Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE: QUANTUM ENTAGLEMENT AND THE COMMUNICATION COMPLEXITY OF THE INNER PRODUCT FUNCTION

AUTHOR(S): Richard Cleve, Univ of Calgary
Wim van Dam, Univ of Oxford
Michael Nielsen, T-6/UNM
Alain Tapp, Univ de Montreal

SUBMITTED TO: 1ST NASA INTERNATIONAL CONFERENCE ON QUANTUM COMPUTING AND QUANTUM COMMUNICATIONS, FEBRUARY 17-20, 1998, PALM SPRINGS, CA

Los Alamos

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible electronic image products. Images are produced from the best available original document.

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‡
[2] University of Oxford and CWI, Amsterdam§
[3] Los Alamos National Laboratory and University of New Mexico¶
[4] Université de Montréal‖

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 multibit communication problems 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 $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ is defined as the minimum amount of communication necessary among two parties, conventionally referred to as Alice and Bob, in order for, say, Alice 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 [15] and has been widely studied (see [12] 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.

‡ Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4. E-mail: cleve@cpsc.ucalgary.ca.

§ Clarendon Laboratory, Department of Physics, University of Oxford, Parks Road, Oxford OX1 3PU, U.K. E-mail: wimvdam@mildred.physics.ox.ac.uk.

¶ T-6 Theoretical Astrophysics, Los Alamos National Laboratory, U.S.A. E-mail: mnielsen@tangelo.phys.unm.edu.

‖ Département IRO, C.P. 6128, Succursale Centre-Ville, Montréal, Québec, Canada H3C 3J7. E-mail: tappa@iro.umontreal.ca.

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

$$IP(x,y) = x_1y_1 + x_2y_2 + \cdots + x_ny_n \bmod 2 \tag{1}$$

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 correctness probability $\frac{1}{2}+\varepsilon$ required, the communication complexity is $n - O(\log(1/\varepsilon))$ [6] (see also [12]).

In 1993, Yao [16] 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 [11] showed that, in this model, the communication complexity of *IP* is $\Omega(n)$, whenever the required correctness probability is $\frac{1}{2} + \varepsilon$ for a constant $\varepsilon > 0$ (Kremer attributes the proof methodology to Yao).

Cleve and Buhrman [7] (see also [5]) 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 [11] 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 $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ be a communication problem. First, for the case of *exact* protocols (i.e. those where no error probability is permitted), let $Q^*(f)$ and $C^*(f)$ denote the communication complexities in the respective settings of qubit communication and classical bit communication (the $*$ superscripts are intended to highlight the fact that prior entanglement is available). Second, for the case of *bounded-error* protocols, in which Alice acquires the correct answer with probability at least $\frac{1}{2} + \varepsilon$, for $\varepsilon > 0$, let $Q^*_\varepsilon(f)$ and $C^*_\varepsilon(f)$ denote the communication complexities in the respective settings of qubit communication and classical bit communication. With this notation, our results are:

$$Q^*(IP) = \lceil n/2 \rceil \tag{2}$$
$$Q^*_\varepsilon(IP) \geq 2\varepsilon^2 n - \tfrac{1}{2} \tag{3}$$
$$C^*(IP) = n \tag{4}$$
$$C^*_\varepsilon(IP) \geq 2\varepsilon^2 \max(1, 8\varepsilon^2) n - \tfrac{1}{2}. \tag{5}$$

Note that all the lower bounds are $\Omega(n)$ whenever ε is held constant. Also, these results subsume the lower bounds in [11], since the qubit model defined by Yao [16] 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, 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 application of Holevo's theorem.

Theorem 1: *Suppose that Bob possesses n bits of information, and wants to convey this information to Alice. Suppose that Alice and Bob possess an arbitrary prior entanglement and qubit communication in either direction is allowed. Then, regardless of the prior entanglement and qubit communication from Alice to Bob, Bob must send at least $\lceil n/2 \rceil$ qubits to Alice. More generally, for Alice to obtain m bits of mutual information with respect to Bob's n bits, Bob must send at least $\lceil m/2 \rceil$ qubits to Alice.*

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

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, Bob can transmit his n classical bits of input to Alice, enabling her 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

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

where $|\Phi_{AB}\rangle$ 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.

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

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

results in the final state

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

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 after the protocol is run once, the answer is recorded and then the protocol is run in the *backwards* direction to "undo the effects of the computation". The answer is recorded on a *new* qubit of Alice (with initial state $|z\rangle$) which is control-negated (with the qubit of Alice that is in the state $|f(x,y)\rangle$ as the control qubit). Note that, for each qubit that Alice sends to Bob when the protocol is run forwards, Bob sends the qubit to Alice when run in the backwards direction. Running the protocol backwards resets all the qubits—except Alice'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 will now show how to transform a clean (m_1+m_2, m_1+m_2)-qubit protocol that 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 Bob to Alice. This is accomplished in four stages:

1. Alice initializes her qubits indicated in Eq. (7) with $z = 1$ and $x_1 = \cdots = x_n = 0$.
2. Alice performs a Hadamard transformation on each of her first $n+1$ qubits.
3. Alice and Bob execute the clean protocol for the inner product function.
4. Alice again performs a Hadamard transformation on each of her first $n+1$ qubits.

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

$$|A_1\rangle = |1\rangle|0,\ldots,0\rangle \tag{9}$$

$$|A_2\rangle = \tfrac{1}{\sqrt{2^{n+1}}} \sum_{a,b_1,\ldots,b_n \in \{0,1\}} (-1)^a|a\rangle|b_1,\ldots,b_n\rangle \tag{10}$$

$$\begin{aligned} |A_3\rangle &= \tfrac{1}{\sqrt{2^{n+1}}} \sum_{a,b_1,\ldots,b_n \in \{0,1\}} (-1)^a|a+b_1y_1+\cdots+b_ny_n\rangle|b_1,\ldots,b_n\rangle \\ &= \tfrac{1}{\sqrt{2^{n+1}}} \sum_{c,b_1,\ldots,b_n \in \{0,1\}} (-1)^{c+b_1y_1+\cdots+b_ny_n}|c\rangle|b_1,\ldots,b_n\rangle \end{aligned} \tag{11}$$

$$|A_4\rangle = |1\rangle|y_1,\ldots,y_n\rangle, \tag{12}$$

where, in Eq. (11), the substitution $c = a+b_1y_1+\cdots+b_ny_n$ has been made (and arithmetic over bits is taken mod 2). The above transformation was inspired by the reading of [13] on superfast quantum searching.

Since the above protocol conveys n bits of information (namely, $y_1,\ldots,y_n$) from Bob to Alice, 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).

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 $\frac{1}{2} + \varepsilon$, where $\varepsilon > 0$. 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

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

Also, assume that, in protocol P, Alice never changes the state of her input qubits $|x_1,\ldots,x_n\rangle$ (so the first n qubits never change). This is always possible, since she can copy $x_1,\ldots,x_n$ into her ancilla qubits at the beginning. After executing P until just before the measurement occurs, the state of the qubits must be of the form

$$\alpha|x_1,\ldots,x_n\rangle|x\cdot y\rangle|J\rangle + \beta|x_1,\ldots,x_n\rangle|\overline{x\cdot y}\rangle|K\rangle, \tag{14}$$

where $|\alpha|^2 \geq \frac{1}{2} + \varepsilon$ and $|\beta|^2 \leq \frac{1}{2} - \varepsilon$. In the above, the $n+1^{\mathrm{st}}$ qubit is the *answer* qubit, $x \cdot y$ 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

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

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

$$|z\rangle \left(\alpha|x_1, \ldots, x_n\rangle|x \cdot y\rangle|J\rangle + \beta|x_1, \ldots, x_n\rangle|\overline{x \cdot y}\rangle|K\rangle\right). \tag{16}$$

After applying the controlled-NOT gate, the state is

$$\begin{aligned}
&\alpha|z + x \cdot y\rangle|x_1, \ldots, x_n\rangle|x \cdot y\rangle|J\rangle + \beta|z + \overline{x \cdot y}\rangle|x_1, \ldots, x_n\rangle|\overline{x \cdot y}\rangle|K\rangle \\
&\quad = \alpha|z + x \cdot y\rangle|x_1, \ldots, x_n\rangle|x \cdot y\rangle|J\rangle + \beta|z + x \cdot y\rangle|x_1, \ldots, x_n\rangle|\overline{x \cdot y}\rangle|K\rangle \\
&\qquad -\beta|z + x \cdot y\rangle|x_1, \ldots, x_n\rangle|\overline{x \cdot y}\rangle|K\rangle + \beta|z + \overline{x \cdot y}\rangle|x_1, \ldots, x_n\rangle|\overline{x \cdot y}\rangle|K\rangle \\
&\quad = |z + x \cdot y\rangle \left(\alpha|x_1, \ldots, x_n\rangle|x \cdot y\rangle|J\rangle + \beta|x_1, \ldots, x_n\rangle|\overline{x \cdot y}\rangle|K\rangle\right) \\
&\qquad +\sqrt{2}\beta \left(\tfrac{1}{\sqrt{2}}|z + \overline{x \cdot y}\rangle - \tfrac{1}{\sqrt{2}}|z + x \cdot y\rangle\right)|x_1, \ldots, x_n\rangle|\overline{x \cdot y}\rangle|K\rangle.
\end{aligned} \tag{17}$$

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

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

where

$$|M_{x,y,z}\rangle = \left(\tfrac{1}{\sqrt{2}}|z + \overline{x \cdot y}\rangle - \tfrac{1}{\sqrt{2}}|z + x \cdot y\rangle\right) P^{\dagger}|x_1, \ldots, x_n\rangle|\overline{x \cdot y}\rangle|K\rangle. \tag{19}$$

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 $x \in \{0,1\}^n$ varies, the states $|M_{x,y,z}\rangle$ are orthonormal, since $|x_1, \ldots, x_n\rangle$ is a factor in each such state (this is where the fact that Alice does not change her 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

$$\begin{aligned}
&\tfrac{1}{\sqrt{2^{n+1}}} \sum_{x_1, \ldots, x_n, z \in \{0,1\}} (-1)^z \sqrt{2}\beta_x|M_{x,y,z}\rangle \\
&= \tfrac{1}{\sqrt{2^{n+1}}} \sum_{x_1, \ldots, x_n \in \{0,1\}} \sqrt{2}\beta_x \left(|M_{x,y,0}\rangle - |M_{x,y,1}\rangle\right) \\
&= \tfrac{2}{\sqrt{2^n}} \sum_{x_1, \ldots, x_n \in \{0,1\}} \beta_x|M_{x,y,0}\rangle,
\end{aligned} \tag{20}$$

which has magnitude bounded above by $2\sqrt{\frac{1}{2}-\varepsilon} = \sqrt{2-4\varepsilon}$, since, for each $x \in \{0,1\}^n$, $|\beta_x|^2 \leq \frac{1}{2} - \varepsilon$, 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 $\sqrt{2-4\varepsilon}$ from

$$|1\rangle|y_1,\ldots,y_n\rangle|0,\ldots,0\rangle|\Phi_{AB}\rangle|y_1,\ldots,y_n\rangle|0,\ldots,0\rangle. \tag{21}$$

Consider the angle θ between this final state and (21). It satisfies $\sin^2\theta + (1-\cos\theta)^2 \geq 2-4\varepsilon$, from which it follows that $\cos\theta \geq 2\varepsilon$. Therefore, if Alice measures her first $n+1$ qubits in the standard basis, the probability of obtaining $|1,y_1,\ldots,y_n\rangle$ is at least $\cos^2\theta = 4\varepsilon^2$.

Now, suppose that $y_1,\ldots,y_n$ are uniformly distributed. Then Fano's inequality (see, for example, [8]) implies that Alice's measurement causes her uncertainty about $y_1,\ldots,y_n$ to drop from n bits to less than $(1-4\varepsilon^2)n + h(4e^2)$ bits, where $h(x) \equiv -x\log x - (1-x)\log(1-x)$ is the binary entropy function. Thus, the mutual information between the result of Alice's measurement and $(y_1,\ldots,y_n)$ is at least $4\varepsilon^2 n - h(4e^2) \geq 4\varepsilon^2 n - 1$ bits. By Theorem 1, the communication from Bob to Alice is at least $(4\varepsilon^2 n - 1)/2$ 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 $\frac{1}{2}+\varepsilon$, one obtains an m-qubit protocol that computes IP_{2n} with probability $(\frac{1}{2}+\varepsilon)^2 + (\frac{1}{2}-\varepsilon)^2 = \frac{1}{2} + 2\varepsilon^2$. By Eq. (3), $m \geq 2(2\varepsilon^2)^2(2n) - \frac{1}{2} =$

$16e^4 n - \frac{1}{2}$. For $\varepsilon < \frac{1}{\sqrt{8}}$, a better bound is obtained by simply noting that $C_\varepsilon^* \geq Q_\varepsilon^*$ (since qubits can always be used in place of bits), so, by Eq. (3), $m \geq 2\varepsilon^2 n - \frac{1}{2}$. 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 $x_1 x_2$ and $y_1 y_2$, for which they want to calculate the inner product modulo 2:

$$f(x,y) = x_1 y_1 + x_2 y_2 \bmod 2 \tag{22}$$

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:

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

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 $A_{x_1 x_2}$ 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 $B_{y_1 y_2}$ 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

[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.

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:

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

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

whereas the receiver uses one of the three rotations:

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

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

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.

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 [12], 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 [16]. 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.

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

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.A.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. Comp.* Vol. 26, No. 5, 1997, pp. 1510–1523. See also Technical Report 9701001, Archive `http://xxx.lanl.gov/archive/quant-ph`, 1997.
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", *Physical Review Letters,* 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", *Physical Review Letters,* Vol. 69, No. 20, 1992, pp. 2881–2884.

5. H. Buhrman, R. Cleve, and W. van Dam, "Quantum Entanglement and Communication Complexity", Technical Report 9705033, Archive http://xxx.lanl.gov/archive/quant-ph, 1997.
6. B. Chor and O. Goldreich, "Unbiased bits from weak sources of randomness and probabilistic communication complexity", *SIAM Journal on Computing,* Vol. 17, No. 2, pp. 230–261, 1988.
7. R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication", *Physical Review A,* Vol. 56, No. 2, pp. 1201–1204, 1997. Also available as Technical Report 9704026, Archive http://xxx.lanl.gov/archive/quant-ph, 1997.
8. T.M. Cover and J.A. Thomas, *Elements of information theory,* John Wiley and Sons, 1991.
9. A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be complete?", *Physical Review,* Vol. 47, 1935, pp. 777–780.
10. 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.
11. I. Kremer, "Quantum Communication", Master's Thesis, The Hebrew University of Jerusalem, 1995.
12. E. Kushilevitz and N. Nisan, *Communication Complexity,* Cambridge University Press, 1997.
13. B.M. Terhal and J.A. Smolin, "Superfast quantum algorithms for coin weighing and binary search problems", Technical Report 9705041, Archive http://xxx.lanl.gov/archive/quant-ph, 1997.
14. 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.
15. A.C. Yao, "Some complexity questions related to distributed computing", *Proceedings of the 11th Annual ACM Symposium on Theory of Computing,* 1979, pp. 209–213.
16. A.C. Yao, "Quantum circuit complexity", *Proceedings of the 34th Annual IEEE Symposium 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, Alice and Bob. These results are used in the main text in the proof of the lower bound on the communication complexity of the inner product function. The results may also be of some 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 looks as shown in Figure 1. Note the difference with the classical result for communication with bits, where the capacity region is given by the equations $n_{AB} \geq n$ and $n_{BA} \geq 0$ – that is, classically, communication from Bob to Alice doesn't help.

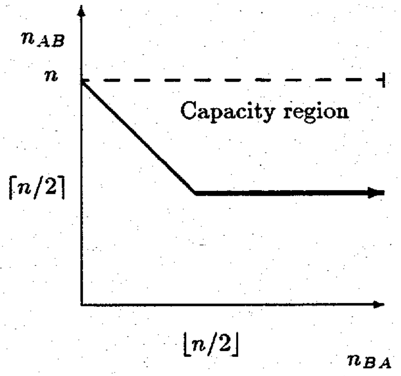

Fig. 1. Capacity region to send n bits from Alice to Bob. n_{AB} is the number of qubits Alice sends to Bob, and n_{BA} is the number of qubits Bob sends to Alice. The dashed line indicates the bottom of the classical capacity region.

Proof of Theorem 2: Suppose n_{AB} and n_{BA} satisfy the constraints. We assume that $n_{AB} < n$, since otherwise Alice encodes the n bits into n qubits in the obvious way. Bob prepares $n - n_{AB} > 0$ EPR pairs and sends half of each pair to Alice. Note that $n_{BA} \geq n - n_{AB}$, so this is possible with Bob's resources. Alice does superdense coding [4] on the $n - n_{AB}$ qubits, and sends them back to Bob, who can extract $2(n - n_{AB})$ bits of information. Alice uses her remaining allotment of $n - (n - n_{AB}) = 2n_{AB} - n \geq 0$ qubits to transmit $2n_{AB} - n$ bits of information in the obvious way. The total information transmitted is thus $2(n - n_{AB}) + 2n_{AB} - n = n$ bits, as required.

The proof that these bounds are the best possible is the more interesting part. The key idea is a simple application of Holevo's theorem [10], which we now review. Suppose a classical information source produces a random variable X. Depending on the value, x, of the random variable, a state ρ_x of a quantum system is prepared. Suppose a measurement is made on the quantum system 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* [10],

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

where p_x are the probabilities the different values X may take, $\rho \equiv \sum_x p_x \rho_x$, and $S(\cdot)$ is the von Neumann entropy function. The quantity on the right hand side of the Holevo bound is known as the *Holevo chi quantity*, $\chi \equiv S(\rho) - \sum_x p_x S(\rho_x)$. The Holevo bound tells us that the amount of information about X that may be deduced by observing ρ_X is bounded above by χ, and it is this fact that we use to prove our lower bounds. A key fact about the Holevo χ quantity concerns the case of a quantum system with two component, A and B. Schumacher, Westmoreland and Wootters [14] have shown that if we consider the χ quantity associated with A, $\chi_A \equiv S(\rho_A) - \sum_x p_x S(\rho_{xA})$, where $\rho_A \equiv \mathrm{tr}_B(\rho)$ and $\rho_{xA} \equiv \mathrm{tr}_B(\rho_x)$ are the states which result when system B is traced out, then $\chi_A \leq \chi$. In the light of the Holevo bound this result is intuitively plausible, since if we make a measurement on system A alone, then we would expect to get no more information about X than we would if we could measure the entire quantum system, AB.

Without loss of generality we may suppose that the quantum protocol for the problem under consideration consists of unitary operations performed alternately by Alice and Bob, interspersed with the communication of qubits from Alice to Bob or Bob to Alice. One might imagine that measurements could be performed in addition to unitary operations, however the effect of any measurements may be simulated using standard techniques by adding ancilla qubits to the description of Alice or Bob's system. The final step of the protocol consists of a measurement performed by Bob, which has outcome Y. We aim to bound the mutual information $I(X:Y)$, where X is Alice's classical data, consisting of n bits. In order that the protocol be reliable, it must be possible to have $I(X:Y) = n$, in the case when Alice's classical data is uniformly distributed. One final convenience is to assume that initially Alice and Bob both start with a system in a standard pure state. It is possible that the protocol starts with either Alice or Bob having a mixed state, however any such protocol can be simulated without extra cost using a purification of the mixed state.

Generically, at any stage of the protocol we will use the notation ρ_x to denote the state of Bob's system, given that Alice's input data was x. We will also use the generic notation $\rho \equiv \sum_x p_x \rho_x$ and $\chi \equiv S(\rho) - \sum_x p_x \rho_x$. We will study the behavior of Bob's χ quantity under the different actions which Alice and Bob may perform. We denote by χ_0 Bob's initial χ quantity, and by χ_F, Bob's final χ quantity. ρ_F denotes ρ upon conclusion of the protocol, immediately before the final measurement.

Note first that Bob's state ρ_x after zero rounds of communication cannot depend on x, and thus $\chi_0 = 0$. Consider the following observations about how

Bob's χ changes. To reduce notational clutter, we will use the notation ρ_x to denote the state of Bob's system before each of the following processes, and ρ'_x to denote the state of Bob's system after each of the following processes. Similar conventions are used for ρ, ρ', χ and χ'.

1. Suppose Alice performs a unitary operation on her system. Then $\Delta\chi = \Delta S(\rho) = 0$ for this process, since the states ρ_x of Bob's system do not change during the process.
2. Suppose Bob performs a unitary operation on his system. It is easy to verify that $\Delta\chi = \Delta S(\rho) = 0$ for this process, from the unitary invariance of the entropy.
3. Suppose Alice sends a qubit to Bob. Let Q denote the qubit, and B Bob's quantum system before the qubit was sent, so QB is Bob's system after the qubit has arrived. For an arbitrary state of QB we have the subadditivity inequality $S(Q,B) \leq S(Q) + S(B) \leq 1 + S(B)$, as $S(Q) \leq 1$. Thus $S(\rho') \leq S(\rho) + 1$. Also for an arbitrary state of QB we have the Araki-Lieb inequality [1] $S(Q,B) \geq S(B) - S(Q) \geq S(B) - 1$, from which we deduce that $S(\rho'_x) \geq S(\rho_x) - 1$. Thus
$$\chi' = S(\rho') - \sum_x p_x S(\rho'_x) \leq S(\rho) - \sum_x p_x S(\rho_x) + 2. \qquad (31)$$
That is, $\Delta\chi \leq 2$ for this process. Note also that $\Delta S(\rho) \leq 1$ for this process.
4. Suppose Bob sends a qubit to Alice. Then $\rho'_x = \mathrm{tr}_Q(\rho_x)$, where Q is the qubit sent to Alice. As we noted above, $\chi' \leq \chi$, so $\Delta\chi \leq 0$ for this process. Note also that $\Delta S(\rho) \leq 1$ for this process, by the Araki-Lieb inequality [1].

Combining the observations about $\Delta\chi$ for these processes, we find that $\Delta\chi$ for the entire communication protocol must satisfy $\Delta\chi \leq n_{AB} \times 2 + n_{BA} \times 0 = 2n_{AB}$. But $\chi(0) = 0$, so $\chi_F \leq 2n_{AB}$. Suppose Bob makes a measurement on his system, with outcome Y, and tries to infer the value of X from that measurement. Then Holevo's theorem tells us that $I(X:Y) \leq \chi_F \leq 2n_{AB}$. But in order that Alice be able to reliably transmit her n bits of information to Bob, we must have $I(X:Y) = n$. Thus $n \leq 2n_{AB}$, and since n_{AB} is an integer, we must have $n_{AB} \leq \lceil n/2 \rceil$, as we set out to prove.

Furthermore, noting that $\chi \leq S(\rho)$ and $S(\rho) = 0$ initially, we can combine the above observations about $\Delta S(\rho)$ to see that $\chi_F \leq S(\rho_F) \leq n_{AB} + n_{BA}$. Holevo's theorem therefore implies that $n \leq n_{AB} + n_{BA}$ if Alice is to reliably transmit n bits of classical information to Bob. **QED**