c^2\log_2 c^2]$ with $d^2=(1-c^2)/2$.

Proof.

We set $N_{tot}=NN_1$ where both N and N_1 are large and apply Lemma 1 to prove Theorem 4. To do so, it suffices to show that, in the *typical* space of N_1 signals, the expression d in Lemma 1 is given by $\log_2 d=\log_2[\mathrm{lcm}(|I_1|,|I_2|,\ldots,|I_M|)]=N_1(1-|c|^2)$. The details are as follows.

The Hilbert space of N_1 signals is spanned by the basis vectors $|x_1,x_2,\ldots,x_{N_1}\rangle$. A normalized basis of the *typical* space (the $|I\rangle$'s in Lemma 1) is given by vectors of the form $|x_1,x_2,\ldots,x_{N_1}\rangle$, where between $N_1(|c|^2-\delta)$ and $N_1(|c|^2+\delta)$ of the x_i's take the value of 2, for some small δ. Let us group those $|x_1,x_2,\ldots,x_{N_1}\rangle$ with the same number and locations of 2's together. Within the same group, each of the x_i's that are not equal to 2 can take a value of either 0 and 1. Consequently, there are between $2^{N_1(1-|c|^2-\delta)}$ and $2^{N_1(1-|c|^2+\delta)}$ basis vectors in each group. Furthermore, the weight (i.e., the sum of the modulus squared of the wave function) of the subspace corresponding to each group is known in advance to Alice and Bob as required in Eq. (11).

The above discussion is rather abstract and can be made clear by a simple example. Consider the case $N_1=3$ and $c^2=1/2$. A typical space is spanned by basis vectors $|x_1,x_2,x_3\rangle$ where one or two of the x_i's take the value of 2, i.e., $|2,j_i,j_2\rangle$, $|j_1,2,j_2\rangle$, $|j_i,j_2,2\rangle$ as well as $|2,2,j_1\rangle$, $|2,j_1,2\rangle$, and $|j_1,2,2\rangle$, where j_i takes the value of 0 or 1. Therefore, by fixing the number and locations of the 2's, we have partitioned the typical space into six subspaces. Furthermore, the weight of each subspace is fixed in advance and is known to both Alice and Bob. For instance, if $\psi_i=a_i|0\rangle+b_i|1\rangle+ce^{i\theta_i}|2\rangle$, then on expanding $\psi_1\otimes\psi_2\otimes\psi_3$, we find that the projection onto the subspace spanned by, say, $\{|2,j_i,j_2\rangle\}$ is simply

$$ce^{i\theta_1}|2\rangle(a_2|0\rangle+b_2|1\rangle)(a_3|0\rangle+b_3|1\rangle). \tag{16}$$

Its weight is, therefore, simply $c^2(1-c^2)^2$, independent of the values of a_i and b_i. [Cf. Eq. (11).]

In summary, the above grouping generally leads to a partition on the set of basis vectors, $I=I_1\cup I_2\cup\cdots\cup I_M$, where the size of I_i, denoted by $|I_i|$, is between $2^{N_1(1-|c|^2-\delta)}$ and $2^{N_1(1-|c|^2+\delta)}$ and the weight in each induced subspace satisfies Eq. (11). Since $|I_i|$ here is always a power of 2, $d=\mathrm{lcm}(|I_1|,|I_2|,\ldots,|I_M|)$ is also of order $2^{N_1(1-|c|^2+\delta)}$. Q.E.D.

V. CONCLUDING REMARKS

In this paper, we studied the classical-communication cost in quantum-information processing. One motivation of our study is to better understand the fundamental laws of quantum-information processing. Another motivation is the fact that CCCIQIP can be regarded as a generalization of quantum-communication complexity, a subject of much recent interest. Our results are as follows. First, we decomposed the usual teleportation process into a two-step process, a result pointed out by Gottesman. This led us immediately to a simple way to reduce by half the classical-communication cost in entanglement dilution compared to the earlier scheme [3]. After that, we considered the more general question of ''remote preparation,'' a phrase coined by Popescu. Just as in teleportation, Alice and Bob here share prior entanglement and also a classical-communication channel. Alice's goal is to help Bob to prepare some state. Its main difference from the usual teleportation is that we allow Alice to know exactly the pure state that she is trying to help Bob to prepare. The question is whether Alice can somehow reduce the amount of classical communication using her knowledge of the state. It is shown here that, if there are some appropriate constraints on the ensemble of the states that Alice is trying to send, Alice will be able to reduce the classical-communication cost below that of teleportation. We suspect that some constraints on the ensemble are necessary for saving classical-communication cost. Therefore, we have the following conjecture.

Conjecture 2. (Does remote preparation of a general pure state of a qubit require two classical bits of communication?) Suppose Alice and Bob share prior entanglement and a classical-communication channel only. Suppose that Alice is asked to help Bob to prepare N *pure* qubit states $\psi=\psi_1\otimes\psi_2\otimes\cdots\otimes\psi_N$, where $\psi_i=a_i|0\rangle+b_i|1\rangle$ is an arbitrary pure state of a qubit. Here, the a_i and b_i are known to Alice but not Bob. We conjecture that such remote preparation requires $2N$ bits of classical communication.

Remark G. The main differences of the scenario in the above conjecture from that of the usual teleportation are that here we allow only pure states but not entangled states, and that Alice actually knows the state that she is missing.

To put things in perspective, only a few examples of remote preparation have been studied in this paper. It would thus be interesting to consider more general examples and to attempt to derive a general principle for the classical-communication cost of remote preparation. In a more general context, the issue of classical-communication cost of other

processes (such as entanglement manipulations [8,7], entanglement purification [18]) in quantum-information processing deserves careful investigation. Let us conclude by saying that classical-communication cost is only one of several types of resources in quantum-information processing. Ultimately, we expect that the fundamental laws of quantum-information processing will take full account of the various types of resources. A study of the trade-off between qubits and classical-communication cost would be an interesting subject. Let us conclude by saying that it is our hope that the study of classical-communication cost in quantum-information processing in combination with other research avenues including [6,12] will lead us one step closer to the yet unknown fundamental laws of quantum-information processing.

ACKNOWLEDGMENTS

The author particularly thanks D. Gottesman for very helpful discussions and S. Popescu for coining the phrase ''remote preparation.'' Conversations with various researchers including C. H. Bennett, S. Braunstein, H. F. Chau, R. de Wolf, D. DiVincenzo, D. Leung, M. Mosca, M. Nielsen, S. Popescu, T. Spiller, and A. Tapp are also gratefully acknowledged. Parts of this paper were developed from work done while the author was at Hewlett-Packard Laboratories, Bristol.

[1] C.H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] H.-K. Lo and S. Popescu, Phys. Rev. Lett. **83**, 1459 (1999).
[4] B. Schumacher, Phys. Rev. A **51**, 2738 (1995); R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994); H. Barnum, C.A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. A **54**, 4707 (1996).
[5] See, for example, H. Buhrman, R. Cleve, and W. van Dam, e-print quant-ph/9705033.
[6] C.H. Bennett *et al.*, Phys. Rev. A **59**, 1070 (1999).
[7] H.-K. Lo and S. Popescu, e-print quant-ph/9707038.
[8] C.H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996).
[9] See, for example, the Appendix of L.P. Hughston, R. Jozsa, and W.K. Wootters, Phys. Lett. A **183**, 14 (1993).
[10] M.A. Nielsen, Phys. Rev. A (to be published) (e-print quant-ph/9909020).
[11] M. A. Nielsen, Ph.D. thesis, University of New Mexico, 1998 (unpublished).
[12] G. Brassard, R. Cleve, and A. Tapp, Phys. Rev. Lett. **83**, 1874 (1999).
[13] The special case of the result where Alice knows the state of the qubit—which is all that is needed for the subsequent sections—was proved by the author first. Then Daniel Gottesman pointed out that the result is, in fact, general (private communication).
[14] S. Popescu (private communication).
[15] C.H. Bennett, Phys. Today **48**, 24 (1995).
[16] A.S. Holevo, Probl. Inf. Transm. **9**, 117 (1973).
[17] S. Popescu, (private communications).
[18] C.H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996); C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).