Quantum Entanglement and the Communication Complexity of the Inner Product Function

Richard Cleve[1]*, Wim van Dam[2], Michael Nielsen[3], and Alain Tapp[4]**

[1] University of Calgary
Department of Computer Science, University of Calgary, Calgary, Alberta, Canada
T2N 1N4. cleve@cpsc.ucalgary.ca.
[2] University of Oxford and CWI, Amsterdam
Clarendon Laboratory, Department of Physics, University of Oxford, Parks Road, Oxford OX1 3PU, U.K. wimvdam@mildred.physics.ox.ac.uk.
[3] Los Alamos National Laboratory and University of New Mexico
T-6 Theoretical Astrophysics, Los Alamos National Laboratory, U.S.A.
mnielsen@tangelo.phys.unm.edu.
[4] Université de Montréal
Département IRO, C.P. 6128, Succursale Centre-Ville, Montréal, Québec, Canada
H3C 3J7. tappa@iro.umontreal.ca.

Abstract. We consider the communication complexity of the binary inner product function in a variation of the two-party scenario where the parties have an *a priori* supply of particles in an entangled quantum state. We prove linear lower bounds for both exact protocols, as well as for protocols that determine the answer with bounded-error probability. Our proofs employ a novel kind of "quantum" reduction from a quantum information theory problem to the problem of computing the inner product. The communication required for the former problem can then be bounded by an application of Holevo's theorem. We also give a specific example of a probabilistic scenario where entanglement reduces the communication complexity of the inner product function by one bit.

1 Introduction and Summary of Results

The *communication complexity* of a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined as the minimum amount of communication necessary among two parties, conventionally referred to as Alice and Bob, in order for, say, Bob to acquire the value of $f(x,y)$, where, initially, Alice is given x and Bob is given y. This scenario was introduced by Yao [16] and has been widely studied (see [13] for a survey). There are a number of technical choices in the model, such as: whether the communication cost is taken as the worst-case (x,y), or the average-case (x,y) with respect to some probability distribution; whether the protocols are

* Research initiated while visiting the Université de Montréal and supported in part by Canada's NSERC.
** Research supported in part by Canada's NSERC.

C.P. Williams (Ed.): QCQC'98, LNCS 1509, pp. 61–74, 1999.

deterministic or probabilistic (and, for probabilistic protocols, whether the parties have independent random sources or a shared random source); and, what correctness probability is required.

The communication complexity of the *inner product modulo two (IP)* function

$$IP(x, y) = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \bmod 2 \tag{1}$$

is fairly well understood in the above "classical" models. For worst-case inputs and deterministic errorless protocols, the communication complexity is n and, for randomized protocols (with either an independent or a shared random source), uniformly distributed or worst-case inputs, and with error probability $\frac{1}{2} - \delta$ required, the communication complexity is $n - O(\log(1/\delta))$ [7] (see also [13]).

In 1993, Yao [17] introduced a variation of the above classical communication complexity scenarios, where the parties communicate with *qubits*, rather than with bits. Protocols in this model are at least as powerful as probabilistic protocols with independent random sources. Kremer [12] showed that, in this model, the communication complexity of *IP* is $\Omega(n)$, whenever the required correctness probability is $1 - \varepsilon$ for a constant $0 \leq \varepsilon < \frac{1}{2}$ (Kremer attributes the proof methodology to Yao).

Cleve and Buhrman [8] (see also [6]) introduced another variation of the classical communication complexity scenario that also involves quantum information, but in a different way. In this model, Alice and Bob have an initial supply of particles in an entangled quantum state, such as Einstein-Podolsky-Rosen (EPR) pairs, but the communication is still in terms of classical bits. They showed that the entanglement enables the communication for a specific problem to be reduced by one bit. Any protocol in Yao's qubit model can be simulated by a protocol in this entanglement model with at most a factor two increase in communication: each qubit can be "teleported" [3] by sending two classical bits in conjunction with an EPR pair of entanglement. On the other hand, we are aware of no similar simulation of protocols in the entanglement model by protocols in the qubit model, and, thus, the entanglement model is potentially stronger.

In this paper, we consider the communication complexity of *IP* in two scenarios: with prior entanglement and qubit communication; and with prior entanglement and classical bit communication. As far as we know, the proof methodology of the lower bound in the qubit communication model without prior entanglement [12] does not carry over to either of these two models. Nevertheless, we show $\Omega(n)$ lower bounds in these models.

To state our lower bounds more precisely, we introduce the following notation. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a communication problem, and $0 \leq \epsilon < \frac{1}{2}$. Let $Q^*_\varepsilon(f)$ denote the communication complexity of f in terms of *qubits*, where quantum entanglement is available and the requirement is that Bob determines the correct answer with probability at least $1-\varepsilon$ (the $*$ superscript is intended to highlight the fact that prior entanglement is available). Also, let $C^*_\varepsilon(f)$ denote the corresponding communication complexity of f in the scenario where the communication is in terms of *bits* (again, quantum entanglement is available and Bob is required to determine the correct answer with probability at least $1-\varepsilon$). When $\varepsilon = 0$, we refer to the protocols as *exact*, and, when $\varepsilon > 0$, we refer to them as *bounded-error* protocols. With this notation, our results are:

$$Q_0^*(IP) = \lceil n/2 \rceil \tag{2}$$
$$Q_\varepsilon^*(IP) \geq \tfrac{1}{2}(1-2\varepsilon)^2 n - \tfrac{1}{2} \tag{3}$$
$$C_0^*(IP) = n \tag{4}$$
$$C_\varepsilon^*(IP) \geq \max(\tfrac{1}{2}(1-2\varepsilon)^2, (1-2\varepsilon)^4)n - \tfrac{1}{2} \tag{5}$$

Note that all the lower bounds are $\Omega(n)$ whenever ε is held constant. Also, these results subsume the lower bounds in [12], since the qubit model defined by Yao [17] differs from the bounded-error qubit model defined above only in that it does not permit a prior entanglement.

Our lower bound proofs employ a novel kind of "quantum" reduction between protocols, which reduces the problem of communicating, say, n bits of information to the *IP* problem. It is noteworthy that, in classical terms, it can be shown that there is no such reduction between the two problems. The appropriate cost associated with communicating n bits is then lower-bounded by the following nonstandard consequence of Holevo's theorem.

Theorem 1: *In order for Alice to convey n bits of information to Bob, where quantum entanglement is available and qubit communication in either direction is permitted, Alice must send Bob at least $\lceil n/2 \rceil$ qubits. This holds regardless of the prior entanglement and the qubit communication from Bob to Alice. More generally, for Bob to obtain m bits of mutual information with respect to Alice's n bits, Alice must send at least $\lceil m/2 \rceil$ qubits.*

A slight generalization of Theorem 1 is described and proven in the Appendix.

It should be noted that, since quantum information subsumes classical information, our results also represent new proofs of nontrivial lower bounds on the *classical* communication complexity of *IP*, and our methodology is fundamentally different from those previously used for classical lower bounds.

Finally, with respect to the question of whether quantum entanglement can *ever* be advantageous for protocols computing *IP*, we present a curious probabilistic scenario with $n = 2$ where prior entanglement enables one bit of communication to be saved.

2 Bounds for Exact Qubit Protocols

In this section, we consider exact qubit protocols computing *IP*, and prove Eq. (2). Note that the upper bound follows from so-called "superdense coding" [4]: by sending $\lceil n/2 \rceil$ qubits in conjunction with $\lceil n/2 \rceil$ EPR pairs, Alice can transmit her n classical bits of input to Bob, enabling him to evaluate *IP*. For the lower bound, we consider an arbitrary exact qubit protocol that computes *IP*, and convert it (in two stages) to a protocol for which Theorem 1 applies.

For convenience, we use the following notation. If an m-qubit protocol consists of m_1 qubits from Alice to Bob and m_2 qubits from Bob to Alice then we refer to the protocol as an (m_1, m_2)-qubit protocol.

2.1 Converting Exact Protocols into Clean Form

A *clean protocol* is a special kind of qubit protocol that follows the general spirit of the reversible programming paradigm in a quantum setting. Namely, one in which all qubits incur no net change, except for one, which contains the answer.

In general, the initial state of a qubit protocol is of the form

$$\underbrace{|y_1, \ldots, y_n\rangle|0, \ldots, 0\rangle|\Phi_{BA}\rangle}_{\text{Bob's qubits}}\underbrace{|x_1, \ldots, x_n\rangle|0, \ldots, 0\rangle}_{\text{Alice's qubits}}, \tag{6}$$

where $|\Phi_{BA}\rangle$ is the state of the entangled qubits shared by Alice and Bob, and the $|0, \ldots, 0\rangle$ states can be regarded as "ancillas". At each turn, a player performs some transformation (which, without loss of generality, can be assumed to be unitary) on all the qubits in his/her possession and then sends a subset of these qubits to the other player. Note that, due to the communication, the qubits possessed by each player varies during the execution of the protocol. At the end of the protocol, Bob measures one of his qubits which is designated as his *output*.

We say that a protocol which exactly computes a function $f(x, y)$ is *clean* if, when executed on the initial state

$$|z\rangle|y_1, \ldots, y_n\rangle|0, \ldots, 0\rangle|\Phi_{BA}\rangle|x_1, \ldots, x_n\rangle|0, \ldots, 0\rangle, \tag{7}$$

results in the final state

$$|z + f(x, y)\rangle|y_1, \ldots, y_n\rangle|0, \ldots, 0\rangle|\Phi_{BA}\rangle|x_1, \ldots, x_n\rangle|0, \ldots, 0\rangle \tag{8}$$

(where the addition is mod 2). The "input", the ancilla, and initial entangled qubits will typically change states during the execution of the protocol, but they are reset to their initial values at the end of the protocol.

It is straightforward to transform an exact (m_1, m_2)-qubit protocol into a clean $(m_1 + m_2, m_1 + m_2)$-qubit protocol that computes the same function. To reset the bits of the input, the ancilla, and the initial entanglement, the protocol is run once, except the output is not measured, but recorded and then the protocol is run in the *backwards* direction to "undo the effects of the computation". The output is recorded on a *new* qubit of Bob (with initial state $|z\rangle$) which is control-negated with the output qubit of Bob (that is in the state $|f(x, y)\rangle$) as the control. Note that, for each qubit that Bob sends to Alice when the protocol is run forwards, Alice sends the qubit to Bob when run in the backwards direction. Running the protocol backwards resets all the qubits—except Bob's new one—to their original states. The result is an $(m_1 + m_2, m_1 + m_2)$-qubit protocol that maps state (7) to state (8).

2.2 Reduction from Communication Problems

We now show how to transform a clean (m_1+m_2, m_1+m_2)-qubit protocol that exactly computes *IP* for inputs of size n, to an (m_1+m_2, m_1+m_2)-qubit protocol that transmits n bits of information from Alice to Bob. This is accomplished in four stages:

1. Bob initializes his qubits indicated in Eq. (7) with $z = 1$ and $y_1 = \cdots = y_n = 0$.
2. Bob performs a Hadamard transformation on each of his first $n+1$ qubits.
3. Alice and Bob execute the clean protocol for the inner product function.
4. Bob again performs a Hadamard transformation on each of his first $n+1$ qubits.

Let $|B_i\rangle$ denote the state of Bob's first $n+1$ qubits after the i^{th} stage. Then

$$|B_1\rangle = |1\rangle|0,\ldots,0\rangle \tag{9}$$

$$|B_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{a,b_1,\ldots,b_n\in\{0,1\}} (-1)^a|a\rangle|b_1,\ldots,b_n\rangle \tag{10}$$

$$\begin{aligned}|B_3\rangle &= \frac{1}{\sqrt{2^{n+1}}} \sum_{a,b_1,\ldots,b_n\in\{0,1\}} (-1)^a|a+b_1x_1+\cdots+b_nx_n\rangle|b_1,\ldots,b_n\rangle \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{c,b_1,\ldots,b_n\in\{0,1\}} (-1)^{c+b_1x_1+\cdots+b_nx_n}|c\rangle|b_1,\ldots,b_n\rangle \end{aligned} \tag{11}$$

$$|B_4\rangle = |1\rangle|x_1,\ldots,x_n\rangle, \tag{12}$$

where, in Eq. (11), the substitution $c = a+b_1x_1+\cdots+b_nx_n$ has been made (and arithmetic over bits is taken mod 2). The above transformation was inspired by the reading of [14] (see also [5]).

Since the above protocol conveys n bits of information (namely, $x_1,\ldots,x_n$) from Alice to Bob, by Theorem 1, we have $m_1+m_2 \geq n/2$. Since this protocol can be constructed from an arbitrary exact (m_1, m_2)-qubit protocol for *IP*, this establishes the lower bound of Eq. (2).

Note that, classically, no such reduction is possible. For example, if a clean protocol for *IP* is executed in any classical context, it can never yield more than one bit of information to Bob (whereas, in this quantum context, it yields n bits of information to Bob).

3 Lower Bounds for Bounded-Error Qubit Protocols

In this section we consider bounded-error qubit protocols for *IP*, and prove Eq. (3). Assume that some qubit protocol P computes *IP* correctly with probability at least $1-\varepsilon$, where $0 < \varepsilon < \frac{1}{2}$. Since P is not exact, the constructions from the previous section do not work exactly. We analyze the extent by which they err.

First, the construction of Section 2.1 will not produce a protocol in clean form; however, it will result in a protocol which *approximates* an exact clean protocol (this type of construction was previously carried out in a different context by Bennett *et al.* [2]).

Denote the initial state as

$$|y_1,\ldots,y_n\rangle|0,\ldots,0\rangle|\Phi_{BA}\rangle|x_1,\ldots,x_n\rangle|0,\ldots,0\rangle. \tag{13}$$

Also, assume that, in protocol P, Bob never changes the state of his input qubits $|y_1,\ldots,y_n\rangle$ (so the first n qubits never change). This is always possible, since he can copy $y_1,\ldots,y_n$ into his ancilla qubits at the beginning. After executing P until just before the measurement occurs, the state of the qubits must be of the form

$$\alpha|y_1,\ldots,y_n\rangle|x\cdot y\rangle|J\rangle+\beta|y_1,\ldots,y_n\rangle|\overline{x\cdot y}\rangle|K\rangle, \tag{14}$$

where $|\alpha|^2\geq(1-\varepsilon)$ and $|\beta|^2\leq\varepsilon$. In the above, the $n+1^{\text{st}}$ qubit is the designated output, $x\cdot y$ denotes the inner product of x and y, and $\overline{x\cdot y}$ denotes the negation of this inner product. In general, α, β, $|J\rangle$, and $|K\rangle$ may depend on x and y.

Now, suppose that the procedure described in Section 2.1 for producing a clean protocol in the exact case is carried out for P. Since, in general, the answer qubit is not in the state $|x\cdot y\rangle$—or even in a pure basis state—this does not produce the final state

$$|z+x\cdot y\rangle|y_1,\ldots,y_n\rangle|0,\ldots,0\rangle|\Phi_{BA}\rangle|x_1,\ldots,x_n\rangle|0,\ldots,0\rangle. \tag{15}$$

However, let us consider the state that is produced instead. After introducing the *new* qubit, initialized in basis state $|z\rangle$, and applying P, the state is

$$|z\rangle\left(\alpha|y_1,\ldots,y_n\rangle|x\cdot y\rangle|J\rangle+\beta|y_1,\ldots,y_n\rangle|\overline{x\cdot y}\rangle|K\rangle\right). \tag{16}$$

After applying the controlled-NOT gate, the state is

$$\begin{aligned}
&\alpha|z+x\cdot y\rangle|y_1,\ldots,y_n\rangle|x\cdot y\rangle|J\rangle+\beta|z+\overline{x\cdot y}\rangle|y_1,\ldots,y_n\rangle|\overline{x\cdot y}\rangle|K\rangle\\
&=\alpha|z+x\cdot y\rangle|y_1,\ldots,y_n\rangle|x\cdot y\rangle|J\rangle+\beta|z+x\cdot y\rangle|y_1,\ldots,y_n\rangle|\overline{x\cdot y}\rangle|K\rangle\\
&\quad-\beta|z+x\cdot y\rangle|y_1,\ldots,y_n\rangle|\overline{x\cdot y}\rangle|K\rangle+\beta|z+\overline{x\cdot y}\rangle|y_1,\ldots,y_n\rangle|\overline{x\cdot y}\rangle|K\rangle\\
&=|z+x\cdot y\rangle\left(\alpha|y_1,\ldots,y_n\rangle|x\cdot y\rangle|J\rangle+\beta|y_1,\ldots,y_n\rangle|\overline{x\cdot y}\rangle|K\rangle\right)\\
&\quad+\sqrt{2}\beta\left(\tfrac{1}{\sqrt{2}}|z+\overline{x\cdot y}\rangle-\tfrac{1}{\sqrt{2}}|z+x\cdot y\rangle\right)|y_1,\ldots,y_n\rangle|\overline{x\cdot y}\rangle|K\rangle.
\end{aligned} \tag{17}$$

Finally, after applying P in reverse to this state, the final state is

$$|z+x\cdot y\rangle|y_1,\ldots,y_n\rangle|0,\ldots,0\rangle|\Phi_{BA}\rangle|x_1,\ldots,x_n\rangle|0,\ldots,0\rangle+\sqrt{2}\beta|M_{x,y,z}\rangle, \tag{18}$$

where

$$|M_{x,y,z}\rangle=\left(\tfrac{1}{\sqrt{2}}|z+\overline{x\cdot y}\rangle-\tfrac{1}{\sqrt{2}}|z+x\cdot y\rangle\right)P^{\dagger}|y_1,\ldots,y_n\rangle|\overline{x\cdot y}\rangle|K\rangle. \tag{19}$$

Note that the vector $\sqrt{2}\beta|M_{x,y,z}\rangle$ is the difference between what an exact protocol would produce (state (15)) and what is obtained by using the inexact (probabilistic) protocol P (state (18)). There are some useful properties of the

$|M_{x,y,z}\rangle$ states. First, as $y \in \{0,1\}^n$ varies, the states $|M_{x,y,z}\rangle$ are orthonormal, since $|y_1,\ldots,y_n\rangle$ is a factor in each such state (this is where the fact that Bob does not change his input qubits is used). Also, $|M_{x,y,0}\rangle = -|M_{x,y,1}\rangle$, since only the $(\frac{1}{\sqrt{2}}|z+\overline{x\cdot y}\rangle - \frac{1}{\sqrt{2}}|z+x\cdot y\rangle)$ factor in each such state depends on z.

Call the above protocol $\tilde{P}$. Now, apply the four stage reduction in Section 2.2, with $\tilde{P}$ in place of an exact clean protocol. The *difference* between the state produced by using $\tilde{P}$ and using an exact clean protocol first occurs after the third stage and is

$$\begin{aligned} &\tfrac{1}{\sqrt{2^{n+1}}} \sum_{y_1,\ldots,y_n,z\in\{0,1\}} (-1)^z\sqrt{2}\beta_y|M_{x,y,z}\rangle \\ &= \tfrac{1}{\sqrt{2^{n+1}}} \sum_{y_1,\ldots,y_n\in\{0,1\}} \sqrt{2}\beta_y\left(|M_{x,y,0}\rangle - |M_{x,y,1}\rangle\right) \\ &= \tfrac{2}{\sqrt{2^n}} \sum_{y_1,\ldots,y_n\in\{0,1\}} \beta_y|M_{x,y,0}\rangle, \end{aligned} \tag{20}$$

which has magnitude bounded above by $2\sqrt{\varepsilon}$, since, for each $y\in\{0,1\}^n$, $|\beta_y|^2 \le \varepsilon$, and the $|M_{x,y,0}\rangle$ states are orthonormal. Also, the magnitude of this difference does not change when the Hadamard transform in the fourth stage is applied. Thus, the final state is within Euclidean distance $2\sqrt{\varepsilon}$ from

$$|1\rangle|x_1,\ldots,x_n\rangle|0,\ldots,0\rangle|\Phi_{BA}\rangle|x_1,\ldots,x_n\rangle|0,\ldots,0\rangle. \tag{21}$$

Consider the angle θ between this final state and (21). It satisfies $\sin^2\theta + (1-\cos\theta)^2 \le 4\varepsilon$, from which it follows that $\cos\theta \ge 1-2\varepsilon$. Therefore, if Bob measures his first $n+1$ qubits in the standard basis, the probability of obtaining $|1,x_1,\ldots,x_n\rangle$ is $\cos^2\theta \ge (1-2\varepsilon)^2$.

Now, suppose that $x_1,\ldots,x_n$ are uniformly distributed. Then Fano's inequality (see, for example, [9]) implies that Bob's measurement causes his uncertainty about $x_1,\ldots,x_n$ to drop from n bits to less than $(1-(1-2\varepsilon)^2)n + h((1-2\varepsilon)^2)$ bits, where $h(x) = -x\log x - (1-x)\log(1-x)$ is the binary entropy function. Thus, the mutual information between the result of Bob's measurement and $(x_1,\ldots,x_n)$ is at least $(1-2\varepsilon)^2 n - h((1-2\varepsilon)^2) \ge (1-2\varepsilon)^2 n - 1$ bits. By Theorem 1, the communication from Alice to Bob is at least $\frac{1}{2}(1-2\varepsilon)^2 n - \frac{1}{2}$ qubits, which establishes Eq. (3).

4 Lower Bounds for Bit Protocols

In this section, we consider exact and bounded-error bit protocols for *IP*, and prove Eqs. (4) and (5).

Recall that any m-qubit protocol can be simulated by a $2m$-bit protocol using teleportation [3] (employing EPR pairs of entanglement). Also, if the communication pattern in an m-bit protocol is such that an even number of bits is always sent during each party's turn then it can be simulated by an $m/2$-qubit protocol by superdense coding [4] (which also employs EPR pairs). However, this latter simulation technique cannot, in general, be applied directly, especially for protocols where the parties take turns sending single bits.

We can nevertheless obtain a slightly weaker simulation of bit protocols by qubit protocols for *IP* that is sufficient for our purposes. The result is that, given any m-bit protocol for IP_n (that is, *IP* instances of size n), one can construct an m-qubit protocol for IP_{2n}. This is accomplished by interleaving two executions of the bit protocol for IP_n to compute two independent instances of inner products of size n. We make two observations. First, by taking the sum (mod 2) of the two results, one obtains an inner product of size $2n$. Second, due to the interleaving, an even number of bits is sent at each turn, so that the above superdense coding technique can be applied, yielding a $(2m)/2 = m$-qubit protocol for IP_{2n}. Now, Eq. (2) implies $m \geq n$, which establishes the lower bound of Eq. (4) (and the upper bound is trivial).

If the same technique is applied to any m-bit protocol computing IP_n with probability $1 - \varepsilon$, one obtains an m-qubit protocol that computes IP_{2n} with probability $(1-\varepsilon)^2 + \varepsilon^2 = 1 - 2\varepsilon(1-\varepsilon)$. Applying Eq. (3) here, with $2n$ replacing n and $2\varepsilon(1-\varepsilon)$ replacing ε, yields $m \geq (1-2\varepsilon)^4 n - \frac{1}{2}$. For $\varepsilon > \frac{2-\sqrt{2}}{4} = 0.146\ldots$, a better bound is obtained by simply noting that $C^*_\varepsilon \geq Q^*_\varepsilon$ (since qubits can always be used in place of bits), and applying Eq. (3). This establishes Eq. (5).

5 An Instance Where Prior Entanglement Is Beneficial

Here we will show that in spite of the preceding results, it is still possible that a protocol which uses prior entanglement outperforms all possible classical protocols. This improvement is done in the probabilistic sense where we look at the number of communication bits required to reach a certain reliability threshold for the *IP* function. This is done in the following setting.

Both Alice and Bob have a 2 bit vector x_1x_2 and y_1y_2, for which they want to calculate the inner product modulo 2:

$$f(x,y) = x_1y_1 + x_2y_2 \bmod 2 \tag{22}$$

with a correctness-probability of at least $\frac{4}{5}$. It will be shown that with entanglement Alice and Bob can reach this ratio with 2 bits of communication, whereas without entanglement 3 bits are necessary to obtain this success-ratio.

5.1 A Two-Bit Protocol with Prior Entanglement

Initially Alice and Bob share a joint random coin and an EPR-like pair of qubits Q_A and Q_B:

$$\text{state}(Q_AQ_B) = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{23}$$

With these attributes the protocol goes as follows.

First Alice and Bob determine by a joint random coin flip[1] who is going to be the 'sender' and the 'receiver' in the protocol. (We continue the description of the protocol by assuming that Alice is the sender and that Bob is the receiver.) After this, Alice (the sender) applies the rotation $A_{x_1x_2}$ on her part of the entangled pair and measures this qubit Q_A in the standard basis. The result m_A of this measurement is then sent to Bob (the receiver) who continues the protocol.

If Bob has the input string '00', he knows with certainty that the outcome of the function $f(x, y)$ is zero and hence he concludes the protocol by sending the bit 0 to Alice. Otherwise, Bob performs the rotation $B_{y_1y_2}$ on his part of the entangled pair Q_B and measure it in the standard basis yielding the value m_B. Now Bob finishes the protocol by sending to Alice the bit $m_A + m_B \bmod 2$.

Using the rotations shown below and bearing in mind the randomization process in the beginning of the protocol with the joint coin flip, this will be a protocol that uses only 2 bits of classical communication and that gives the correct value of $f(x, y)$ with a probability of at least $\frac{4}{5}$ for every possible combination of x_1x_2 and y_1y_2.

The unitary transformations used by the sender in the protocol are:

$$A_{00} = \begin{pmatrix} \sqrt{\frac{2}{5}} & -\mathrm{i}\sqrt{\frac{3}{5}} \\ -\mathrm{i}\sqrt{\frac{3}{5}} & \sqrt{\frac{2}{5}} \end{pmatrix} \qquad A_{01} = \begin{pmatrix} \sqrt{\frac{4}{5}} & \sqrt{\frac{3}{16}} + \mathrm{i}\sqrt{\frac{1}{80}} \\ -\sqrt{\frac{3}{16}} + \mathrm{i}\sqrt{\frac{1}{80}} & \sqrt{\frac{4}{5}} \end{pmatrix} \tag{24}$$

$$A_{10} = \begin{pmatrix} \sqrt{\frac{4}{5}} & -\sqrt{\frac{3}{16}} + \mathrm{i}\sqrt{\frac{1}{80}} \\ \sqrt{\frac{3}{16}} + \mathrm{i}\sqrt{\frac{1}{80}} & \sqrt{\frac{4}{5}} \end{pmatrix} \quad A_{11} = \begin{pmatrix} \sqrt{\frac{1}{5}} & \mathrm{i}\sqrt{\frac{4}{5}} \\ \mathrm{i}\sqrt{\frac{4}{5}} & \sqrt{\frac{1}{5}} \end{pmatrix},$$

whereas the receiver uses one of the three rotations:

$$B_{01} = \begin{pmatrix} \sqrt{\frac{3}{5}} & -\frac{1}{2} + \mathrm{i}\sqrt{\frac{3}{20}} \\ -\frac{1}{2} - \mathrm{i}\sqrt{\frac{3}{20}} & -\sqrt{\frac{3}{5}} \end{pmatrix} \quad B_{10} = \begin{pmatrix} \sqrt{\frac{3}{5}} & \frac{1}{2} + \mathrm{i}\sqrt{\frac{3}{20}} \\ -\frac{1}{2} + \mathrm{i}\sqrt{\frac{3}{20}} & \sqrt{\frac{3}{5}} \end{pmatrix} \tag{25}$$

$$B_{11} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The matrices were found by using an optimization program that suggested certain numerical values. A closer examination of these values revealed the above analytical expressions.

[1] Because a joint random coin flip can be simulated with an EPR-pair, we can also assume that Alice and Bob start the protocol with two shared EPR-pairs and no random coins.

5.2 No Two-Bit Classical Probabilistic Protocol Exists

Take the probability distribution π on the input strings x and y, defined by:

$$\pi(x,y) = \begin{cases} 0 \text{ iff } x = 00 \text{ or } y = 00 \\ \frac{1}{9} \text{ iff } x \neq 00 \text{ and } y \neq 00 \end{cases} \tag{26}$$

It is easily verified that for this distribution, every *deterministic* protocol with only two bits of communication will have a correctness ratio of at most $\frac{7}{9}$. Using Theorem 3.20 of [13], this shows that every possible randomized protocol with the same amount of communication will have a success ratio of at most $\frac{7}{9}$. (It can also be shown that this $\frac{7}{9}$ bound is tight but we will omit that proof here.) This implies that in order to reach the requested ration of $\frac{4}{5}$, at least three bits of communication are required if we are not allowed to use any prior entanglement.

5.3 Two Qubits Suffice Without Prior Entanglement

A similar result also holds for qubit protocols without prior entanglement [17]. This can be seen by the fact that after Alice applied the rotation $A_{x_1x_2}$ and measured her qubit Q_A with the result $m_A = 0$, she knows the state of Bob's qubit Q_B exactly. It is therefore also possible to envision a protocol where the parties assume the measurement outcome $m_A = 0$ (this can be done without loss of generality), and for which Alice simply sends this qubit Q_B to Bob, after which Bob finishes the protocol in the same way as prescribed by the 'prior entanglement'-protocol. The protocol has thus become as follows.

First Alice and Bob decide by a random joint coin flip who is going to be the sender and the receiver in protocol. (Again we assume here that Alice is the sender.) Next, Alice (the sender) sends a qubit $|Q_{x_1x_2}\rangle$ (according to the input string x_1x_2 of Alice and the table 27) to the receiver Bob who continues the protocol.

$$\begin{aligned} |Q_{00}\rangle &= \sqrt{\tfrac{2}{5}}|0\rangle - \mathrm{i}\sqrt{\tfrac{3}{5}}|1\rangle & |Q_{01}\rangle &= \sqrt{\tfrac{4}{5}}|0\rangle + \left(\sqrt{\tfrac{3}{16}} + \mathrm{i}\sqrt{\tfrac{1}{80}}\right)|1\rangle \\ |Q_{10}\rangle &= \sqrt{\tfrac{4}{5}}|0\rangle + \left(-\sqrt{\tfrac{3}{16}} + \mathrm{i}\sqrt{\tfrac{1}{80}}\right)|1\rangle & |Q_{11}\rangle &= \sqrt{\tfrac{1}{5}}|0\rangle - \mathrm{i}\sqrt{\tfrac{4}{5}}|1\rangle \end{aligned} \tag{27}$$

If Bob has the input string $y_1y_2 = 00$, he concludes the protocol by sending a zero bit to Alice. In the other case, Bob applies the rotation $B_{y_1y_2}$ to the received qubit, measures the qubit in the standard basis, and sends this measurement outcome to Alice as the answer of the protocol. By doing so, the same correctness-probability of $\frac{4}{5}$ is reached for the *IP* function with two qubits of communication, whereas the classical setting requires 3 bits of communication as shown above.

Acknowledgments

We would like to thank Gilles Brassard, Harry Buhrman, Peter Høyer, and Tal Mor for their comments about this research. R.C. would like to thank the Laboratoire d'Informatique Théorique et Quantique, Université de Montréal for their gracious hospitality while this research was initiated. M.N. thanks the Office of Naval Research (Grant No. N00014-93-1-0116).

References

1. H. Araki and E.H. Lieb, “Entropy inequalities”, *Commun. Math. Phys.*, Vol. 18, 1970, pp. 160–170.
2. C.H. Bennett, E. Bernstein, G. Brassard, U. Vazirani, “Strengths and weaknesses of quantum computing”, *SIAM J. on Comput.*, Vol. 26, No. 5, 1997, pp. 1510–1523.
3. C.H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres, W.K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”, *Phys. Rev. Lett.*, Vol. 70, 1993, pp. 1895–1899.
4. C.H. Bennett and S.J. Wiesner, “Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states”, *Phys. Rev. Lett.*, Vol. 69, No. 20, 1992, pp. 2881–2884.
5. E. Bernstein, U. Vazirani, “Quantum Complexity Theory”, *SIAM J. Comput.*, Vol. 26, No. 5, 1997, pp. 1411–1473.
6. H. Buhrman, R. Cleve, and W. van Dam, “Quantum Entanglement and Communication Complexity”, preprint available from the LANL quant-ph archive 9705033, 1997.
7. B. Chor and O. Goldreich, “Unbiased bits from weak sources of randomness and probabilistic communication complexity”, *SIAM J. on Comput.*, Vol. 17, No. 2, pp. 230–261, 1988.
8. R. Cleve and H. Buhrman, “Substituting quantum entanglement for communication”, *Phys. Rev. A*, Vol. 56, No. 2, pp. 1201–1204, 1997.
9. T.M. Cover and J.A. Thomas, *Elements of Information Theory*, John Wiley and Sons, 1991.
10. A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be complete?”, *Phys. Rev.*, Vol. 47, 1935, pp. 777–780.
11. A.S. Holevo, “Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel”, *Problemy Peredachi Informatsii*, Vol. 9, No. 3, 1973, pp. 3–11. English translation *Problems of Information Transmission*, Vol. 9, 1973, pp. 177–183.
12. I. Kremer, “Quantum Communication”, Master’s Thesis, The Hebrew University of Jerusalem, 1995.
13. E. Kushilevitz and N. Nisan, *Communication Complexity*, Cambridge University Press, 1997.
14. B.M. Terhal and J.A. Smolin, “Superfast quantum algorithms for coin weighing and binary search problems”, preprint available from the LANL quant-ph archive 9705041, 1997.
15. B. Schumacher, M. Westmoreland and W. K. Wootters, “Limitation on the amount of accessible information in a quantum channel”, *Phys. Rev. Lett.*, Vol. 76, 1996, pp. 3453–3456.
16. A.C. Yao, “Some complexity questions related to distributed computing”, *Proc. of the 11th Ann. ACM Symp. on Theory of Computing*, 1979, pp. 209–213.
17. A.C. Yao, “Quantum circuit complexity”, *Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Science*, 1993, pp. 352–361.

Appendix: Capacity Results for Communication Using Qubits

In this appendix, we present results about the quantum resources required to transmit n classical bits between two parties when two-way communication is available. These results are used in the main text in the proof of the lower bound on the communication complexity of the inner product function, and may also be of independent interest.

Theorem 2: *Suppose that Alice possesses n bits of information, and wants to convey this information to Bob. Suppose that Alice and Bob possess no prior entanglement but qubit communication in either direction is allowed. Let n_{AB} be the number of qubits Alice sends to Bob, and n_{BA} the number of qubits Bob sends to Alice (n_{AB} and n_{BA} are natural numbers). Then, Bob can acquire the n bits if and only if the following inequalities are satisfied:*

$$n_{AB} \geq \lceil n/2 \rceil \tag{28}$$

$$n_{AB} + n_{BA} \geq n. \tag{29}$$

More generally, Bob can acquire m bits of mutual information with respect to Alice's n bits if and only if the above equations hold with m substituted for n.

Note that Theorem 1 follows from Theorem 2 because, if the communication from Bob to Alice is not counted then this can be used to set up an arbitrary entanglement at no cost.

Graphically, the capacity region for the above communication problem is shown in Fig. 1. Note the difference with the classical result for communication with bits, where the capacity region is given by the equation $n_{AB} \geq n$; that is, classically, communication from Bob to Alice does not help.

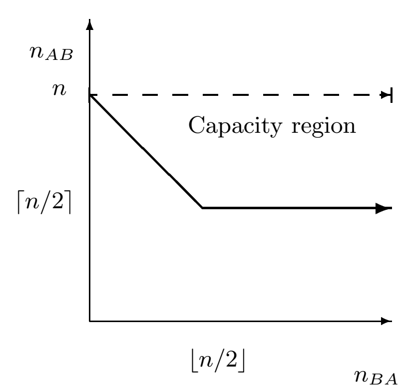

Fig. 1. Capacity region to send n bits from Alice to Bob. n_{AB} is the number of qubits Alice sends to Bob, and n_{BA} is the number of qubits Bob sends to Alice. The dashed line indicates the bottom of the classical capacity region.

Proof of Theorem 2: The sufficiency of Eqns. (28) and (29) follows from the superdense coding technique [4]. The nontrivial case is where $n_{AB} < n$. Bob prepares $n - n_{AB} \leq n_{BA}$ EPR pairs and sends one qubit of each pair to Alice, who can use them in conjunction with sending $n - n_{AB} \leq n_{AB}$ qubits to Bob to transmit $2(n - n_{AB})$ bits to Bob. Alice uses her remaining allotment of $2n_{AB} - n$ qubits to transmit the remaining $2n_{AB} - n$ bits in the obvious way.

The proof that Eqns. (28) and (29) are necessary follows from an application of Holevo's Theorem [11], which we now review. Suppose that a classical information source produces a random variable X. Depending on the value, x, of X, a quantum state with density operator ρ_x is prepared. Suppose that a measurement is made on this quantum state in an effort to determine the value of X. This measurement results in an outcome Y. Holevo's theorem states that the mutual information $I(X : Y)$ between X and Y is bounded by the *Holevo bound* [11]

$$I(X : Y) \leq S(\rho) - \sum_x p_x S(\rho_x), \tag{30}$$

where p_x are the probabilities associated with the different values of X, $\rho = \sum_x p_x \rho_x$, and S is the von Neumann entropy function. The quantity on the right hand side of the Holevo bound is known as the *Holevo chi quantity*, $\chi(\rho_X) = S(\rho) - \sum_x p_x S(\rho_x)$.

Let X be Alice's n bits of information, which is uniformly distributed over $\{0,1\}^n$. Without loss of generality, it can be assumed that the protocol between Alice and Bob is of the following form. For any value $(x_1, \ldots, x_n)$ of X, Alice begins with a set of qubits in state $|x_1, \ldots, x_n\rangle|0, \ldots, 0\rangle$ and Bob begins with a set of qubits in state $|0, \ldots, 0\rangle$. The protocol first consists of a sequence of steps, where at each step one of the following processes takes place.

1. Alice performs a unitary operation on the qubits in her possession.
2. Bob performs a unitary operation on the qubits in his possession.
3. Alice sends a qubit to Bob.
4. Bob sends a qubit to Alice.

After these steps, Bob performs a measurement on the qubits in his possession, which has outcome Y. (Note that one might imagine that the initial states could be mixed and that measurements could be performed in addition to unitary operations; however, these processes can be simulated using standard techniques involving ancilla qubits.)

Let ρ_i^X be the density operator of the set of qubits that are in Bob's possession after i steps have been executed. Due to Holevo's Theorem, it suffices to upper bound the final value of $\chi(\rho_i^X)$—which is also bounded above by $S(\rho_i)$. We consider the evolution of $\chi(\rho_i^X)$ and $S(\rho_i)$. Initially, $\chi(\rho_0^X) = S(\rho_0) = 0$, since Bob begins in a state independent of X. Now, consider how $\chi(\rho_i^X)$ and $S(\rho_i)$ change for each of the four processes above.

1. This does not affect ρ_i^X and hence has no effect on $\chi(\rho_i^X)$ or $S(\rho_i)$.
2. It is easy to verify that χ and S are invariant under unitary transformations, so this does not affect $\chi(\rho_i^X)$ and $S(\rho_i)$ either.
3. Let B denote Bob's qubits after i steps and Q denote the qubit that Alice sends to Bob at the $i+1^{\text{st}}$ step. By the subadditivity inequality and the fact that, for a single qubit Q, $S(Q) \leq 1$, $S(BQ) \leq S(B) + S(Q) \leq S(B) + 1$. Also, by the Araki-Lieb inequality [1], $S(BQ) \geq S(B) - S(Q) \geq S(B) - 1$. It follows that $S(\rho_{i+1}) \leq S(\rho_i) + 1$ and

$$\begin{aligned}\chi(\rho_{i+1}^X) &= S(\rho_{i+1}) - \sum_{x \in \{0,1\}^n} p_x S(\rho_{i+1}^x) \\ &\leq (S(\rho_i) + 1) - \sum_{x \in \{0,1\}^n} p_x (S(\rho_i^x) - 1) \\ &= \chi(\rho_i^X) + 2. \end{aligned} \tag{31}$$

4. In this case, ρ_{i+1}^X is ρ_i^X with one qubit traced out. It is known that tracing out a subsystem of any quantum system does not increase χ [15], so $\chi(\rho_{i+1}^X) \leq \chi(\rho_i^X)$. Note also that $S(\rho_{i+1}) \leq S(\rho_i) + 1$ for this process, by the Araki-Lieb inequality [1].

Now, since $\chi(\rho_i^X)$ can only increase when Alice sends a qubit to Bob and by at most 2, Eq. (28) follows. Also, since $S(\rho_i)$ can only increase when one party sends a qubit to the other and by at most 1, Eq. (29) follows. This completes the proof of Theorem 2.