Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial

Gilles Brassard,[1] Harry Buhrman,[2,3] Noah Linden,[4] André Allan Méthot,[1] Alain Tapp,[1] and Falk Unger[3]

[1]*Département IRO, Université de Montréal, C.P. 6128, Succursale Centre-Ville, Montréal, Québec H3C 3J7, Canada*
[2]*ILLC, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands*
[3]*Centrum voor Wiskunde en Informatica (CWI), Post Office Box 94079, 1090 GB Amsterdam, The Netherlands*
[4]*Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom*

(Received 2 March 2006; published 27 June 2006)

Bell proved that quantum entanglement enables two spacelike separated parties to exhibit classically impossible correlations. Even though these correlations are stronger than anything classically achievable, they cannot be harnessed to make instantaneous (faster than light) communication possible. Yet, Popescu and Rohrlich have shown that even stronger correlations can be defined, under which instantaneous communication remains impossible. This raises the question: Why are the correlations achievable by quantum mechanics not maximal among those that preserve causality? We give a partial answer to this question by showing that slightly stronger correlations would result in a world in which communication complexity becomes trivial.

DOI: 10.1103/PhysRevLett.96.250401 PACS numbers: 03.65.Ud, 03.67.Hk, 03.67.Mn

Entanglement can be harnessed to accomplish amazing information processing feats. The first proof that genuinely nonclassical behavior could be produced by quantum-mechanical devices was given by Bell, who proved that entanglement enables two spacelike separated parties to exhibit correlations that are stronger than anything allowed by classical physics [1]. Later, Clauser, Horne, Shimony, and Holt (CHSH), inspired by the work of Bell, proposed another inequality [2], which was easier to translate into a feasible experiment to test local hidden-variable theories. Their proposal fits nicely into the more modern framework of nonlocal boxes, introduced by Popescu and Rohrlich [[3], Eq. (7)].

A *nonlocal box* (NLB) is an imaginary device that has an input-output port at Alice's location and another one at Bob's, even though Alice and Bob can be spacelike separated. Whenever Alice feeds a bit x into her input port, she gets a uniformly distributed random output bit a, locally uncorrelated with anything else, including her own input bit. The same applies to Bob, whose input and output bits we call y and b, respectively. The "magic" appears in the form of a correlation between the pair of outputs and the pair of inputs: the exclusive OR (sum modulo two, denoted "⊕") of the outputs is always equal to the logical AND of the inputs: $a \oplus b = x \wedge y$. Much like the correlations that can be established by use of quantum entanglement, this device is atemporal: Alice gets her output as soon as she feeds in her input, regardless of if and when Bob feeds in *his* input, and vice versa. Also inspired by entanglement, this is a *one-shot* device: the correlation appears only as a result of the first pair of inputs fed in by Alice and Bob. Of course, they can have more than one NLB at their disposal, which is then seen as a *resource* [4] of a different nature than entanglement [5].

NLBs cannot be used by Alice and Bob to signal instantaneously to one another. This is because the outputs that can be observed are purely random from a local perspective. In other words, NLBs are nonlocal, yet they are *causal*: they cannot make an effect precede its cause in the context of special relativity. We are interested in the question of how well the correlation of NLBs can be *approximated* by devices that follow the laws of physics.

Although originally presented differently, the CHSH inequality can be recast in terms of imperfect NLBs. The availability of shared entanglement allows Alice and Bob to approximate NLBs with success probability

$$\wp = \cos^2 \frac{\pi}{8} = \frac{2 + \sqrt{2}}{4} \approx 85.4\%.$$

This can be used to test local hidden-variable theories because it follows also from CHSH that no local realistic (classical) theory can succeed with probability greater than 3/4 if Alice and Bob are spacelike separated. Later, Tsirelson [6] proved the optimality of the CHSH inequality, which translates into saying that quantum mechanics does not allow for a success probability greater than $\wp$ at the game of simulating NLBs. See also Ref. [7] for an information-theoretic proof of the same result.

There are two questions of interest in this Letter: (1) Considering that perfect NLBs would not violate causality, why do the laws of quantum mechanics only allow us to implement NLBs better than anything classically possible, yet not perfectly? (2) Why do they provide us with an approximation of NLBs that succeeds with probability $\wp$ rather than something better?

Before we can pursue this line of thought further, we need to review briefly the field of *communication complexity* [8–11]. Assume Alice and Bob wish to compute some Boolean function $f(x, y)$ of input x, known to Alice only, and input y, known to Bob only. Their concern is to minimize the amount of communication required between them for Alice to learn the answer. It is clear that this task cannot be accomplished without at least *some* communication (even if Alice and Bob share prior entanglement), unless $f(x, y)$ does not actually depend on y, because otherwise instantaneous signalling would be possible. Thus, we say that the communication complexity of f is *trivial* if the problem can be solved with a *single bit* of communication.

It is known that prior entanglement shared between Alice and Bob helps sometimes but not always. Some functions can be computed with exponentially less communication than with a purely classical protocol [12]. However, other functions, such as the *inner product* $\mathrm{IP}(x, y) = \bigoplus_i (x_i \wedge y_i)$, require as many bits to be communicated as the size of the input, whether or not prior entanglement is available [13]. Surprisingly, van Dam [14], and independently Cleve [15], proved that the availability of perfect NLBs makes the communication complexity of *all* Boolean functions trivial. This answers the first question above: If we take as an axiom that communication complexity should not be trivial, it had to be impossible for quantum mechanics to provide a perfect implementation of NLBs. Indeed, most computer scientists would consider a world in which communication complexity is trivial to be as surprising as a modern physicist would find the violation of causality.

In order to answer the second question, we turn our attention to the *probabilistic* version of communication complexity, in which we do not require Alice to learn the value of $f(x, y)$ with certainty. Instead, we shall be satisfied if she can obtain an answer that is correct with probability bounded away from $1/2$. In other words, there must exist some real number $p > 1/2$ such that the probability that Alice guesses the correct value of $f(x, y)$ is at least p for *all* pairs (x, y) of inputs. The probability is taken over possible probabilistic behavior by Alice and Bob, as well as over the value of random variables shared between them.

When we extend the notion of "trivial" communication complexity to fit this probabilistic framework, the inner product remains nontrivial according to quantum mechanics: Alice and Bob cannot succeed with probability $p > 1/2$ if they transmit less than $\max(\frac{1}{2}(2p - 1)^2, (2p - 1)^4)n - \frac{1}{2}$ bits, even if they share prior entanglement [13].

Our main theorem, stated below and proved in the rest of the Letter, shows that the availability of NLBs, *even imperfect*, would dramatically change this picture.

Theorem 1.—In any world in which it is possible, without communication, to implement an approximation to the NLB that works correctly with probability greater than $\frac{3+\sqrt{6}}{6} \approx 90.8\%$, every Boolean function has trivial probabilistic communication complexity.

To prove this theorem, we introduce the notion of *distributed computation* and the notion of *bias* for such computations. Then, we show how to amplify the natural bias of *any* Boolean function by having Alice and Bob calculate it many times and taking the majority. We determine how imperfect a majority gate can be and still increase the bias. Finally, we construct a majority gate with the use of NLBs, and we determine to what extent we can allow *them* to be faulty.

Definition 1. A bit c is *distributed* if Alice has bit a and Bob bit b such that $c = a \oplus b$.

Definition 2. A Boolean function f is *distributively computed* by Alice and Bob if, given inputs x and y, they can produce a distributed bit equal to $f(x, y)$.

Definition 3. A Boolean function is *biased* if it can be distributively computed without any communication and with probability strictly greater than $1/2$.

Lemma 1.—Provided Alice and Bob are allowed to share random variables, *all* Boolean functions are biased.

Proof.—Let f be an arbitrary Boolean function and let Alice and Bob share a uniformly distributed random variable z of the same size n as Bob's input y. Upon receiving her input x, Alice produces $a = f(x, z)$. Bob's strategy is to test if $y = z$. If so, he produces $b = 0$; if not, he produces a uniformly distributed random bit b. In the lucky event that $y = z$, the bit distributed between Alice and Bob is correct since $a \oplus b = f(x, z) \oplus 0 = f(x, y)$. In all other cases, the distributed bit $a \oplus b$ is uniformly random. Summing up, the distributed bit is correct with probability $\frac{1}{2^n} + (1 - \frac{1}{2^n})\frac{1}{2} = \frac{1}{2} + \frac{1}{2^{n+1}} > 1/2$. □

Definition 4. A Boolean function has *bounded bias* if it can be distributively computed without any communication and with probability bounded away from $1/2$.

Remark 1.—The difference between bias and *bounded* bias is that the probability of being correct in the former case can come arbitrarily close to $1/2$ as the input size increases. In the latter case, there must be some fixed $p > 1/2$ such that the probability of being correct is at least p no matter how large the inputs are.

Lemma 2.—Any Boolean function that has bounded bias has trivial probabilistic communication complexity.

Proof.—Assume Boolean function f has bounded bias. For all inputs x and y, Alice and Bob can produce bits a and b, respectively, without communication, such that $a \oplus b = f(x, y)$ with probability at least $p > 1/2$. If Bob transmits his single bit b to Alice, she can compute $a \oplus b$, which is correct with bounded error probability. □

Definition 5. The *nonlocal majority* problem consists in computing the distributed majority of three distributed bits. More precisely, let Alice have bits x_1, x_2, x_3 and Bob have y_1, y_2, y_3. The purpose is for Alice and Bob to compute a and b, respectively, such that

$$a \oplus b = \mathrm{Maj}(x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3),$$

where $\mathrm{Maj}(u, v, w)$ denotes the bit occurring the most among u, v, and w. The computation must be achieved without any communication between Alice and Bob.

In 1956, von Neumann proved a statement rather similar to Lemma 3 below, albeit not in the context of distributed computation [16]. We sketch the proof nevertheless for the sake of completeness.

Lemma 3.—For any q such that $5/6 < q \leq 1$, if Alice and Bob can compute nonlocal majority with probability at least q, every Boolean function has bounded bias.

Proof.—Let f be an arbitrary Boolean function, fix Bob's input size, and consider any $p > 1/2$ so that Alice and Bob can distributively compute f with probability at least p. We know from Lemma 1 that such a p exists (although it can depend on the input size). Let Alice and Bob apply their distributed computational process three times, with independent random choices and shared random variables each time. This produces three distributed bits such that each of them is correct with probability at least p. Now, let Alice and Bob compute the nonlocal majority of these three outcomes with correctness probability at least q, which we assumed they can do. Because the overall result will be correct either if most of the distributed outcomes were correct and the distributed majority calculation was performed correctly, or if most of the distributed outcomes were wrong and the distributed majority calculation was performed incorrectly, the probability that the distributed majority as computed yields the correct value of f is at least

$$h(p) = q(p^3 + 3p^2(1-p)) + (1-q)(3p(1-p)^2 + (1-p)^3).$$

Define

$$\delta = q - 5/6 > 0 \quad \text{and} \quad s = \frac{1}{2} + \frac{3\sqrt{\delta}}{2\sqrt{1+3\delta}} > \frac{1}{2}.$$

It can be shown that $p < h(p) < s$ provided $1/2 < p < s$. Because of this and the fact that $h(p)$ is continuous over the entire range $1/2 < p < s$, iteration of the above process can boost the probability of distributively computing the correct answer arbitrarily close to s. This proves that f has bounded bias because, given any fixed value of $q > 5/6$, we can choose an arbitrary constant $t < s$ such that $t > 1/2$ and distributively compute f with probability at least t, independently of the input size. □

Definition 6. The *nonlocal equality* problem consists in distributively deciding if three distributed bits are equal. More precisely, let Alice have bits x_1, x_2, x_3 and Bob have y_1, y_2, y_3. The purpose is for Alice and Bob to compute a and b, respectively, such that

$$a \oplus b = \begin{cases} 1 & \text{if } x_1 \oplus y_1 = x_2 \oplus y_2 = x_3 \oplus y_3 \\ 0 & \text{otherwise.} \end{cases}$$

The computation of a and b must be achieved without any communication between Alice and Bob.

Lemma 4.—Nonlocal equality can be computed using only two (perfect) nonlocal boxes.

Proof.—The goal is to obtain a and b such that:

$$a \oplus b = (x_1 \oplus y_1 = x_2 \oplus y_2) \wedge (x_2 \oplus y_2 = x_3 \oplus y_3). \quad (1)$$

First, Alice and Bob compute locally $x' = \overline{x_1} \oplus x_2$, $y' = y_1 \oplus y_2$, $x'' = \overline{x_2} \oplus x_3$ and $y'' = y_2 \oplus y_3$. Then (1) becomes equivalent to $(x' \oplus y') \wedge (x'' \oplus y'') = a \oplus b$. Hence, it is sufficient to show how Alice and Bob can compute the AND of the distributed bits $x' \oplus y'$ and $x'' \oplus y''$.

By distributivity of the AND over the exclusive OR,

$$(x' \oplus y') \wedge (x'' \oplus y'') = (x' \wedge x'') \oplus (x' \wedge y'') \oplus (x'' \wedge y') \oplus (y' \wedge y'').$$

Using two nonlocal boxes, Alice and Bob can compute distributed bits $a' \oplus b'$ and $a'' \oplus b''$ with $a' \oplus b' = x' \wedge y''$ and $a'' \oplus b'' = x'' \wedge y'$. Setting $a = (x' \wedge x'') \oplus a' \oplus a''$ and $b = (y' \wedge y'') \oplus b' \oplus b''$ yields (1), as desired. □

Lemma 5.—Nonlocal majority can be computed using only two (perfect) nonlocal boxes.

Proof.—Let x_1, x_2, x_3 be Alice's input and y_1, y_2, y_3 be Bob's. For $i \in \{1, 2, 3\}$, let $z_i = x_i \oplus y_i$ be the ith distributed input bit. By virtue of Lemma 4, Alice and Bob use their two NLBs to compute the nonlocal equality of their inputs, yielding a and b so that $a \oplus b = 1$ if and only if z_1, z_2, and z_3 are equal. Finally, Alice produces $a' = \overline{a} \oplus x_1 \oplus x_2 \oplus x_3$ and Bob produces $b' = b \oplus y_1 \oplus y_2 \oplus y_3$. Let

$$z = a' \oplus b' = (\overline{a} \oplus b) \oplus (z_1 \oplus z_2 \oplus z_3)$$

be the distributed bit computed by this protocol. Four cases need to be considered, depending on the number ℓ of 1's among the z_i's: (1) if $\ell = 0$, then $a \oplus b = 1$ and $z_1 \oplus z_2 \oplus z_3 = 0$; (2) if $\ell = 1$, then $a \oplus b = 0$ and $z_1 \oplus z_2 \oplus z_3 = 1$; (3) if $\ell = 2$, then $a \oplus b = 0$ and $z_1 \oplus z_2 \oplus z_3 = 0$; (4) if $\ell = 3$, then $a \oplus b = 1$ and $z_1 \oplus z_2 \oplus z_3 = 1$.

We see that $z = 0$ in the first two cases and $z = 1$ in the last two, so that $z = \text{Maj}(z_1, z_2, z_3)$ in all cases. □

We are now ready to prove our main theorem.

Proof of Theorem 1.—Assume NLBs can be approximated with some probability p of yielding the correct result. Using them, we can compute nonlocal majority with probability $q = p^2 + (1-p)^2$ since the protocol given in the proof of Lemma 5 succeeds precisely if none or both of the NLBs behave incorrectly. The result follows from Lemmas 2 and 3 because $q > 5/6$ whenever $p > \frac{3+\sqrt{6}}{6}$. □

Corollary 1.—In any world in which probabilistic communication complexity is nontrivial, nonlocal boxes cannot be implemented without communication, even if we are satisfied in obtaining the correct behavior with probability $\frac{3+\sqrt{6}}{6} \approx 90.8\%$.

Remark 2.—Neither nonlocal majority nor nonlocal equality can be solved exactly with a single nonlocal box. Otherwise, entanglement could approximate that NLB well enough to solve the nonlocal majority problem with probability $\wp \approx 0.854 > 5/6$ of being correct [2]. It would follow from Lemmas 2 and 3 that all Boolean functions have trivial probabilistic communication complexity according to quantum mechanics. But we know this not to be the case for the inner product [13].

Remark 3.—Our results also give bounds on the maximum admissible error for purely classical fault-tolerant computation. Suppose that we could transform any classical circuit into a fault-tolerant version that would work with probability bounded away from $1/2$ even if each gate failed independently with probability $1/4$. Assume furthermore that the fault-tolerant circuit is composed only of unary and binary gates, henceforth called a UB-*gate circuit*. In the proof of Lemma 4, we showed how to simulate *distributed* AND gates by use of two NLBs. Similarly, it is easy to see that all other UB gates can be computed distributively with at most two NLBs. (Several gates require no NLBs at all, such as the unary NOT and binary XOR, also known as CNOT, the controlled NOT gate.) Now, quantum mechanics provides us with NLBs with correctness probability $\wp$, which yields distributed gates that are correct with probability at least $(1-\wp)^2 + \wp^2 = 3/4$. This allows us to use the assumed fault-tolerant circuit in a distributed way and conclude that all Boolean functions have bounded bias, and therefore trivial quantum probabilistic communication complexity. But this is impossible since most Boolean functions, for example, the inner product, require $\Omega(n)$ bits of communication even if Alice and Bob share entanglement and are satisfied with a probability of correct answer bounded away from $1/2$ [13]. It follows that UB-gate fault-tolerant circuits cannot in general allow each gate to fail with probability $1/4$, even if NOT and XOR gates are perfect. As an interesting coincidence, the best known upper bound on the error threshold, due to Evans and Pippenger [17], states that fault tolerance is impossible in general for UB-gate circuits if gates fail with probability $1-\wp = \frac{2-\sqrt{2}}{4}$ or worse.

In conclusion, we have shown that in any world in which communication complexity is nontrivial, there is a bound on how much nature can be nonlocal. This bound, which is an improvement over previous knowledge that nonlocal boxes could not be implemented exactly [14,15], approaches the actual bound $\wp \approx 85.4\%$ imposed by quantum mechanics. The obvious open question is to close the gap between these probabilities. A proof that nontrivial communication complexity forbids nonlocal boxes to be approximated with probability greater than $\wp$ would be very interesting, as it would render Tsirelson's bound [6] inevitable, making it a candidate for a new information-theoretic axiom for quantum mechanics [18].

The authors are grateful to Richard Cleve and Ben Toner for stimulating discussions. H. B., N. L., and F. U. thank the Newton Institute where part of this work was done. G. B. is supported by Canada's NSERC, CIAR, and the Canada Research Chair Programme. H. B., N. L., and F. U. are supported by the EU under projects RESQ and QAP. H. B. and F. U. are supported also by the NWO vici project 2004-2009. N. L. is supported also by the UK EPSRC's IRC in QIP. A. T. is supported by NSERC, CIAR, MITACS, and Québec's FQRNT.

[1] J. S. Bell, Physics **1**, 195 (1964).

[2] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[3] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).

[4] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).

[5] A. Broadbent and A. A. Méthot, "On the Power of Non-Local Boxes," Theor. Comput. Sci. (to be published).

[6] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).

[7] H. Buhrman and S. Massar, "Causality and Cirel'son bounds," http://arxiv.org/quant-ph/0409066 (2004).

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

[9] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[10] R. de Wolf, Theor. Comput. Sci. **287**, 337 (2002).

[11] G. Brassard, Found. Phys. **33**, 1593 (2003).

[12] H. Buhrman, R. Cleve, and A. Wigderson, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1988), p. 63.

[13] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, in *Quantum Computing and Quantum Communication, Proceedings of First NASA International Conference, Palm Springs, California, 1998* Lecture Notes in Computer Science, Vol. 1509 (Springer-Verlag, Heidelberg, 1999), p. 61.

[14] W. van Dam, Ph.D. thesis, University of Oxford (2000), Chap. 9; see also http://arxiv.org/quant-ph/0501159.

[15] R. Cleve (personal communication).

[16] J. von Neumann, in *Automata Studies*, edited by C. E. Shannon and J. McCarthy (Princeton University Press, Princeton, NJ, 1956), pp. 43–98.

[17] W. Evans and N. Pippenger, IEEE Trans. Inf. Theory **44**, 1299 (1998).

[18] G. Brassard, Nature Phys. **1**, 2 (2005).