The cost of exactly simulating a Bell pair using classical communication

János A. Csirik
AT&T Labs–Research
(Dated: March 14, 2002)

The paper [1] begins thus: *"Bell's celebrated theorem [2] shows that certain scenarious involving bipartite quantum measurements result in correlations that are impossible to simulate with a classical system if the measurement events are spacelike separated. If the measurement events are timelike separated, then classical simulation is possible, at the expense of some communication. Our goal is to quantify the required amount of communication."* In this note we tighten the bounds on the amount of communication required to simulate a von Neumann measurement on a Bell pair.

PACS numbers: 03.67.Hk

INTRODUCTION

Consider the following experiment. Let Alice and Bob share one half each of a Bell pair $(|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$. Given $a \in [0, \pi)$, Alice can measure her half with respect to the basis $|0_A\rangle = \cos(a)|0\rangle + \sin(a)|1\rangle$, $|1_A\rangle = -\sin(a)|0\rangle + \cos(a)|1\rangle$. Bob can carry out a similar measurement on his half using $b \in [0, \pi)$ to define the basis $|0_B\rangle$, $|1_B\rangle$. For any choice of a and b as above, the probability that they obtain the same result is $\cos^2(a - b)$.

In the spirit of [1], we investigate the exact number of bits Alice must transmit to Bob in a classical local hidden variable model to be able to produce the same probabilistic correlation. In that paper it is shown that 4 bits suffice. In this note we demonstrate that 3 bits suffice and that at least 2 bits are necessary. The measurements described here all lie on the equator of the Poincaré sphere. Using the method described in [1], *any* von Neumann measurement can be resolved to two of the measurements considered here, and hence can be simulated using only 6 bits of communication.

This problem falls in the general area of *classical entanglement simulation*, which was investigated in [3]. In the terminology of that paper, we are concerned with the *bounded communication model*, in which we insist that the number of bits exchanged be uniformly bounded. The *average communication model*, where the number of bits needs to be bounded on average only, was investigated in [4] and refined in [5]: in that model the local hidden variables can be entirely dispensed with.

The author thanks Peter Shor, Jeff Lagarias, and an anonymous referee for helpful suggestions.

SETUP

By using a classical hidden variable scheme augmented with n bits of (one-way) communication to simulate a Bell pair, we mean

- a probability space Ω;
- for each $a \in [0, \pi)$, and for each $0 \le i \le 2^n - 1$, a random variable $\omega \mapsto m_i^\omega(a)$ on Ω; and
- for each $b \in [0, \pi)$, and for each $0 \le i \le 2^n - 1$, a random variable $\omega \mapsto o_i^\omega(b)$ on Ω.

These data must satisfy the following conditions:

- for any $a, b \in [0, \pi)$, $1 \le i \le 2^n$, and $\omega \in \Omega$, we require $0 \le m_i^\omega(a) \le 1$ and $0 \le o_i^\omega(b) \le 1$;
- for any $a \in [0, \pi)$ and $\omega \in \Omega$, we need $\sum_{i=0}^{2^n-1} m_i^\omega(a) = 1$.

The intended interpretation of this setup is that Alice and Bob have shared access (maybe in the past, before they became separated, or through using some fancy model of physics) to a sample $\omega \in \Omega$. Since Alice can send n bits of information to Bob, she can choose one of 2^n messages to send. In fact, given $a \in [0, \pi)$, she will send the ith message with probability $m_i^\omega(a)$. Given $b \in [0, \pi)$, if Bob receives the ith message from Alice then he will output "Same" with probability $o_i^\omega(b)$, and "Different" otherwise.[1]

[1] The letters m and o were used to denote these functions since they assist in the selection of the message and the output, respectively.

In order then to achieve the output "Same" with probability $\cos^2(a-b)$, regardless of the values of a and b that Alice and Bob are given, we additionally require that

$$\int_\Omega \left(\sum_{i=0}^{2^n-1} m_i^\omega(a) o_i^\omega(b) \right) \mathrm{d}\omega = \cos^2(a-b). \tag{1}$$

REMARK.One might require, as was done in [1], that Alice and Bob actually output 0 or 1 to indicate the result of their measurement. This can be easily incorporated into our framework by adding a random bit z in addition to our Ω, and having Alice output z, with Bob outputting z if he would have output "Same" in the above scenario (and its opposite otherwise).

THE NON-EXISTENCE OF A 1-BIT SCHEME

We prove by *reductio ad absurdum* that there is no solution to the above problem with $n = 1$.

First of all, observe that since $m_0^\omega(a)$ and $m_1^\omega(a)$ are both non-negative and they sum to 1, for any $a, b \in [0, \pi)$ and $\omega \in \Omega$ we have

$$\min(o_0^\omega(b), o_1^\omega(b)) \leq \sum_{i=0}^{1} m_i^\omega(a) o_i^\omega(b) \leq \max(o_0^\omega(b), o_1^\omega(b)).$$

We shall also use the following lemma:

Lemma 1 *Let f be a non-negative valued random variable on a probability space Ω. Then $\int_\Omega f(\omega)\mathrm{d}\omega \leq 0$ implies that $f(\omega) = 0$ on a set of probability 1 (i.e., almost surely).*

PROOF.For any $\varepsilon > 0$, let $A(\varepsilon) = \mathbf{P}(f(\omega) > \varepsilon)$. Since $\int_\Omega f(\omega)\mathrm{d}\omega > \varepsilon A(\varepsilon)$, we conclude that $A(\varepsilon) = 0$. Finally, since the set where f is positive is the union for all integers n of $A(2^{-n})$, we conclude that $f(\omega) = 0$ almost surely.

VARIANT. Using the same method as above, we can show that if $g(\omega) \leq 1$ and $\int_\Omega g(\omega)\mathrm{d}\omega \geq 1$ then almost surely $g(\omega) = 1$.

Now we fix b and set $a = b + \pi/2$. (Here we might need to reduce a modulo π to place it in $[0, \pi)$. We shall do this here, and everywhere else in this note, without further comment.) Then, using the observation before the lemma, we get

$$\int_\Omega \min(o_0^\omega(b), o_1^\omega(b))\mathrm{d}\omega \leq \cos^2(a-b) = 0.$$

Applying the lemma, we obtain that for any $b \in [0, \pi)$, we almost surely (a.s.) have $\min(o_0^\omega(b), o_1^\omega(b)) = 0$.

Similarly (using the variant of the lemma) we can see that for any $b \in [0, \pi)$, we almost surely (a.s.) have $\max(o_0^\omega(b), o_1^\omega(b)) = 1$. Therefore we can define a function $s(b, \cdot) : \Omega \to \{0, 1\}$ which a.s. gives us which of the two indices i results in $o_i^\omega(b) = 1$ for given ω and b. Using the function s to rewrite (1), we obtain

$$\int_\Omega m_{s(b,\omega)}^\omega(a)\mathrm{d}\omega = \cos^2(a-b).$$

Setting $b = a$ and using the variant of our lemma again, we obtain that a.s. $m_{s(a,\omega)}^\omega(a) = 1$. Using the fact that $m_0^\omega(a) + m_1^\omega(a) = 1$, we can conlude that $m_i^\omega(a) = 1$ if and only if $i = s(a, \omega)$.

We can therefore rewrite (1) again to conclude that

$$\mathbf{P}(s(a, \omega) = s(b, \omega)) = \cos^2(a-b),$$

or equivalently

$$\mathbf{P}(s(a, \omega) \neq s(b, \omega)) = \sin^2(a-b). \tag{2}$$

We can use (2) to derive a contradiction as follows. For any set X, the set of functions from Ω to X is endowed with a pseudometric, where the distance between f and g is $\mathbf{P}(f(\omega) \neq g(\omega))$. However, one can check immediately that because of (2), the functions $s(0, \cdot)$, $s(0.01, \cdot)$ and $s(0.02, \cdot)$ do not satisfy the triangle inequality!

THE EXISTENCE OF A 3-BIT SCHEME

We shall now describe a communication protocol using only three bits that carries out our task.

The probability space Ω is chosen to be the interval $[0, \pi/4)$, with a uniform probability distribution.

In this construction, $m_i^\omega(a)$ is always 0 or 1, i.e., Alice chooses her message deterministically when given a and ω. The first bit of her message is 1 if $a \geq \pi/2$ and 0 otherwise. The second bit of her message is 1 if $(a \bmod \pi/2) \geq \pi/4$ and 0 otherwise. The third bit of her message is 1 if $(a \bmod \pi/4) < \omega$ and 0 otherwise.

If the first bit of Alice's message is a 1, Bob sets it to 0 and remembers to flip his final answer from "Same" to "Different" and vice versa. This works since $\cos^2(\alpha) = 1 - \cos^2(\alpha + \pi/2)$ and since the rest of the bits in the message only depend on $a \bmod \pi/2$. Now we just have to specify $o_i^\omega(b)$ for $0 \leq i \leq 3$. (The above argument amount to setting $o_k^\omega(b) = 1 - o_{k+4}^\omega(b)$ for $k \in \{0, 1, 2, 3\}$.)

We first describe Bob's strategy if $0 \leq b < \pi/4$.

Let $o_0^\omega(b)$ be 1 if $b < \omega$ and $1 - \pi \sin(2|\omega - b|)/4$ otherwise. Let $o_1^\omega(b)$ be 1 if $b\omega$ and $1 - \pi \sin(2|\omega - b|)/4$ otherwise. Let $\lambda \in [0, 1]$ be defined by

$$\cos^2(\pi/2 - b) = \lambda(1 - \cos^2(\pi/4 - b) + \cos^2(\pi/2 - b)).$$

Then we can set $o_2^\omega(b) = \lambda(1 - \pi \sin(2|\omega - b|)/4)$ and $o_3^\omega(b) = \lambda + (1 - \lambda) \sin(2|\omega - b|)/4)$. It is then simple to check that this scheme satisfies all the conditions given.

For $\pi/4 \leq b < \pi/2$, it is easy to check that $o_{f(k)}^\omega(b) = o_k^\omega(b - \pi/4)$ works, where f takes $0, 1, 2, 3$ to $2, 3, 4, 5$, again completing the definition by setting $o_k^\omega(b) = 1 - o_{k+4}^\omega(b)$ for $k \in \{0, 1, 2, 3\}$.

Finally, for $\pi/2 \leq b$, we can set $o_k^\omega(b) = 1 - o_k^\omega(b - \pi/2)$ for all k.

THE POSSIBLE EXISTENCE OF A 2-BIT SCHEME

Here we present a result that might be useful in deciding whether a 2-bit scheme exists. Assume now that $m_i^\omega(a)$ is always either 0 or 1 (this is not a serious restriction, as for any scheme without this restriction, we can easily contruct one with probability space $\Omega \times [0, 1]$ that satisfies this restriction). Then we can construct a function $s(a, \cdot) : \Omega \to \{0, 1, \ldots, 2^n - 1\}$ such that $m_{s(a,\omega)}^\omega(a) = 1$. Then we have

Lemma 2 *Given $a, a' \in [0, \pi)$, the distance between the functions $s(a, \cdot)$ and $s(a', \cdot)$ is at least $sin(|a - a'|)$.*

REMARK.Such a result might be useful in concluding that for a certain n, the space of functions $\Omega \to \{0, 1, \ldots, 2^n - 1\}$ is not large enough to contain each of the functions $\{s(a_i, \cdot) : i \in I\}$ for some cleverly chosen set $\{a_i : i \in I\}$.

PROOF.Let Ω_i and Ω'_j denote the parts of Ω where $s(a, \omega) = i$ and $s(a', \omega) = j$, respectively. With this notation, (1) takes the form

$$\sum_{i=0}^{2^n-1} \int_{\Omega_i} o_i^\omega(b) \mathrm{d}\omega = \cos^2(a - b).$$

Applying this to a and a' (with the same b) and taking the difference, we conclude that

$$\cos^2(a - b) - \cos^2(a' - b) \leq \sum_{i=0}^{2^n-1} \int_{\Omega_i \setminus \Omega'_i} o_i^\omega(b) \mathrm{d}\omega.$$

Since $o_i^\omega(b) \leq 1$, we can conclude that

$$\cos^2(a - b) - \cos^2(a' - b) \leq \sum_{i=0}^{2^n-1} \int_{\Omega_i \setminus \Omega'_i} 1 \mathrm{d}\omega = \mathbf{P}(s(a, \omega) \neq s(a', \omega)).$$

Choosing b appropriately, the left hand side of the above inequality is maximized at $\sin(|a - a'|)$. This concludes the proof of our lemma.

---

[1] G. Brassard, R. Cleve, and A. Tapp, Physical Review Letters **83**, 1874 (1999), also available as `quant-ph/9901035`.

[2] J. S. Bell, Physics **1**, 195 (1964).
[3] S. Massar, D. Bacon, N. Cerf, and R. Cleve, Physical Reviews A **63**, Article 052305 (2000), also available as `quant-ph/0009088`.
[4] M. Steiner, in *Proc. of 29th Winter Colloquium on the Physics of Quantum Electronics, Snowbird, Utah, 1999* (1999), also available from `quant-ph/9902014`.
[5] N. Cerf, N. Gisin, and S. Massar, Physical Review Letters **84**, 2521 (2000).