SIAM J. COMPUT.
Vol. 30, No. 6, pp. 1829–1841

QUANTUM ENTANGLEMENT AND COMMUNICATION COMPLEXITY*

HARRY BUHRMAN†, RICHARD CLEVE‡, AND WIM VAN DAM§

Abstract. We consider a variation of the communication complexity scenario, where the parties are supplied with an extra resource: particles in an entangled quantum state. We note that "quantum nonlocality" can be naturally expressed in the language of communication complexity. These are communication complexity problems where the "output" is embodied in the correlations between the outputs of the individual parties. Without entanglement, the parties must communicate to produce the required correlations; whereas, with entanglement, *no* communication is necessary to produce the correlations. In this sense, nonlocality proofs can also be viewed as communication complexity problems where the presence of quantum entanglement reduces the amount of necessary communication. We show how to transform examples of nonlocality into more traditional communication complexity problems, where the output is explicitly determined by each individual party. The resulting problems require communication with or without entanglement, but the required communication is less when entanglement is available. All these results are a noteworthy contrast to the well-known fact that entanglement cannot be used to actually simulate or compress classical communication between remote parties.

Key words. complexity theory, communication complexity, quantum computing

AMS subject classifications. 68Q15, 68Q40

PII. S0097539797324886

1. Introduction and summary of results.

One of the most remarkable aspects of quantum physics is the notion of *quantum entanglement*. If two particles are in an entangled state, then, even if the particles are physically separated by a great distance, they behave in some respects as a single entity. The entangled particles exhibit what physicists call *nonlocal* effects. Informally, these are effects that cannot occur in a world governed by the laws of "classical" physics unless communication occurs between the particles. Moreover, if the physical separation between the particles is large and the time between the observations is small, then this entailed communication may exceed the speed of light! Nonlocal effects were alluded to in a famous 1935 paper by Einstein, Podolsky, and Rosen [13]. Einstein later referred to this as *spukhafte Fernwirkungen* (spooky actions at a distance) (see [12, 25, 30] for more historical background). In 1964, Bell [3] formalized the notion of two-particle nonlocality in terms of correlations among probabilities in a scenario where one of a number of a measurements are performed on each particle. He showed that the results of the measurements that occur quantum physically can be correlated in a way that cannot occur classically unless the type of measurement selected to be per-

*Received by the editors July 24, 1997; accepted for publication (in revised form) August 3, 2000; published electronically March 13, 2001.

http://www.siam.org/journals/sicomp/30-6/32488.html

†CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands (buhrman@cwi.nl). This author was supported in part by NWO, SION Project 612-34-002, EU through NeuroCOLT ESPRIT Working Group 8556, HC&M grant CCR 92-09833, and Fifth Framework Program FET project QAIP IST-1999-11234.

‡Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4 (cleve@cpsc.ucalgary.ca). This author was supported in part by Canada's NSERC.

§CWI, and Computer Science Division, University of California, 665 Soda Hall, Berkeley, CA 94720 (vandam@eecs.berkeley.edu). This author was supported by iLLc Amsterdam, EU project QAIP IST-1999-11234, and NWO's TALENT grant S 62-552.

formed on one particle affects the result of the measurement performed on the other particle.

In reality—which is quantum physical—the nonlocal effects exhibited by entangled particles do not involve any communication (consequently, nonlocality does not entail communication faster than the speed of light). In operational terms, the "spooky actions at a distance" that Einstein referred to cannot be used to simulate a communication channel. More precisely, if two physically separated parties, Alice and Bob, initially possess entangled particles and then Alice is given an arbitrary n-bit string x, there is no way for Alice to manipulate her particles in order to convey any information about x to Bob (unless she explicitly sends that information to him). Moreover, entanglement cannot even be used to *compress* the information in x: for Alice to convey x to Bob, she must in general send n bits—any smaller number will not suffice. The proof of this is based on a fundamental theorem in quantum information theory due to Holevo [17] (see also [16, 10]). Similar results apply to communication involving more than two parties.

Now consider the *communication complexity* scenario introduced by Yao [33]. Alice obtains an n-bit string x and Bob obtains an n-bit string y, and the goal is for them to determine $f(x, y)$, for some function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, with as little communication between them as possible. Clearly, $n + 1$ bits of communication always suffice (Alice sends all her n bits to Bob, Bob computes $f(x, y)$ and sends the one-bit answer to Alice), but for some functions fewer bits suffice. This scenario and variations of it have been widely studied (see [23] for an extensive survey).

In one variation of the above communication complexity scenario, there are more than two parties, each of which is given a subset of the input data. In another variation, all parties have access to a common "public" string of random bits. This string can be assumed to have been communicated during a "set up" stage prior to the parties being given their input data. For some functions, this prior random string reduces the communication complexity for a worst-case input if a small error probability is permitted (here, a worst-case input is understood to be chosen independently of the random string).

The first variation of the communication complexity scenario that incorporates quantum information was proposed by Yao [34]. In this model, Alice and Bob are allowed to communicate with *quantum bits (qubits)* rather than classical bits. Kremer [22] includes many important definitions and basic results for this model, including a proof that for the INNER PRODUCT function $f(x, y) = x_0 \cdot y_0 + x_1 \cdot y_1 + \cdots + x_{n-1} \cdot y_{n-1} \bmod 2$, the qubit communication must be $\Omega(n)$ qubits. These works leave open the question of whether quantum information can ever be advantageous over classical information for a communication complexity problem.

In the present paper, we consider an alternate way of incorporating quantum information into the communication complexity scenario. Here Alice and Bob's communication is with classical bits, but they are provided with a priori information that is entangled. On the face of it, it may appear that a prior quantum entanglement cannot reduce communication complexity because of the aforementioned theorem of Holevo. Consider the following informal argument, where Alice and Bob are given input strings x and y, and their goal is to collectively determine $f(x, y)$:

1. Assume that the classical communication complexity of function $f(x, y)$ is k. That is, k bits of communication are necessary for Alice and Bob to acquire the answer.

2. By Holevo's Theorem [17], the prior entanglement cannot simulate or even compress any particular message in a classical communication protocol.
3. Ergo, even with prior entanglement, the communication complexity of $f(x, y)$ is k.

A similar informal argument could be made for three-party scenarios. We shall demonstrate that this conclusion is incorrect for both scenarios.

Our first counterexample is in a three-party setting. We give an example of a function $f : \{0,1\}^2 \times \{0,1\}^2 \times \{0,1\}^2 \to \{0,1\}$, where, without prior quantum entanglement, four bits of communication are *necessary* to compute $f(x, y, z)$; whereas, with prior quantum entanglement, three bits of communication are *sufficient* to compute $f(x, y, z)$. The function is actually a partial function, defined on a subset of $\{0,1\}^2 \times \{0,1\}^2 \times \{0,1\}^2$ (i.e., the input data (x, y, z) obeys a certain "promise"). If we want to allow any input combination, then f can be defined as a relation (rather than a function). The protocol employing quantum entanglement uses less communication than necessary by any classical protocol by manipulating the entanglement so as to *circumvent* (rather than simulate) communication. Our technique is based on an interesting example of tripartite nonlocality due to Mermin [26]. Mermin's result is a refinement (from four components to three) of a similar result by Greenberger, Horne, and Zeilinger [14].

We also give an example of a two-party probabilistic communication complexity scenario with a function $g : \{0,1\}^2 \times \{0,1\}^2 \to \{0,1\}$ for which, with a classical shared random string but no prior entanglement, three bits of communication are *necessary* to compute $g(x, y)$ with probability at least $\cos^2(\frac{\pi}{8}) = 0.853\ldots$; whereas, with prior entanglement, two bits of communication are *sufficient* to compute $g(x, y)$ with the same probability. Unlike the previous three-party example, this function does not require a promise on the input data (x, y). The correlations in this two-party scenario are based on an example of nonlocality due to Clauser et al. [8].

Although, in both of the above cases, the savings in communication are not in an asymptotic setting, these results demonstrate that quantum entanglement can change the nature of communication complexity. After the initial announcement of these results and those of [9], several stronger quantum vs. classical separations appeared, and these are briefly reviewed in section 5.

2. Three-party deterministic scenarios. Let us begin by considering the following scenario, which is a reformulation of the one in [26] but cast in terms of data processing. Alice, Bob, and Carol receive input bits x, y, and z, respectively, which are arbitrary subject to the condition that $x \oplus y \oplus z = 0$. Once they receive their input data, they are forbidden from having any communication between them. Their goal is to produce output bits a, b, and c, respectively, such that

$$a \oplus b \oplus c = \begin{cases} 0 & \text{if } xyz = 000, \\ 1 & \text{if } xyz \in \{011, 101, 110\}. \end{cases} \tag{2.1}$$

Let us consider whether or not the trio can accomplish the above in terms of classical information. Since Alice cannot receive any information from Bob or Carol, her output bit a can depend only on the value of her input bit x. Let a_0 (respectively, a_1) be Alice's output when her input bit is 0 [1]. Similarly, let b_0, b_1 and c_0, c_1 be Bob and Carol's outputs for their respective input values. Note that the six bits $a_0, a_1, b_0, b_1, c_0, c_1$ completely characterize any (deterministic) strategy of Alice, Bob, and Carol (and probabilistic strategies will not help here since no error probability is

permitted). The conditions of the problem translate into the equations

$$\begin{aligned} a_0 \oplus b_0 \oplus c_0 &= 0, \\ a_0 \oplus b_1 \oplus c_1 &= 1, \\ a_1 \oplus b_0 \oplus c_1 &= 1, \\ a_1 \oplus b_1 \oplus c_0 &= 1. \end{aligned} \tag{2.2}$$

It is impossible to satisfy all four equations simultaneously. This is because summing the four equations (modulo two) yields $0 = 1$. Therefore, for any strategy, there exists an input configuration $xyz \in \{000, 011, 101, 110\}$ for which it fails.

Now consider the same problem, but where Alice, Bob, and Carol are supplied with qubits Q_A, Q_B, and Q_C, respectively, where the state of $\mathsf{Q}_A\mathsf{Q}_B\mathsf{Q}_C$ is initialized to

$$\tfrac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle). \tag{2.3}$$

The parties are allowed to apply unitary transformations and perform measurements on their individual qubits, but communication between the parties is still forbidden. It turns out that now the parties *can* produce a, b, c satisfying (2.1). This is achieved by the following procedures:

Procedure for Alice:
if $x = 1$ **then apply** H **to** Q_A
measure Q_A **yielding bit** a

Procedure for Bob:
if $y = 1$ **then apply** H **to** Q_B
measure Q_B **yielding bit** b

Procedure for Carol:
if $z = 1$ **then apply** H **to** Q_C
measure Q_C **yielding bit** c

In the above, H is the Hadamard transform, which is represented in the standard basis ($|0\rangle$ and $|1\rangle$) as

$$H = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{2.4}$$

and the measurements are performed in the standard basis.

We claim that the described procedure produces three output bits a, b, and c, satisfying (2.1). To see why this is so, first consider the case where $xyz = 000$. In this case, no H transform is applied to any of the three qubits. Therefore $\mathsf{Q}_A\mathsf{Q}_B\mathsf{Q}_C$ is measured directly in state (2.3), so the results will satisfy $a \oplus b \oplus c = 0$.

Next, in the case where $xyz = 011$, a Hadamard transform is applied to Q_B and to Q_C but not to Q_A. Therefore $\mathsf{Q}_A\mathsf{Q}_B\mathsf{Q}_C$ is measured in state

$$I \otimes H \otimes H \left(\tfrac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)\right) = \tfrac{1}{2}(|001\rangle + |010\rangle - |100\rangle + |111\rangle), \tag{2.5}$$

so $a \oplus b \oplus c = 1$. The remaining cases where $xyz = 101$ and 110 are similar by the symmetry of state (2.3).

Note that a, b, and c by themselves are just random bits, uncorrelated with xyz. It is only the *trivariate correlations* among a, b, and c that are related to the input data xyz. Although the above task has some of the flavor of a communication complexity problem, it is technically different in that individual parties acquire no information.

We now construct a function based on the above where the presence of entanglement reduces its communication complexity.

Consider the function f defined on all triples $(x, y, z) \in \{0,1,2,3\} \times \{0,1,2,3\} \times \{0,1,2,3\}$ which satisfy the condition

$$x + y + z \equiv 0 \pmod 2 \tag{2.6}$$

for which its value is given as

$$f(x, y, z) = \frac{(x + y + z) \bmod 4}{2} \tag{2.7}$$

(the value is always 0 or 1 by (2.6)). We represent the numbers x, y, and z in binary notation as x_1x_0, y_1y_0, and z_1z_0. In terms of these bits, the condition of (2.6) is

$$x_0 \oplus y_0 \oplus z_0 = 0, \tag{2.8}$$

and the function of (2.7) for inputs satisfying (2.8) is

$$f(x, y, z) = x_1 \oplus y_1 \oplus z_1 \oplus (x_0 \vee y_0 \vee z_0). \tag{2.9}$$

We assume the standard multiparty communication channel, where each bit that a party sends is broadcast to all other parties. Also, at the conclusion of the protocol, *all* parties must be able to determine the value of the function.

In the following two subsections, we show that with a prior entanglement, three bits of communication are sufficient to compute $f(x, y, z)$, whereas, without a prior entanglement, four bits of communication are necessary to compute $f(x, y, z)$.

2.1. The communication complexity with quantum entanglement is three bits. We now show that if Alice, Bob, and Carol initially share qubits Q_A, Q_B, and Q_C, respectively, in state (2.3), then there is a protocol for f where each party broadcasts only a single classical bit. The idea is based on applying the procedures at the beginning of this section using $x_0y_0z_0$ as the input. This requires no communication and provides Alice, Bob, and Carol with bits a, b, and c, respectively, such that $a \oplus b \oplus c = x_0 \vee y_0 \vee z_0$ (by (2.1)). Next Alice broadcasts the bit $(x_1 \oplus a)$, Bob broadcasts $(y_1 \oplus b)$, and Carol broadcasts $(z_1 \oplus c)$. At this point, each party knows $(x_1 \oplus a)$, $(y_1 \oplus b)$, and $(z_1 \oplus c)$, from which they can each determine the bit

$$\begin{aligned}(x_1 \oplus a) \oplus (y_1 \oplus b) \oplus (z_1 \oplus c) &= x_1 \oplus y_1 \oplus z_1 \oplus (a \oplus b \oplus c) \\ &= x_1 \oplus y_1 \oplus z_1 \oplus (x_0 \vee y_0 \vee z_0) \\ &= f(x, y, z),\end{aligned} \tag{2.10}$$

as required.

2.2. The communication complexity without quantum entanglement is four bits. In this section, we show that in the classical setting, four bits of communication are necessary to compute $f(x, y, z)$.

One can view any k-bit protocol as a binary tree of depth k, where each node that is not a leaf is labeled A(lice), B(ob), or C(arol). This labeling indicates which party will broadcast the next bit. An execution of the protocol corresponds to a path from the root of the tree to a leaf. Each leaf node is labeled 0 or 1, indicating the common output that results from the execution leading to that leaf. To establish our lower

bound, it suffices to show that no protocol-tree of depth three correctly computes $f(x, y, z)$.

We use the following lemma, which implies that in any correct protocol, all three parties must broadcast at least one bit.

LEMMA 2.1. *For any correct protocol-tree, on every path from its root to a leaf, each of A, B, and C must occur as a label at least once.*

Proof. Suppose that there exists a path along which one party, say, A, does not occur as a label. Let the leaf of that path be labeled $l \in \{0, 1\}$. Since this path does not include any reference to Alice's data, the same path is taken if x_1 is negated and all other input bits are held constant. However, by (2.9), negating x_1 also negates the value of $f(x, y, z)$, so the protocol cannot be correct for both possible values of x_1. □

Next suppose we have a protocol-tree of depth three for $f(x, y, z)$. Assume, without loss of generality, that the root of the tree is labeled A. The bit that Alice broadcasts is some function $\phi : \{0, 1\}^2 \to \{0, 1\}$ of her input data x alone. The function ϕ partitions $\{0, 1\}^2$ into two classes, $\phi^{-1}(0)$ and $\phi^{-1}(1)$. Call these two classes S_0 and S_1 and assume (without loss of generality) that $00 \in S_0$.

Next assume for the moment that the two children of the root of the protocol-tree are both labeled B (we shall see later that the other cases can be handled similarly). Then, by Lemma 2, the four children of B are all labeled C. Therefore, after Alice and Bob each send a bit, Carol must have enough information to determine the value of $f(x, y, z)$, since Carol broadcasts the third bit and does not gain any information from doing this. We shall show that this is impossible whatever S_0 and S_1 are.

There are two cases (the second of which has three subcases).

Case 1. $|S_0| = 1$. Recall that $00 \in S_0$, so $01, 10, 11 \in S_1$. Now, should the bit that Alice broadcasts specify that $x \in S_1$, Bob must follow this by broadcasting one bit from which Carol can completely determine the value of $f(x, y, z)$. Suppose that Bob sends the bit consistent with $y = 01$. If $z = 00$, then, from Carol's perspective, the possible values of (x, y, z) include $(01, 01, 00)$ and $(11, 01, 00)$ for which the respective values of $f(x, y, z)$ are 1 and 0. Therefore Carol cannot determine the value of $f(x, y, z)$ in this case.

Case 2. $|S_0| \geq 2$. There are three subcases where S_0 contains 01, 10, or 11 in addition to 00.

Case 2.1. S_0 *contains* 00 *and* 01. Here we consider the case where Alice broadcasts the bit specifying that $x \in S_0$. Bob must follow this by broadcasting one bit from which Carol can completely determine the value of $f(x, y, z)$. The bit that Bob broadcasts induces a partition of the possible values for y into two classes. If $z = 00$, then, from Carol's perspective, after receiving Alice's bit but before receiving Bob's bit, the possible values of (x, y, z) include $(00, 00, 00)$, $(00, 10, 00)$, $(01, 01, 00)$, and $(01, 11, 00)$, and the respective values of $f(x, y, z)$ on these points are 0, 1, 1, and 0. Therefore, for the protocol to be successful in this case, the partition that Bob's bit induces on y must place 00 and 11 in one class and 01 and 10 in the other class (otherwise Carol would not be able to determine $f(x, y, z)$ when $z = 00$). On the other hand, if $z = 01$, then, from Carol's perspective, the possible values of (x, y, z) include $(00, 01, 01)$, $(00, 11, 01)$, $(01, 00, 01)$, and $(01, 10, 01)$, and the respective values of $f(x, y, z)$ on these points are 1, 0, 1, and 0. Since we have established that Bob's bit does not distinguish between $y = 00$ and $y = 11$, Bob's bit is not sufficient information for Carol to determine $f(x, y, z)$ in this case.

Case 2.2. S_0 *contains* 00 *and* 10. The argument is similar to that in Case 1. Assume that Alice sends the bit specifying that $x \in S_0$. If Bob follows this by sending the bit consistent with $y = 00$ and $z = 00$, then, from Carol's perspective, the possible values of (x, y, z) include $(00, 00, 00)$ and $(10, 00, 00)$, and the respective values of $f(x, y, z)$ on these points are 0 and 1. Thus Carol cannot determine the value of $f(x, y, z)$ in this case.

Case 2.3. S_0 *contains* 00 *and* 11. The argument is similar to Case 2.1. Suppose that Alice broadcasts the bit specifying that $x \in S_0$. Consider Carol's perspective. If $z = 00$, then the possible values of (x, y, z) include $(00, 00, 00)$, $(00, 10, 00)$, $(11, 01, 00)$, and $(11, 11, 00)$, and the respective values of $f(x, y, z)$ on these points are 0, 1, 0, and 1; whereas, if $z = 01$, then the possible values of (x, y, z) include $(00, 01, 10)$, $(00, 11, 01)$, $(11, 00, 01)$, and $(11, 10, 01)$, and the respective values of $f(x, y, z)$ on these points are 1, 0, 0, 1. No binary partitioning of y will work for both possibilities.

The cases where the two children of the root of the protocol-tree are CC, CB, and BC have an analogous proof as above with the roles of B and C possibly reversed.

This completes the proof of the lower bound of four bits. The following deterministic four-bit protocol shows that this bound is tight.

A classical four bit protocol. First, Bob and Carol start by broadcasting the bits y_0, y_1 (Bob) and z_1 (Carol). After that, Alice now knows—by the promise of (2.8)—the bit $z_0 = x_0 \oplus y_0$ and hence all six bit values involved. The fourth and last bit of communication is therefore the announcement of the answer $f(x, y, z)$ by Alice to Bob and Carol.

3. Two-party probabilistic scenarios. The following scenario can be viewed as a reformulation of the nonlocality proof in [8] into data processing terminology. Alice and Bob receive input bits x and y, respectively, and, after this, they are forbidden from communicating with each other. Their goal is to produce output bits a and b, respectively, such that

$$a \oplus b = x \wedge y, \tag{3.1}$$

or, failing that, to satisfy this condition with as high a probability as possible.

To analyze the situation in terms of classical information, first consider the case of deterministic strategies. For these, Alice's output bit depends solely on her input bit x and similarly for Bob. Let a_0, a_1 be the two possibilities for Alice and b_0, b_1 be the two possibilities for Bob. These four bits completely characterize any deterministic strategy. Condition (3.1) translates into the equations

$$\begin{aligned} a_0 \oplus b_0 &= 0, \\ a_0 \oplus b_1 &= 0, \\ a_1 \oplus b_0 &= 0, \\ a_1 \oplus b_1 &= 1. \end{aligned} \tag{3.2}$$

It is impossible to satisfy all four equations simultaneously (since summing them modulo two yields $0 = 1$). Therefore it is impossible to satisfy condition (3.1) absolutely.

By using a probabilistic strategy, Alice and Bob can satisfy condition (3.1) with probability $\frac{3}{4}$. For such a strategy, we allow Alice and Bob to have a priori classical random variables, whose distribution is independent of that of the inputs x and y. Note that any three of the four equations of (3.2) *can* be simultaneously satisfied. The probabilistic strategy now works as follows. Alice and Bob have random variables

R_A and R_B, respectively, which are each uniformly distributed over $\{0,1,2,3\}$ and completely correlated with each other (i.e., $R_A = R_B$). These variables specify to both of them one of the four equations to violate while satisfying the other three. Alice and Bob then follow the deterministic procedure corresponding to a preagreed a_0, a_1, b_0, b_1 which satisfy the three equations determined by R_A and R_B. It is easy to see that (a) for any input xy, the resulting outputs satisfy condition (3.1) with probability $\frac{3}{4}$, and (b) this is optimal in that no probabilistic strategy can attain a success probability greater than $\frac{3}{4}$.

Now consider the same problem but where Alice and Bob are supplied with qubits Q_A and Q_B, respectively (instead of random variables), where the state of $\mathsf{Q}_A\mathsf{Q}_B$ is initialized to

$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \tag{3.3}$$

It turns out that now the parties can produce data that satisfies condition (3.1) with probability $\cos^2(\frac{\pi}{8}) = 0.853\ldots$, which is higher than what is possible in the classical case. This is achieved by the following procedures:

Procedure for Alice:	Procedure for Bob:
if $x = 0$ **then**	**if** $y = 0$ **then**
apply $R(-\frac{\pi}{16})$ to Q_A	**apply** $R(-\frac{\pi}{16})$ to Q_B
else	**else**
apply $R(\frac{3\pi}{16})$ to Q_A	**apply** $R(\frac{3\pi}{16})$ to Q_B
measure Q_A **yielding bit** a	**measure** Q_B **yielding bit** b

In the above, $R(\theta)$ is the rotation by angle θ which is represented in the standard basis as

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \tag{3.4}$$

and the measurements are performed in the standard basis. If Alice rotates by θ_1 and Bob rotates by θ_2, then the state of $\mathsf{Q}_A\mathsf{Q}_B$ becomes

$$\frac{1}{\sqrt{2}}\left(\cos(\theta_1+\theta_2)(|00\rangle - |11\rangle) + \sin(\theta_1+\theta_2)(|01\rangle + |10\rangle)\right), \tag{3.5}$$

and, after the measurements, the probability that $a \oplus b = 0$ is $\cos^2(\theta_1 + \theta_2)$. It is now straightforward to verify that condition (3.1) is satisfied with probability $\cos^2(\frac{\pi}{8})$ for all input possibilities.

From the above, we can construct a function for which the presence of entanglement reduces its communication complexity in a probabilistic sense. Define $g : \{0,1\}^2 \times \{0,1\}^2 \to \{0,1\}$ as

$$g(x,y) = x_1 \oplus y_1 \oplus (x_0 \wedge y_0). \tag{3.6}$$

An execution of a probabilistic protocol for g is considered successful if and only if the value determined by Alice and the value determined by Bob are *both* correct.

In the following two subsections, we show that, with a prior quantum entanglement and two bits of communication, the probability of success can be at least $\cos^2(\frac{\pi}{8}) = 0.853\ldots$, whereas, with a shared random string instead of quantum entanglement and two bits of communication, the probability of success cannot exceed $\frac{3}{4}$. Thus, without prior entanglement, to achieve a success probability of at least $\cos^2(\frac{\pi}{8})$, *three* bits of communication are necessary.

TABLE 3.1
The values of $g(x, y)$. The columns are indexed by x and the rows are indexed by y.

$g(x,y)$	00	01	10	11
00	0	0	1	1
01	0	1	1	0
10	1	1	0	0
11	1	0	0	1

3.1. With quantum entanglement. Here we show that if Alice and Bob initially share qubits Q_A and Q_B, respectively, in state (3.3), then there is a protocol which successfully computes g with probability $\cos^2(\frac{\pi}{8})$. Alice and Bob first apply the procedures at the beginning of this section using $x_0 y_0$ as input. This requires no communication and provides Alice and Bob with bits a and b, respectively, such that $\Pr[a \oplus b = x_0 \wedge y_0] = \cos^2(\frac{\pi}{8})$. Then Alice sends $(a \oplus x_1)$ to Bob, and Bob sends $(b \oplus y_1)$ to Alice. At this point, each party can determine the bit

$$(a \oplus x_1) \oplus (b \oplus y_1) = x_1 \oplus y_1 \oplus (a \oplus b), \tag{3.7}$$

which equals $x_1 \oplus y_1 \oplus (x_0 \wedge y_0) = g(x, y)$ with probability $\cos^2(\frac{\pi}{8})$, as required.

3.2. With shared classical random bits but no quantum entanglement. We now show that if Alice and Bob initially share classical random bits but no quantum entanglement, then there is no two-bit protocol in which both parties output the correct value of $g(x, y)$ with probability greater than $\frac{3}{4}$. By Theorem 3.20 of [23], it is sufficient to prove the lower bound on the error probability for all deterministic protocols with respect to *random inputs* from $\{0,1\}^2 \times \{0,1\}^2$ (which we can take to be uniformly distributed). As noted in section 2.2, we can represent any two-bit protocol as a binary tree of depth two with nonleaf nodes labeled A(lice) and B(ob).

Assume, without loss of generality, that the root of the protocol-tree is labeled A. The first bit that Alice sends is some function $\phi : \{0,1\}^2 \to \{0,1\}$ of her input data x alone. The function ϕ partitions $\{0,1\}^2$ into two classes $S_0 = \phi^{-1}(0)$ and $S_1 = \phi^{-1}(1)$. Let the first and second children of the root correspond to the paths traversed when the first bit sent (by Alice) indicates that $x \in S_0$ and $x \in S_1$, respectively. We must consider all partitions S_0 and S_1 in combination with all cases where the two children of the root are BB, AB, or AA (the case BA can be omitted by symmetry).

LEMMA 3.1. *If the child corresponding to S_i is labeled B, then, conditioned on $x \in S_i$, the probability that Bob correctly determines $g(x, y)$ is at most 1 if $|S_i| = 1$; $\frac{3}{4}$ if $|S_i| = 2$; $\frac{2}{3}$ if $|S_i| = 3$; and $\frac{1}{2}$ if $|S_i| = 4$. There is no well-defined probability for the empty set $|S_i| = 0$.*

Proof. The case where $|S_i| = 1$ is trivial.

For the case where $|S_i| = 2$, first consider the subcase where $S_i = \{00, 01\}$. Under the condition $x \in S_i$, (x, y) is a position in one of the first two columns of Table 3.1, and Alice's bit to Bob indicates this to him. From Bob's perspective, if $y = 00$, then $g(x, y) = 0$, so Bob can determine the correct answer. Similarly, if $y = 10$, then $g(x, y) = 1$, so Bob can determine the correct answer. However, if $y = 01$, then, since the first two columns of the table differ in this row, whatever function of Alice's message and y Bob computes, the probability that it will match $g(x, y)$ is at most $\frac{1}{2}$. Similarly, if $y = 01$, then Bob computes the correct answer with probability at most $\frac{1}{2}$. Since these four values of y are equiprobable, the probability that Bob correctly computes $g(x, y)$ conditioned on $x \in S_i$ is at most $\frac{1}{4} \cdot 1 + \frac{1}{4} \cdot 1 + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} = \frac{3}{4}$. The other five subcases in which $|S_i| = 2$ are handled similarly.

For the case where $|S_i| = 3$, first consider the subcase where $S_i = \{00, 01, 10\}$. Under the condition $x \in S_i$, (x, y) is a position in one of the first three columns of Table 3.1, and Alice's bit to Bob indicates this to him. By looking at these three columns of Table 3.1, we observe that, from Bob's perspective, whatever the value of y, the probability of Bob determining $g(x, y)$ is at most $\frac{2}{3}$. The other two subcases in which $|S_i| = 3$ are handled similarly.

The last case $|S_i| = 4$ immediately implies $S_i = \{00, 01, 10, 11\}$, where Bob receives no information about the the string x of Alice. For all possible y's, the probability that Bob guesses $g(x, y)$ correctly is therefore $\frac{1}{2}$.

As the probabilities are conditioned on x being an element of S_i, the case of the empty set $|S_i| = 0$ is not well-defined. □

Now, by Lemma 3.1, if the two children of the root are BB, then the probability that Bob correctly determines $g(x, y)$ is at most $\frac{1}{4} \cdot 1 + \frac{3}{4} \cdot \frac{2}{3} = \frac{3}{4}$ if $|S_0| \neq |S_1|$, and $\frac{1}{2} \cdot \frac{3}{4} + \frac{1}{2} \cdot \frac{3}{4} = \frac{3}{4}$ if $|S_0| = |S_1|$.

Next, we show that for protocol-trees in which the two children of the root are *not* BB, the correctness probability is actually less than $\frac{3}{4}$.

LEMMA 3.2. *If the child corresponding to S_i is labeled A, then, conditioned on $x \in S_i$, the probability that Alice correctly determines $g(x, y)$ is at most $\frac{1}{2}$.*

Proof. If the condition $x \in S_i$ occurs, then Alice receives no information from Bob. Therefore, from Alice's perspective, the value of $g(x, y)$ is either y_1, $y_1 \oplus y_0$, $1 \oplus y_1$, or $1 \oplus y_1 \oplus y_0$ (corresponding to the cases $x = 00$, 01, 10, and 11, respectively). The result now follows from the fact that, from Alice's perspective, y is uniformly distributed over $\{0, 1\}^2$. □

By Lemma 3.2, it follows that if the two children of the root are AA, then the probability that Bob correctly determines $g(x, y)$ is at most $\frac{1}{2}$. The remaining case is where the two children of the root are AB. By applying Lemma 3.2 for the first child and Lemma 3.1 for the second child, the probability that both Alice and Bob correctly determine $g(x, y)$ is at most

- $\frac{1}{4} \cdot \frac{1}{2} + \frac{3}{4} \cdot \frac{2}{3} = \frac{5}{8}$ if $|S_0| = 1$ and $|S_1| = 3$,
- $\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{3}{4} = \frac{5}{8}$ if $|S_0| = 2$ and $|S_1| = 2$,
- $\frac{3}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot 1 = \frac{5}{8}$ if $|S_0| = 3$ and $|S_1| = 1$.

This completes the proof that no two-bit protocol is correct with probability more than $\frac{3}{4}$. There is a straightforward errorless three-bit protocol.

4. The qubit model of communication complexity. In the previous two sections, novel protocols were obtained in the *entanglement model* for communication complexity, where communication is with classical bits, but the parties have an a priori supply of entangled qubits. In the *qubit model* (introduced by Yao [34] and Kremer [22]), the parties have no entanglement but are allowed to communicate with qubits in place of classical bits. Qubits cannot be broadcast [32], so in a multiparty setting a qubit of communication must be sent to a specific party.

In this section, we show how to translate the protocols from sections 2 and 3 in the entanglement model into protocols in the qubit model. By doing so we also prove the same separation between qubit communication complexity and classical communication complexity.

4.1. A deterministic three-party qubit protocol. The following protocol requires only two qubits plus one classical bit of communication to compute f from section 2 with the one-qubit rotation R that we used earlier.

Procedure for Alice:
initialize qubit Q to state $|0\rangle$
apply $R(x \cdot \frac{\pi}{4})$ **to** Q
send Q **to Bob**

Procedure for Bob:
receive Q **from Alice**
apply $R(y \cdot \frac{\pi}{4})$ **to** Q
send Q **to Carol**

Procedure for Carol:
receive Q **from Bob**
apply $R(z \cdot \frac{\pi}{4})$ **to** Q
measure Q**, yielding bit** m
announce the answer m

It is straightforward to verify that the final state of qubit Q is

$$\begin{aligned} R(z \cdot \tfrac{\pi}{4}) \cdot R(y \cdot \tfrac{\pi}{4}) \cdot R(x \cdot \tfrac{\pi}{4})|0\rangle &= \cos((x+y+z) \cdot \tfrac{\pi}{4})|0\rangle + \sin((x+y+z) \cdot \tfrac{\pi}{4})|1\rangle \\ &= |f(x,y,z)\rangle, \end{aligned} \tag{4.1}$$

which implies that the answer as announced by Carol is indeed correct.

4.2. A probabilistic two-party qubit protocol. Also the two-party problem of section 2 can be translated to the qubit model. The following protocol computes g from section 2 with correctness probability 0.853... using only one qubit and one bit of communication:

Procedure for Alice:
initialize qubit Q **to state** $|0\rangle$
apply $R((2x_1 + x_0 - \frac{1}{2}) \cdot \frac{\pi}{4})$ **to** Q
send Q **to Bob**

Procedure for Bob:
receive Q **from Alice**
apply $R((2y_1 + y_0) \cdot \frac{\pi}{4})$ **to** Q
measure Q**, yielding bit** m
announce the answer m

For any combination of input x and y, this final answer m will be the correct value $g(x,y)$ with probability $\cos^2(\frac{\pi}{8}) = 0.853\ldots$, which is identical to the success rate of the entanglement protocol of section 3.1.

5. Discussion of subsequent work. After the publication of [9] and the announcement of this article in 1997, several other results in quantum communication complexity were obtained. In [6] the three-party problem of Chapter 2 was generalized into a k-party problem for which the separation between quantum and classical communication complexity is k versus $\Theta(k \log k)$ bits. For the one-round, three-party setting this article also proved a difference of $n+1$ versus $(3/2)n+1$ bits between communication with and without initial entanglement.

A lower bound of $\Omega(n)$ on the quantum communication complexity of the (two-party) INNER PRODUCT function in [10] showed that the entanglement model does not always allow an improvement over the classical scenario. On the other hand, a significant decrease in communication complexity was established for the DISJOINT function

$$\text{DISJOINT}(x,y) = \begin{cases} 0 & \text{if there exists an } i \text{ such that } x_i = y_i = 1, \\ 1 & \text{otherwise.} \end{cases} \tag{5.1}$$

This well-studied problem has a classical probabilistic communication complexity of $\Omega(n)$ [18, 28], while the authors of [5] gave a qubit protocol requiring only $O(\sqrt{n} \log n)$ qubits of communication. The question whether there exists a more efficient quantum protocol for DISJOINT is still an important open problem. This is especially relevant as

DISJOINT is a complete problem for the communication class "co-NP" [2]. The same article [5] also contained the first exponential separation for the exact distributed computation of a partial two-party function that is related to the Deutsch–Jozsa problem of [11].

In [27] Raz improved on these results by establishing an exponential separation between classical and quantum communication in the bounded-error probabilistic setting. The problem involved is the question for Alice whether her normalized n-dimensional vector $\vec{v} \in \mathbf{C}^n$, after Bob's unitary transformation U, lies in a particular subspace $S \subset \mathbf{C}^n$ or in the orthogonal complement $S^\perp$. (The promise here is that the vector $U\vec{v}$ is close to either S or $S^\perp$.) It is clear that this can be solved with only $2 \log n$ qubits of communication if we store the coefficients of $\vec{v}$ (and $U\vec{v}$) in the amplitudes of a $\log n$ qubit message. The classical lower bound, on the other hand, was proved to be polynomial in n. It is currently still an open problem if it is possible to have an exponential quantum vs. classical reduction in communication complexity for a *total* function.

The "sampling complexity" of a function f and a probability distribution μ is the amount of communication that is required to create a mixture of the possible states $(f(x,y),x,y)$ according to the distribution $\mu(x,y)$ over the input states. In [1] it was shown that we can have an exponential gap between the quantum and the classical sampling complexity of the DISJOINT function.

Separations for nondeterministic (quantum) communication complexity are exhibited in the articles [31] and [24]. In [7], there is a general framework for establishing lower bounds on exact communication complexity with entanglement. For the zero-error (Las Vegas) model, Klauck [20] has given a polynomial difference between the quantum and the classical setting. The question whether quantum information, in general, can reduce the number of rounds is addressed in [21]. (See [29, 19] for spectacular examples of such a reduction in the context of interactive proof systems.)

The preliminary communication complexity results that appear in this article were inspired by examples of quantum nonlocality. Conversely, in [4] new powerful examples of nonlocality are given that follow from the results in [5].

Acknowledgments. We would like to thank Charles Bennett, Lance Fortnow, Richard Jozsa, and Lev Vaidman for helpful discussions.

REFERENCES

[1] A. AMBAINIS, L.J. SCHULMAN, A. TA-SHMA, U. VAZIRANI, AND A. WIGDERSON, *The quantum communication complexity of sampling*, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science, 1998, pp. 342–351.

[2] L. BABAI, P.G. FRANKL, AND J. SIMON, *Complexity classes in communication complexity theory*, in Proceedings of the 27th IEEE Symposium on Foundations of Computer Science, 1986, pp. 337–347.

[3] J.S. BELL, *On the Einstein-Podolsky-Rosen paradox*, Physics, 1 (1964), pp. 195–200.

[4] G. BRASSARD, R. CLEVE, AND A. TAPP, *Cost of exactly simulation quantum entanglement with classical communication*, Phys. Rev. Lett., 83 (1999), pp. 1874–1877.

[5] H. BUHRMAN, R. CLEVE, AND A. WIGDERSON, *Quantum vs. classical communication and computation*, in Proceedings of the 30th Annual ACM Symposium on Theory of Computing, 1998, pp. 63–68.

[6] H. BUHRMAN, W. VAN DAM, P. HØYER, AND A. TAPP, *Multiparty quantum communication complexity*, Phys. Rev. A, 60 (1999), pp. 2737–2741.

[7] H. BUHRMAN AND R. DE WOLF, *Communication complexity lower bounds by polynomials*, in Proceedings of the 16th Annual Conference on Computational Complexity, 2001, to appear.

[8] J.F. CLAUSER, M.A. HORNE, A. SHIMONY, AND R.A. HOLT, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett., 23 (1969), pp. 880–884.

[9] R. CLEVE AND H. BUHRMAN, *Substituting quantum entanglement for communication*, Phys. Rev. A, 56 (1997), pp. 1201–1204.
[10] R. CLEVE, W. VAN DAM, M. NIELSEN, AND A. TAPP, *Quantum entanglement and the communication complexity of the inner product function*, in Proceedings of the First NASA International Conference on Quantum Computing and Quantum Communications, Colin P. Williams, ed., Lecture Notes in Comput. Sci. 1509, Springer-Verlag, Berlin, 1999, pp. 61–74.
[11] D. DEUTSCH AND R. JOZSA, *Rapid solution of problems by quantum computation*, Proc. Roy. Soc. London Ser. A, 439 (1992), pp. 553–558.
[12] A. EINSTEIN, *The Born-Einstein Letters; Correspondence between Albert Einstein and Max and Hedwig Born from* 1916 *to* 1955, Walker, New York, 1971.
[13] A. EINSTEIN, B. PODOLSKY, AND N. ROSEN, *Can quantum-mechanical description of physical reality be complete?*, Phys. Rev., 47 (1935), pp. 777–780.
[14] D.M. GREENBERGER, M. HORNE, AND A. ZEILINGER, *Going beyond Bell's theorem*, in Bell's Theorem, Quantum Theory, and Conceptions of the Universe, M. Kafatos, ed., Kluwer Academic, Dordrecht, 1989, pp. 69–72.
[15] L.K. GROVER, *Quantum Telecomputation*, quant-ph archive, report 9704012, 1997.
[16] P. HAUSLADEN, R. JOZSA, B. SCHUMACHER, M. WESTMORELAND, AND W.K. WOOTTERS, *Classical information capacity of a quantum channel*, Phys. Rev. A (3), 54 (1996), pp. 1869–1876.
[17] A.S. HOLEVO, *Some estimates of the information transmitted by quantum communications channels*, Problemy Peredachi Informatsii, 9 (1973), pp. 3–11, Problems of Information Transmission (USSR), 9 (1973), pp. 177–183 (in English).
[18] B. KALYANASUNDARAM AND G. SCHNITGER, *The probabilistic communication complexity of set intersection*, SIAM J. Discrete Math., 5 (1992), pp. 545–557.
[19] A. KITAEV AND J. WATROUS, *Parallelization, amplification, and exponential time simulation of quantum interactive proof systems*, in Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, 2000, pp. 608–617.
[20] H. KLAUCK, *On quantum and probabilistic communication: Las Vegas and one-way protocols*, in Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, 2000, pp. 644–651.
[21] H. KLAUCK, A. NAYAK, A. TA-SHMA, AND D. ZUCKERMAN, *Interaction in quantum communication and the complexity of set disjointness*, in Proceedings of the 33rd Annual ACM Symposium on Theory of Computing, 2001, to appear.
[22] I. KREMER, *Quantum Communication*, Master's thesis, Hebrew University of Jerusalem, Jerusalem, Israel, 1995.
[23] E. KUSHILEVITZ AND N. NISAN, *Communication Complexity*, Cambridge University Press, Cambridge, UK, 1997.
[24] S. MASSAR, D. BACON, N. CERF, AND R. CLEVE, *Classical simulation of quantum entanglement without local hidden variables*, Phys. Rev. A, to appear.
[25] N.D. MERMIN, *Is the moon there when nobody looks? Reality and the quantum theory*, Phys. Today, 38 (1985), pp. 38–47.
[26] N.D. MERMIN, *What's wrong with these elements of reality?*, Phys. Today, 43 (1990), pp. 9–11.
[27] R. RAZ, *Exponential separation of quantum and classical communication complexity*, in Proceedings of the 31st Annual ACM Symposium on Theory of Computing, 1999, pp. 358–367.
[28] A.A. RAZBOROV, *On the distributional complexity of disjointness*, Theoret. Comput. Sci., 6 (1992), pp. 385–390.
[29] J. WATROUS, *PSPACE has constant-round quantum interactive proof systems*, in Proceedings of the 40th Annual Symposium on Foundations of Computer Science, 1999, pp. 341–351.
[30] J.A. WHEELER AND W.H. ZUREK, EDS., *Quantum Theory and Measurement*, Princeton University Press, Princeton, NJ, 1983.
[31] R. DE WOLF, *Characterization of non-deterministic quantum query and quantum communication complexity*, in Proceedings of the 15th Annual IEEE Conference on Computational Complexity, 2000, pp. 271–278.
[32] W.K. WOOTTERS AND W.H. ZUREK, *A single quantum cannot be cloned*, Nature, 299 (1982), pp. 802–803.
[33] A.C. YAO, *Some complexity questions related to distributed computing*, in Proceedings of the 11th Annual ACM Symposium on Theory of Computing, 1979, pp. 209–213.
[34] A.C. YAO, *Quantum circuit complexity*, in Proceedings of the 34th IEEE Symposium on Foundations of Computer Science, 1993, pp. 352–361.