BRICS

Basic Research in Computer Science

BRICS RS-97-40 Buhrman et al.: Quantum Entanglement and Communication Complexity

Quantum Entanglement
and
Communication Complexity

Harry Buhrman
Richard Cleve
Wim van Dam

BRICS Report Series **RS-97-40**

ISSN 0909-0878 **December 1997**

See back inner page for a list of recent BRICS Report Series publications. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark

Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/97/40/`

Quantum Entanglement and Communication Complexity

Harry Buhrman [*]
CWI, Amsterdam [†]

Richard Cleve [‡]
University of Calgary [§]

Wim van Dam
CWI, Amsterdam [†]

Abstract

We consider a variation of the multi-party communication complexity scenario where the parties are supplied with an extra resource: particles in an entangled quantum state. We show that, although a prior quantum entanglement cannot be used to simulate a communication channel, it can reduce the communication complexity of functions in some cases. Specifically, we show that, for a particular function among three parties (each of which possesses part of the function's input), a prior quantum entanglement enables them to learn the value of the function with only three bits of communication occurring among the parties, whereas, without quantum entanglement, four bits of communication are necessary. We also show that, for a particular two-party probabilistic communication complexity problem, quantum entanglement results in less communication than is required with only classical random correlations (instead of quantum entanglement). These results are a noteworthy contrast to the well-known fact that quantum entanglement cannot be used to actually simulate communication among remote parties.

[*]Partially supported by: NWO by SION Project 612-34-002, EU through NeuroCOLT ESPRIT Working Group Nr. 8556, and HC&M grant CCR 92-09833.

[†]CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands. E-mail: `buhrman@cwi.nl`, `wimvdam@cwi.nl`.

[‡]Partially supported by Canada's NSERC.

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

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 rather than as two separate entities. 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 [6]. Einstein later referred to this as *spukhafte Fernwirkungen* [spooky actions at a distance] (see [3, 10] for more historical background). In 1964, Bell [1] 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 performed 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 bit x, there is no way for Alice to manipulate her particles in order to convey x to Bob when he performs measurements on his particles. The probabilities pertaining to any conceivable measurement that Bob can perform on his particles are all determined by the *(reduced) density matrix* of Bob's particles (see [12] for definitions and discussion), and this density matrix does not change when Alice manipulates her particles by unitary transformations and measurements. Moreover, entanglement cannot even be used to *compress* information in the following sense: for Alice to convey n arbitrary bits to Bob, she must in general send n bits—sending $n-1$ bits will not suffice.

Similar results apply to communications involving more than two parties. For example, suppose that Alice, Bob, and Carol share entangled particles, and then each is given an arbitrary n-bit string. If each party wants to convey his n bits to the other parties using (say) a global broadcast channel then, in spite of the quantum entanglement, Alice must send n bits to the channel, and so must Bob and Carol. The argument is again in terms of the fact that the reduced density matrix of each party's particles cannot be changed by the other parties.

Now, consider the related but different scenario of *communication complexity*. Yao [13] introduced and investigated the following problem. Alice obtains an n-bit string x, and Bob obtains an n-bit string y and the goal is for both of 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 [9] 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 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). If no error probability is allowed then a prior shared random string does not reduce the communication complexity (in a worst-case execution). Also, if the input is selected randomly with respect to some arbitrary but fixed probability distribution then, even if a particular error probability is permitted, the communication complexity does not decrease by having a prior shared random string ([13, 9]).

In the present paper, we consider a variation of the above "classical" communication complexity scenarios where a prior quantum entanglement is available to the parties. We first consider the case where no error probability is permitted. On the face of it, it may appear that a prior quantum entanglement does not reduce the communication complexity of functions. Consider the following informal argument, which we phrase in a three-party setting, where Alice, Bob, and Carol are given input strings x, y, and z respectively, and the goal is to collectively determine $f(x, y, z)$:

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

2. A prior entanglement cannot simulate or even compress any particular act of communication.

3. *Ergo*, even with a prior quantum entanglement, the communication complexity of function $f(x, y, z)$ is k.

We shall demonstrate that this conclusion is incorrect by a counterexample $f(x, y, z)$ where: without a prior quantum entanglement, four bits of communication are *necessary* to compute $f(x, y, z)$; whereas, with a prior quantum entanglement, three bits of communication are *sufficient* to compute $f(x, y, z)$.

Our protocol employing quantum entanglement uses less communication than necessary by any classical protocol by manipulating entangled states to *circumvent* (rather than simulate) communication. Our technique is based on an interesting variation of Bell's Theorem, due to Mermin [11], for three particles which is "deterministic" in the sense that all the associated probabilities are either zero or one. Mermin's result is a refinement of a previous four-particle result, due to Greenberger, Horne, and Zeilinger [7].

We also give an example of a two-party probabilistic communication complexity scenario with a function $g(x, y)$ where: with a classical shared random string but no prior quantum entanglement, three bits of communication are *necessary* to compute $g(x, y)$ with probability at least $\cos^2(\frac{\pi}{8}) = 0.853...$; whereas, with a prior quantum entanglement, two bits of communication are *sufficient* to compute $g(x, y)$ with the same probability. This is based on a variation of Bell's Theorem, due to Clauser, Horne, Shimony, and Holt [5].

Although, in both of the above cases, the savings in communication are not in an asymptotic setting, we consider these results as evidence that quantum entanglement can potentially change the nature of communication complexity.

This paper is an extension of our previous version of these results [4]. Also, Grover [8] recently independently obtained results related to communication complexity in a probabilistic setting.

2 A three-party deterministic scenario

Consider the following three-party scenario. Alice, Bob, and Carol receive x, y, and z respectively, where $x, y, z \in \{0, 1, 2, 3\}$, and the condition

$$x + y + z \equiv 0 \pmod 2 \tag{1}$$

is promised. The common goal is to compute the value of the function

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

(which has value 0 or 1 by Eq. (1)). 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 promise of Eq. (1) is

$$x_0 \oplus y_0 \oplus z_0 = 0, \tag{3}$$

and the function of Eq. (2) for inputs satisfying Eq. (3) is

$$f(x, y, z) = x_1 \oplus y_1 \oplus z_1 \oplus (x_0 \vee y_0 \vee z_0). \tag{4}$$

We assume the standard multi-party 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 quantum entanglement, three bits of communication are sufficient to compute $f(x, y, z)$, whereas, without a prior quantum 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 a certain entanglement of three qubits then there is a protocol in which each party broadcasts one classical bit such that the value $f(x, y, z)$ is known to all parties afterwards. The entanglement is

$$|\mathsf{Q}_A\mathsf{Q}_B\mathsf{Q}_C\rangle = \tfrac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle), \tag{5}$$

where Alice, Bob, and Carol have qubits Q_A, Q_B, and Q_C, respectively. (This is equivalent to the state examined in [11] in an alternate basis.)

The idea is based on applying Mermin's result [11] to enable Alice, Bob, and Carol to obtain bits a, b, and c respectively, such that $a \oplus b \oplus c = x_0 \vee y_0 \vee z_0$. This is achieved by the following procedures:

Procedure for Alice:
if $x_0 = 1$ **then apply** H **to** Q_A
measure Q_A **yielding bit** a

Procedure for Bob:
if $y_0 = 1$ **then apply** H **to** Q_B
measure Q_B **yielding bit** b

Procedure for Carol:
if $z_0 = 1$ **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

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{6}$$

and the measurements are performed in the standard basis. In the language of operators, if a party's low-order bit is 0 then the measurement is with respect to the Pauli matrix σ_z; otherwise (if the low-order bit is 1), the measurement is with respect to the Pauli matrix σ_x.

Lemma 1: *In the described procedure,* $a \oplus b \oplus c = x_0 \vee y_0 \vee z_0$.

Proof: Recall that, by the promise of Eq. (3), $x_0 y_0 z_0 \in \{000, 011, 101, 110\}$.

First, consider the case where $x_0 y_0 z_0 = 000$. In this case, no H transform is applied to any of the qubits Q_A, Q_B, or Q_C. Therefore, $\mathsf{Q}_A\mathsf{Q}_B\mathsf{Q}_C$ is measured in state (5), which implies that $a \oplus b \oplus c = 0 = x_0 \vee y_0 \vee z_0$.

Next, in the case where $x_0 y_0 z_0 = 011$, 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

$$\begin{aligned} I \otimes H \otimes H \left(\tfrac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)\right) &= \\ &\tfrac{1}{2}(|001\rangle + |010\rangle - |100\rangle + |111\rangle), \end{aligned} \tag{7}$$

so $a \oplus b \oplus c = 1 = x_0 \vee y_0 \vee z_0$. The remaining cases where $x_0 y_0 z_0 = 101$ and 110 are similar by the the symmetry of state (5). □

After the above procedure, 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

$$\begin{aligned} (x_1 \oplus a) \oplus (y_1 \oplus b) \oplus (z_1 \oplus c) &= x_1 \oplus y_1 \oplus z_1 \oplus (a \oplus b \oplus c) \\ &= x_1 \oplus y_1 \oplus z_1 \oplus (x_0 \vee y_0 \vee z_0), \end{aligned} \tag{8}$$

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 labelled A(lice), B(ob), or C(arol). This labelling 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 labelled 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: *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 labelled $l \in \{0, 1\}$. 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. But, by Eq. (4), 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. $\Box$

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 labelled A. The bit that Alice broadcasts is some function $\phi : \{0, 1\}^2 \rightarrow \{0, 1\}$ 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 labelled B (we shall see later that the other cases can be handled similarly). Then, by Lemma 2, the four children of B are all labelled 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 were 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. There is a straightforward four-bit protocol, demonstrating that this bound is tight.

2.3 Application to a three-party variation of the inner product function

In this section, we show that $f(x, y, z)$ is a generalization of a restricted version the three-party inner product. The following function is considered in [4]. Alice, Bob, and Carol are given n-bit strings x, y, and z respectively, which are subject to the condition that

$$x \oplus y \oplus z = \overbrace{11\ldots1}^{n}, \tag{9}$$

(where $\oplus$ is applied bitwise) and the goal is to determine the function

$$GIP(x, y, z) = (x_1 \wedge y_1 \wedge z_1) \oplus \cdots \oplus (x_n \wedge y_n \wedge z_n). \tag{10}$$

An alternative way of expressing this problem is to impose no restriction on the inputs, x, y, z, and to extend GIP to a *relation* such that on the points where Eq. (9) is violated, both 0 and 1 are acceptable outputs. Clearly, this problem has the same communication complexity as the original one.

Note that, from the perspective of any two of the three parties, this problem is exactly equivalent to the two-party inner product. Thus, if only two parties participate in the communication, the classical communication complexity is the same as that of the two-party inner product function, which is $n + 1$ ([9]). From this, one might suspect that, even if all three parties participate in the communication, the classical communication complexity remains close to n. In fact, in [4], it is shown that, to solve this problem, it suffices for Alice, Bob, and Carol to: (a) count the number of 0s in their respective input strings; (b) determine the sum of these three quantities modulo four. Also, this sum must be even. This is equivalent to the problem defined by Eqs. (1) and (2), which has classical communication complexity four, and quantum communication complexity three. Therefore, for $GIP(x,y,z)$ as defined by Eqs. (9) and (10), the classical communication complexity is at most four and the quantum communication complexity is at most three. Also, in [4], it is shown that, in a slightly different communication model, the classical communication complexity of $GIP(x,y,z)$ is at least three. A classical lower bound of four in our current communication model can be obtained by slightly modifying the proof in [4].

3 A two-party probabilistic scenario

Consider the following probabilistic two-party communication complexity scenario. Alice and Bob receive x and y respectively, where $x, y \in \{0,1\}^2$. The common goal is to compute the value of the function

$$g(x,y) = x_1 \oplus y_1 \oplus (x_0 \wedge y_0), \tag{11}$$

with as high probability as possible. An execution 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 $\cos^2(\frac{\pi}{8}) = 0.853...$, whereas, with a shared random string instead of quantum entanglement, and two bits of communication, the probability of success cannot exceed 0.75. Thus, without prior entanglement, to achieve a success probability of at least $\cos^2(\frac{\pi}{8})$, *three* bits of communication are necessary.

3.1 With quantum entanglement

We now show that if Alice and Bob initially share a certain entanglement of two qubits then there is a two-bit protocol in which both parties output the correct value of $g(x,y)$ with probability $\cos^2(\frac{\pi}{8}) = 0.853....$ The entanglement is a so-called Einstein-Podolsky-Rosen (EPR) pair

$$|\mathsf{Q}_A \mathsf{Q}_B\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \tag{12}$$

The idea is based on applying the result of Clauser, Horne, Shimony, and Holt [5] to enable Alice and Bob to obtain bits a and b such that

$$\Pr[a \oplus b = x_0 \wedge y_0] = \cos^2(\tfrac{\pi}{8}). \tag{13}$$

This is achieved by the following procedures:

Procedure for Alice:	Procedure for Bob:
if $x_0 = 0$ **then**	**if** $y_0 = 0$ **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

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \tag{14}$$

and the measurements are performed in the standard basis.

The fact that the above protocol satisfies Eq. (13) follows from the fact that if $R(\theta_1) \otimes R(\theta_2)$ is applied to state (12) then the resulting state is

$$|\mathsf{Q}_A\mathsf{Q}_B\rangle = \tfrac{1}{\sqrt{2}}\left(\cos(\theta_1+\theta_2)(|00\rangle - |11\rangle) + \sin(\theta_1+\theta_2)(|01\rangle + |10\rangle)\right), \tag{15}$$

which is straightforward to verify.

After this procedure, 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

$$(a \oplus x_1) \oplus (b \oplus y_1) \quad = \quad x_1 \oplus y_1 \oplus (a \oplus b), \tag{16}$$

which equals $x_1 \oplus y_1 \oplus (x_0 \wedge y_0)$ 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 [9], 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 2-bit protocol as a binary tree of depth 2, with non-leaf nodes labelled A(lice) and B(ob).

Assume, without loss of generality, that the root of the protocol-tree is labelled 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

	00	01	10	11
00	0	0	1	1
01	0	1	1	0
10	1	1	0	0
11	1	0	0	1

Table 1: The values of $g(x, y)$. The columns are indexed by x and the rows are indexed by y.

$S_0 = \phi^{-1}(0)$ and $S_1 = \phi^{-1}(1)$. Let the first child and second child 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: *If the child corresponding to S_i is labelled* 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 $|S_i| = 2$; and $\frac{2}{3}$, if $|S_i| = 3$.*

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 the table, 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 the table, and Alice's bit to Bob indicates this to him. By looking at these three columns of the table, 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. $\Box$

Now, by Lemma 3, 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 4: *If the child corresponding to S_i is labelled* 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 $\{0,1\}^2$. $\Box$

By Lemma 4, 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 4 for the first child and Lemma 3 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 Acknowledgments

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

References

[1] J.S. Bell, "On the Einstein-Podolsky-Rosen paradox", *Physics*, Vol. 1, 1964, pp. 195–200.

[2] M. Ben-Or and R. Cleve, "Computing Algebraic Formulas Using a Constant Number of Registers", *SIAM Journal on Computing*, Vol. 21(1), 1992, pp. 54–58.

[3] *The Born-Einstein Letters*, with comments by M. Born, Walker, 1971.

[4] R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication", Technical Report 9704026, Archive `http://xxx.lanl.gov/archive/quant-ph`, 1997.

[5] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, "Proposed experiment to test local hidden-variable theories", *Physical Review Letters*, Vol. 23, 1969, pp. 880–884.

[6] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be complete?", *Physical Review*, Vol. 47, 1935, pp. 777–780.

[7] D.M. Greenberger, M. Horne, and A. Zeilinger, "Going beyond Bell's theorem", in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos, Kluwer Academic, 1989, pp. 69–72.

[8] L.K. Grover, "Quantum telecomputation", Technical Report 9704012, Archive `http://xxx.lanl.gov/archive/quant-ph`, 1997.

[9] E. Kushilevitz and N. Nisan, *Communication Complexity*, Cambridge University Press, 1997.

[10] N.D. Mermin, "Is the moon there when nobody looks? Reality and the quantum theory", *Physics Today*, Vol. 38, 1985, pp. 38–47.

[11] N.D. Mermin, "What's wrong with these elements of reality?", *Physics Today*, Vol. 43, 1990, pp. 9–11.

[12] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic, 1993.

[13] 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.

Recent BRICS Report Series Publications

RS-97-40 **Harry Buhrman, Richard Cleve, and Wim van Dam.** ***Quantum Entanglement and Communication Complexity.*** **December 1997. 14 pp.**

RS-97-39 **Ian Stark.** ***Names, Equations, Relations: Practical Ways to Reason about 'new'.*** **December 1997. ii+33 pp. This supersedes the earlier BRICS Report RS-96-31. It also expands on the paper presented in Groote and Hindley, editors,** ***Typed Lambda Calculi and Applications: 3rd International Conference*****, TLCA '97 Proceedings, LNCS 1210, 1997, pages 336–353.**

RS-97-38 **Michał Hańćkowiak, Michał Karoński, and Alessandro Panconesi.** ***On the Distributed Complexity of Computing Maximal Matchings.*** **December 1997. 16 pp. To appear in** ***The Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*****, SODA '98.**

RS-97-37 **David A. Grable and Alessandro Panconesi.** ***Fast Distributed Algorithms for Brooks-Vizing Colourings (Extended Abstract).*** **December 1997. 20 pp. To appear in** ***The Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*****, SODA '98.**

RS-97-36 **Thomas Troels Hildebrandt, Prakash Panangaden, and Glynn Winskel.** ***Relational Semantics of Non-Deterministic Dataflow.*** **December 1997. 21 pp.**

RS-97-35 **Gian Luca Cattani, Marcelo P. Fiore, and Glynn Winskel.** ***A Theory of Recursive Domains with Applications to Concurrency.*** **December 1997. ii+23 pp.**

RS-97-34 **Gian Luca Cattani, Ian Stark, and Glynn Winskel.** ***Presheaf Models for the π-Calculus.*** **December 1997. ii+27 pp. Appears in Moggi and Rosolini, editors,** ***Category Theory and Computer Science: 7th International Conference*****, CTCS '97 Proceedings, LNCS 1290, 1997, pages 106–126.**

RS-97-33 **Anders Kock and Gonzalo E. Reyes.** ***A Note on Frame Distributions.*** **December 1997. 15 pp.**

RS-97-32 **Thore Husfeldt and Theis Rauhe.** ***Hardness Results for Dynamic Problems by Extensions of Fredman and Saks' Chronogram Method.*** **November 1997. i+13 pp.**