The cost of exactly simulating quantum entanglement with classical communication

Gilles Brassard [*] *Université de Montréal* [†]

Richard Cleve [‡] *University of Calgary* [§]

Alain Tapp [‡] *Université de Montréal* [†]

15 January 1999

Abstract

We investigate the amount of communication that must augment classical local hidden variable models in order to simulate the behaviour of entangled quantum systems. We consider the scenario where a bipartite measurement is given from a set of possibilities and the goal is to obtain exactly the same correlations that arise when the actual quantum system is measured. We show that, in the case of a single pair of qubits in a Bell state, a constant number of bits of communication is always sufficient—regardless of the number of measurements under consideration. We also show that, in the case of a system of n Bell states, a constant times 2^n bits of communication are necessary.

1 Introduction

Bell's celebrated theorem [1] shows that certain scenarios involving bipartite quantum measurements result in correlations that are impossible to simulate with a classical system if the measurement events are space-like separated. If the measurement events are time-like separated then classical simulation is possible, at the expense of some communication. Our goal is to quantify the required amount of communication.

The issue that we are addressing is part of the broader question of how quantum information affects various resources required to perform tasks in information processing. A two-way classical communication channel between two separated parties can be regarded as a *resource*, and a natural goal is for two parties to produce classical information satisfying a specific stochastic property. One question is, if the parties have an *a priori* supply of quantum entanglement, can they accomplish such goals with less classical communication than necessary in

[*] Supported in part by Canada's NSERC, Québec's FCAR and the Canada Council.

[†] Département IRO, Université de Montréal, C.P. 6128, succursale centre-ville, Montréal (Québec), Canada H3C 3J7. Email: {brassard,tappa}@iro.umontreal.ca.

[‡] Supported in part by Canada's NSERC.

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

the case where their *a priori* information consists of only classical probabilistic information? And, if so, by how much? Our question is, to what extent does the fundamental behaviour of an entangled quantum system itself provide savings, in terms of communication compared with classical systems?

Imagine a scenario involving two "particles" that may have been "together" (and interacted) at some previous point in time, but are "separated" (in a sense which implies that they can no longer interact) at the present time. Suppose that a measurement is then arbitrarily selected and performed on each particle (not necessarily the same measurement on both particles). If the underlying physics governing the behaviour of the system is "classical" then the behaviour of such a system could be based on correlated random variables (usually called "local hidden variables"), reflecting the possible results of a previous interaction. If no communication can occur between the components at the time when the measurements take place then this imposes restrictions on the possible behaviour of such a system. In fact, if the underlying physics governing the behaviour of the system is "quantum" (in the sense that it can be based on entangled quantum states, rather than correlated random variables) then behaviour can occur that is impossible in the classical case. This is a natural way of interpreting Bell's theorem [1, 3]. To formalize—and later generalize—this, we shall define *quantum measurement scenarios* and *(classical) local hidden variable schemes.*

2 Definitions and preliminary results

Define a *quantum measurement scenario* as a triple of the form $(|\Psi\rangle_{AB}, M_A, M_B)$, where $|\Psi\rangle_{AB}$ is a bipartite quantum state, M_A is a set of measurements on the first component, and M_B is a set of measurements on the second component.

It is convenient to parametrize the simplest von Neumann measurements on individual qubits by points on the unit circle (more general von Neumann measurements, which involve complex numbers, are considered later in this paper). Let the parameter $x \in [0, 2\pi)$ denote a measurement with respect to the operator

$$R(x) = \begin{pmatrix} \cos x & \sin x \\ \sin x & -\cos x \end{pmatrix} \tag{1}$$

(whose eigenvectors are $\cos(\frac{x}{2})|0\rangle + \sin(\frac{x}{2})|1\rangle$ and $\sin(\frac{x}{2})|0\rangle - \cos(\frac{x}{2})|1\rangle$).

Consider the case of a pair of qubits in the Bell state $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$. [Our results are written for such states, but can be modified to apply to any of the other Bell states, including the Einstein-Podolsky-Rosen singlet state $|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$.] Let $x, y \in [0, 2\pi)$ be the respective measurement parameters of the two components and let $a, b \in \{0, 1\}$ be the respective outcomes. Then the joint probability distribution of these outcomes is given as:

	$\Pr[b=0]$	$\Pr[b=1]$
$\Pr[a=0]$	$\frac{1}{2}\cos^2(\frac{x-y}{2})$	$\frac{1}{2}\sin^2(\frac{x-y}{2})$
$\Pr[a=1]$	$\frac{1}{2}\sin^2(\frac{x-y}{2})$	$\frac{1}{2}\cos^2(\frac{x-y}{2})$

Two simple but noteworthy examples of bipartite quantum measurement scenarios with the Bell state $|\Phi^+\rangle_{AB}$ are:

Example 1: $(|\Phi^+\rangle_{AB}, M_A, M_B)$, where $M_A = M_B = \{0, \frac{\pi}{2}\}$.

Example 2: $(|\Phi^+\rangle_{AB}, M_A, M_B)$, where $M_A = \{-\frac{\pi}{8}, \frac{3\pi}{8}\}$ and $M_B = -M_A = \{\frac{\pi}{8}, -\frac{3\pi}{8}\}$.

In both examples, each individual outcome is a uniformly distributed bit regardless of the measurements. In Example 1, if the two measurements are the same then the outcomes are completely correlated; whereas, if the two measurements are different, the outcomes are completely independent. In Example 2, the two outcomes are equal with probability $\sin^2(\frac{\pi}{8})$ if $x = -y = +\frac{3\pi}{8}$; and with probability $\cos^2(\frac{\pi}{8})$ otherwise. These examples are interesting in the context of local hidden variable schemes, which are defined next.

Intuitively, we are interested in classical devices that simulate bipartite quantum measurement scenarios to varying degrees, and such devices are naturally explained as local hidden variable schemes. To define a *local hidden variable scheme*, it is convenient to view it as a two-party procedure whose execution occurs in two stages: a *preparation stage* and a *measurement stage*. For ease of reference, call the two parties Alice and Bob. During the preparation stage, *local hidden variables* u for Alice and v for Bob are determined by a classical random process. During this stage, arbitrary communication can occur between the two parties, so u and v may be arbitrarily correlated. During the measurement stage, measurements x and y are given to Alice and Bob (respectively), who produce outcomes $a = A(x, u)$ and $b = B(y, v)$ (respectively). During this stage, no communication is permitted between the parties, which is reflected by the fact that the value of $A(x, u)$ is independent of the value of y (and vice versa).

A local hidden variable scheme *simulates* a measurement scenario $(|\Psi\rangle_{AB}, M_A, M_B)$ if, for any $x \in M_A$ and $y \in M_B$, the outputs produced by Alice and Bob, (namely, a and b respectively), have exactly the same bivariate distribution as the outcomes of the quantum measurement scenario as dictated by the laws of quantum physics.

The measurement scenario in Example 1 is easily simulatable by the following local hidden variable scheme. Let u and v each consist of a copy of the *same* uniformly distributed two-bit string. Then let Alice and Bob each output the first bit of this string if their measurement is 0 and the second bit if their measurement is $\frac{\pi}{2}$. On the other hand, for the measurement scenario of Example 2, it turns out that *there does not exist* a local hidden variable scheme that simulates it [3].

Now, we consider a more powerful classical instrument for simulating measurement scenarios. Define a local hidden variable scheme *augmented by k bits of communication*, as follows. Informally, it is a local hidden variable scheme, except that the prohibition of communication between the parties during the measurement stage is relaxed to a condition that allows up to k bits of communication (but no more). More formally, a local hidden variable scheme augmented by k bits of communication, has a preparation stage where random variables u and v for Alice and Bob are determined and during which arbitrary communication is permitted between the two parties. Then there is a measurement stage which begins by measurements x and y being given to Alice and Bob (respectively). Then one party computes a bit (as a function of his/her measurement and local hidden variables) which is sent to the

other party. This constitutes one *round* of communication. Then again one party (the same one or a different one) computes a bit (as a function of his/her measurement, local hidden variables, and any data communicated from the other party at previous rounds) and sends it to the other party. And this continues for k rounds, after which Alice and Bob output bits a and b (respectively).

For example, for the measurement scenario of Example 2, a local hidden variable scheme augmented with one single bit of communication can simulate it. This is a consequence of the following more general result, whose easy proof we include for completeness.

Theorem 1. *For any quantum measurement scenario $(|\Psi\rangle_{AB}, M_A, M_B)$, there exists a local hidden variable scheme augmented with $\log_2(|M_A|)$ bits of communication (from Alice to Bob) that exactly simulates it.*

Proof. First note that, if we allow $\log_2(|M_A|)$ bits of communication from Alice to Bob *and* $\log_2(|M_B|)$ bits of communication from Bob to Alice then it is trivial to simulate the quantum measurement scenario. With this much communication, Alice can obtain y and Bob can obtain x, which effectively defeats any "nonlocality" in the scenario. More precisely, during the preparation stage, Alice and Bob can construct $|M_A| \cdot |M_B|$ random variable pairs, $(a^{(x,y)}, b^{(x,y)})$, one for each value of $x \in M_A$ and $y \in M_B$. Each such random variable pair would specify the values of the outcomes of Alice and Bob for the given values of x and y, with the appropriate correlation. During the measurement stage, after the communication of x and y between them, Alice and Bob can simply output $a^{(x,y)}$ and $b^{(x,y)}$ (respectively).

To obtain a protocol in which only $\log_2(|M_A|)$ bits of communication from Alice to Bob occurs, note that the unconditional probability distribution of $a^{(x,y)}$ (the output of Alice when the measurements are x and y) is independent of the value of y. This is because the distribution of $a^{(x,y)}$ is completely determined by x and the reduced density matrix of $|\Psi\rangle_{AB}$ with the second component traced out ($\mathrm{Tr}_B(|\Psi\rangle_{AB})$), and this quantity is independent of y. Therefore, the local hidden variables can be set up as follows. For each $x \in M_A$, $a^{(x)}$ is sampled according to the appropriate probability distribution, and then, for each $x \in M_A$ and $y \in M_B$, $b^{(x,y)}$ is sampled according the appropriate conditional probability distribution (conditioned on the value of $a^{(x)}$) in order to produce the correct bivariate distribution for $(a^{(x)}, b^{(x,y)})$. Then, during the measurement stage it suffices for Alice to send x to Bob, and for Alice and Bob to output $a^{(x)}$ and $b^{(x,y)}$ (respectively). ∎

We shall see that in some cases the upper bound of Theorem 1 is asymptotically tight while in other cases it is not. In the sections that follow, we focus on the case of a single Bell state and the case of n Bell states, and provide a new upper or lower bound in each case.

3 The case of a single Bell state

Consider the case of a single Bell state $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$, but where the sizes of M_A and M_B may be arbitrarily large. By Theorem 1, we only obtain an upper bound of $\log_2(|M_A|)$ bits for the amount of communication necessary for an augmented local hidden variable scheme to simulate it. In the case where M_A and M_B are each the entire interval $[0, 2\pi)$, this communication upper bound would be infinite. If only a finite number, k, bits of

communication are permitted then one alternative that might seem reasonable is for Alice to send x', a k-bit approximation of x, to Bob. The protocol for Alice and Bob would be along the lines of the one in Theorem 1, but using x' in place of x. This would clearly not produce an exact simulation for a general $x \in [0, 2\pi)$, but it would produce an *approximation* that improves as k increases. Is this the best that can be done with k bits of communication? The next theorem demonstrates that it is possible to obtain an *exact* simulation for any $x, y \in [0, 2\pi)$ with only a *constant* number of bits of communication.

Theorem 2. *For the quantum measurement scenario* $(|\Phi^+\rangle_{AB}, M_A, M_B)$ *with* $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$ *and* $M_A = M_B = [0, 2\pi)$*, there exists a local hidden variable scheme augmented with four of bits of communication (from Alice to Bob) that exactly simulates it.*

Proof. The local hidden variables are $c \in \{0, 1\}$ and $\theta \in [0, \frac{3\pi}{5})$, and both are uniformly distributed.

For $j \in \{0, 1, \ldots, 9\}$, define $\alpha_j = \frac{j\pi}{5}$. It is useful to view $\alpha_0, \alpha_1, \ldots, \alpha_9$ as ten equally-spaced points on the unit circle. Define the j^{th} *α-slot* as the interval $[\alpha_j, \alpha_{(j+1) \bmod 10})$. Also, define $\beta_0 = \alpha_0 + \theta$, $\beta_1 = \alpha_3 + \theta$, and $\beta_2 = \alpha_6 + \theta$ and $\gamma_0 = \alpha_5 + \theta$, $\gamma_1 = \alpha_8 + \theta$, and $\gamma_2 = \alpha_1 + \theta$ (where the addition is understood to be modulo 2π). Define the j^{th} *β-slot* as the interval $[\beta_j, \beta_{(j+1) \bmod 3})$, and the j^{th} *γ-slot* as the interval $[\gamma_j, \gamma_{(j+1) \bmod 3})$.

The protocol starts by Alice sending Bob information specifying the α-slot, β-slot, and γ-slot in which x is located. Note that these slots partition the unit circle into sixteen intervals, so Alice can convey this information by sending four bits to Bob. Then Alice outputs the bit c.

The full procedure for Bob is summarized below, but, in order to explain the idea behind it, it is helpful to first consider the special case where y is in the 2^{nd} α-slot and the α-slot number of x is within two of that of y (in other words, the α-slot number of x is in $\{0, 1, 2, 3, 4\}$). Note that these conditions depend on the values of x and y only (and not on the values of the local hidden variables). Also, these conditions imply that $|x - y| \leq \frac{3\pi}{5}$. In this case, Bob does the following. If the β-slots of x and y are the same then Bob outputs c. If the β-slots of x and y are different then exactly one β_k is between x and y. Let $u = |y - \beta_k|$. Then Bob's procedure is to output c with probability $1 - \frac{3\pi}{10}\sin(u)$.

To analyse the stochastic behaviour of this procedure (still in the special case), let $r = |x - y|$ and note that the probability of x and y being in different β-slots is $\frac{5r}{3\pi}$. Also, conditional on x and y being in different β-slots, the probability distribution of the position of the β_k between x and y is uniform. Therefore,

$$\begin{aligned} \Pr[a = b] &= \left(1 - \tfrac{5r}{3\pi}\right) + \left(\tfrac{5r}{3\pi}\right)\left(\tfrac{1}{r}\right)\int_0^r \left(1 - \tfrac{3\pi}{10}\sin(u)\right)du \\ &= \tfrac{1}{2}(1 + \cos(r)) \\ &= \cos^2(\tfrac{r}{2}), \end{aligned} \tag{2}$$

which is exactly what is required.

The procedure for Bob in the above special case can be generalized to apply to the other possible cases by considering various similarities and symmetries among the cases. First note that the above procedure actually works in all cases where the α-slot number of y is in $\{2, 3, 4, 5, 6\}$ and the α-slot number of x is within two of that of y. This is because, in these

cases, the interval between x and y (of length $\leq \frac{3\pi}{5}$) lies entirely within the interval $[0, \frac{9\pi}{5})$ and $\beta_0, \beta_1, \beta_2$ are uniformly distributed points spaced $\frac{3\pi}{5}$ apart in this interval.

Now, consider the cases where the α-slot number of y is in $\{7, 8, 9, 0, 1\}$ and the α-slot number of x is still within two of that of y. In these cases, the interval containing x and y may not lie entirely within $[0, \frac{9\pi}{5})$, and so the distribution of $\beta_0, \beta_1, \beta_2$ may no longer satisfy the relevant properties. To avoid this problem, Bob applies the above procedure with $\gamma_0, \gamma_1, \gamma_2$ substituted in place of $\beta_0, \beta_1, \beta_2$. This works because $\gamma_0, \gamma_1, \gamma_2$ are uniformly distributed points spaced $\frac{3\pi}{5}$ apart in the interval $[\pi, \frac{4}{5}\pi)$ (taken *clockwise*) and the interval containing x and y is within this interval.

The above covers all cases where the α-slot number of x is within two of that of y. To handle the remaining cases, Bob works with $y' = y + \pi$ (whose α-slot number will then be within two of that of x) instead of y. Let $r' = |x - y'|$. Then, since $\cos^2(\frac{r'}{2}) = \sin^2(\frac{r}{2})$, Bob will obtain the required distribution if he applies the above procedure but negates his output bit.

In summary, Bob's procedure after obtaining information specifying the α-slot, β-slot, and γ-slot of x from Alice is:

if the difference between the α-slot numbers of x and y is more than two then
    set y **to** $y + \pi$
    set c **to** $\neg c$
if the α-slot number of y is in $\{7, 8, 9, 0, 1\}$ then
    set $\beta_0, \beta_1, \beta_2$ **to** $\gamma_0, \gamma_1, \gamma_2$
if x and y are in the same β-slot then
    output c
else there exists a β_k between x and y
    set u **to** $|y - \beta_k|$
    output c **with probability** $1 - \frac{3\pi}{10}\sin(u)$

∎

Theorem 2 applies to all measurements with respect to operators of the form given in Eq. (1). The most general possible von Neumann measurement on an individual qubit can be parametrized by $(x, x') \in [0, 2\pi) \times [0, 2\pi)$ and taken with respect to the operator

$$S(x, x') = \begin{pmatrix} \cos x & e^{-ix'} \sin x \\ e^{ix'} \sin x & -\cos x \end{pmatrix} \tag{3}$$

(whose eigenvectors are $\cos(\frac{x}{2})|0\rangle + e^{ix'}\sin(\frac{x}{2})|1\rangle$ and $\sin(\frac{x}{2})|0\rangle - e^{ix'}\cos(\frac{x}{2})|1\rangle$). If Alice and Bob make such measurements with respective parameters (x, x') and (y, y') and a and b are the respective outcomes then $\Pr[a = 0] = \Pr[b = 0] = \frac{1}{2}$ and

$$\Pr[a = b] \;=\; \cos^2(\tfrac{x'+y'}{2})\cos^2(\tfrac{x-y}{2}) + \sin^2(\tfrac{x'+y'}{2})\cos^2(\tfrac{x+y}{2}). \tag{4}$$

Theorem 3. *For the quantum measurement scenario $(|\Phi^+\rangle_{AB}, M_A, M_B)$ with $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$ and $M_A = M_B = [0, 2\pi) \times [0, 2\pi)$, there exists a local hidden variable scheme augmented with eight bits of communication (from Alice to Bob) that exactly simulates it.*

Proof. The local hidden variable scheme consists of two executions of the four-bit protocol of Theorem 2. In the first execution, Alice and Bob use measurement parameters x' and $-y'$ to obtain output bits a' and b' (respectively) such that

$$\Pr[a' = b'] = \cos^2(\tfrac{x'+y'}{2}). \tag{5}$$

In the second execution, Alice and Bob use measurement parameters $(-1)^{a'}x$ and $(-1)^{b'}y$ to obtain their final output bits a and b (respectively). Note that

$$\Pr[a = b] = \begin{cases} \cos^2(\frac{x-y}{2}) & \text{if } a' = b' \\ \cos^2(\frac{x+y}{2}) & \text{if } a' \neq b', \end{cases} \tag{6}$$

which, combined with Eq. (5), implies Eq. (4) as required. ∎

We do not know whether a similar result holds in the case of quantum measurements that are more general than von Neumann measurements (e.g. positive operator valued measures).

4 The case of n Bell states

Consider the case of n Bell states, i.e. the tensor product of $|\Phi^+\rangle_{AB}$ with itself n times. This state can be written as $|\Phi^+\rangle_{AB}^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle|i\rangle$. Theorem 3 implies that any n *independent* von Neumann measurements performed on the n Bell states can be simulated by a local hidden variable scheme augmented with $8n$ bits of communication. In the case of *coherent* measurements on such a state, the exact simulation cost can be much larger, as shown by the following theorem.

Theorem 4. *There exists a pair of sets of measurements, M_A and M_B (each of size 2^{2^n}) on n qubits, such that, for the quantum measurement scenario $(|\Phi^+\rangle_{AB}^{\otimes n}, M_A, M_B)$ with $|\Phi^+\rangle_{AB}^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle|i\rangle$, any local hidden variable scheme must be augmented with a constant times 2^n bits of communication in order to exactly simulate it.*

Proof. The proof is based on connections between a measurement scenario and a communication complexity problem examined in [2]. We begin by defining a set of 2^{2^n} measurements, which we call *Deutsch-Jozsa* measurements, due to their connection with the algorithm in [4]. The measurements are parametrized by the set $\{0,1\}^{2^n}$. For a parameter value $z \in \{0,1\}^{2^n}$, we index the bits of z by the set $\{0,1\}^n$. That is, for $i \in \{0,1\}^n$, z_i denotes the "i^{th}" bit of z. The measurement on n qubits corresponding $z \in \{0,1\}^{2^n}$ is easily described as two unitary transformations followed by a measurement in the computational basis. The first unitary transformation is a phase shift that maps $|i\rangle$ to $(-1)^{z_i}|i\rangle$ for each $i \in \{0,1\}^n$. The second unitary transformation is the n-qubit Hadamard transformation, which maps $|i\rangle$ to

$$\tfrac{1}{\sqrt{2^n}} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} |j\rangle, \tag{7}$$

where $i \cdot j$ is the inner product of the two n-bit strings i and j (that is, $i \cdot j = i_0 j_0 + i_1 j_1 + \cdots + i_{n-1} j_{n-1}$). These two unitary transformations are followed by a measurement in the computational basis $\{|i\rangle : i \in \{0,1\}^n\}$, yielding an outcome in $\{0,1\}^n$.

Set $M_A = M_B = \{0,1\}^{2^n}$, the set of Deutsch-Jozsa measurements. We will now show that, for $x \in M_A$ and $y \in M_B$, the joint probability distribution of the outcomes a and b satisfies the following properties:

1. If $x = y$ then $\Pr[a = b] = 1$.

2. If the Hamming distance between x and y is 2^{n-1} then $\Pr[a = b] = 0$.

To show this, consider the quantum state after the phase flips and Hadamard transformations have been performed, but before the measurement. First, applying the phase flips to $|\Phi^+\rangle_{AB}^{\otimes n}$ yields the state

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i + y_i} |i\rangle |i\rangle. \tag{8}$$

Next, after applying the Hadamard transformations, the state becomes

$$\frac{1}{\sqrt{2^{3n}}} \sum_{j,k,i \in \{0,1\}^n} (-1)^{x_i + y_i + i \cdot (j \oplus k)} |j\rangle |k\rangle \tag{9}$$

(where $j \oplus k$ is the bit-wise exclusive-or of j and k). To prove property 1, note that if $x = y$ then state (9) becomes

$$\frac{1}{\sqrt{2^{3n}}} \sum_{j,k,i \in \{0,1\}^n} (-1)^{i \cdot (j \oplus k)} |j\rangle |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle |i\rangle,$$

so $\Pr[a = b] = 1$ when the measurement is performed. To prove property 2, note that if the Hamming distance between x and y is 2^{n-1} then $x_i + y_i$ is even for 2^{n-1} values of i and odd for 2^{n-1} values of i. Therefore, the amplitude of any ket of the form $|j\rangle|j\rangle$ in state (9) is

$$\frac{1}{\sqrt{2^{3n}}} \sum_{i \in \{0,1\}^n} (-1)^{x_i + y_i} = 0, \tag{10}$$

so $\Pr[a = b] = 0$.

Now we reduce a communication complexity problem in [2] to the problem of designing an augmented local hidden scheme that satisfies properties 1 and 2. The communication complexity problem (called EQ' in [2]) is a restricted version of the "equality" problem, and is defined as follows. Alice and Bob get inputs $x, y \in \{0,1\}^{2^n}$ (respectively), and one of them (say, Bob) must output 1 if $x = y$ and 0 if the Hamming distance between x and y is 2^{n-1} (the output of Bob can be arbitrary in all other cases). In [2], it is proven that any classical protocol that exactly solves this restricted equality problem requires $c2^n$ bits of communication for some constant $c > 0$ (the proof is based on a combinatorial result in [5]). Suppose that there exists a local hidden variable scheme augmented with $f(n)$ bits of communication that simulates the measurement scenario $(|\Phi^+\rangle_{AB}^{\otimes n}, M_A, M_B)$. Then one can use this to construct a protocol for restricted equality with $f(n)+n$ bits of communication as follows. Alice and Bob first execute the protocol for $(|\Phi^+\rangle_{AB}^{\otimes n}, M_A, M_B)$ and then Alice sends her output a to Bob, who outputs 1 if $a = b$ and 0 if $a \neq b$. It follows that $f(n) + n \geq c2^n$, so $f(n) \geq c2^n - n \geq c'2^n$, for some $c' > 0$ and sufficiently large n. The theorem extends to all $n \geq 1$, possibly using a smaller constant c'', because it follows from [3] that Example 2 cannot be simulated without communication. ∎

References

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

[2] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation", *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC 98)*, 1998, pp. 63-68.

[3] 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.

[4] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation", *Proceedings of the Royal Society of London*, Series A, Vol. 439, 1992, pp. 553–558.

[5] P. Frankl and V. Rödl, "Forbidden intersections", *Transactions of the American Mathematical Society*, Vol. 300, No. 1, 1987, pp. 259–286.