Quantum Nonlocality and Beyond: Limits from Nonlocal Computation

Noah Linden,[1] Sandu Popescu,[2,3] Anthony J. Short,[2] and Andreas Winter[1]

[1]*Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, United Kingdom*
[2]*H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom*
[3]*Hewlett-Packard Laboratories, Stoke Gifford, Bristol BS12 6QZ, United Kingdom*

(Received 8 June 2007; published 30 October 2007)

We address the problem of ''nonlocal computation,'' in which separated parties must compute a function without any individual learning anything about the inputs. Surprisingly, entanglement provides no benefit over local classical strategies for such tasks, yet stronger nonlocal correlations allow perfect success. This provides intriguing insights into the limits of quantum information processing, the nature of quantum nonlocality, and the differences between quantum and stronger-than-quantum nonlocal correlations.

DOI: 10.1103/PhysRevLett.99.180502 PACS numbers: 03.67.−a, 03.65.Ud

Nonlocality is a fundamental aspect of quantum mechanics [1]. However, relativity allows stronger-than-quantum mechanical correlations [2]. What characterizes the nature of quantum nonlocality? To address this question, we define a very natural nonlocal task, namely, ''nonlocal computation,'' in which separated parties must compute a function without any individual learning anything about the inputs. This task is very close to others for which quantum nonlocality is known to be of benefit [3,4]. However, surprisingly, quantum mechanics provides no advantage over classical mechanics for nonlocal computation. Indeed, neither quantum nor classical mechanics can do better than a trivial linear approximation. On the other hand, nonlocal correlations stronger than quantum [2,5–9] allow perfect nonlocal computation. Our results provide intriguing connections between computation and nonlocality and new insights into the nature and limits of quantum nonlocality.

Following earlier work [5] in which the problems of ''nonlocal equality'' and ''nonlocal majority'' were introduced, we define here the ''nonlocal computation'' of a general boolean function by two parties. At the end of the Letter, we generalize the situation to more parties and to more general nonlocal tasks.

The ordinary computation of a boolean function f takes as input a string of n bits $z = z_1 z_2, \ldots, z_n$, and gives as output a single bit c such that

$$c = f(z) = f(z_1, z_2, \ldots, z_n). \tag{1}$$

To each ordinary computation we now associate a nonlocal version. The idea is for two parties, Alice and Bob, to compute the function in a collaborative way, but without communicating with each other during the computation, and without learning anything individually about the input bits z. Note the distinction between this and distributed computation. In the latter, some input bits are given to Alice and the rest to Bob, and hence each party learns something about the global input. Furthermore, we allow no communication, rather than evaluating the minimum amount required (the communication-complexity), such as in the quantum advantage of [4].

Alice and Bob know in advance what function they have to compute and may arrange a common strategy, but they are separated before being given their inputs. For each input bit z_i, Alice is given a bit x_i and Bob a bit y_i, such that their XOR is equal to z_i ($z_i = x_i \oplus y_i$). However, individually x_i and y_i are totally random, being with equal probability 0 or 1. Since Alice and Bob are not allowed to communicate, they therefore learn nothing about the input z_i. To successfully perform the nonlocal computation, Alice must produce an output bit a and Bob an output bit b, such that $c = a \oplus b$, i.e.,

$$a \oplus b = f(x \oplus y) = f(x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n), \tag{2}$$

with the shorthand $x = x_1 x_2, \ldots, x_n$ and $y = y_1 y_2, \ldots, y_n$ for Alice's and Bob's input bit strings. The task we consider is for Alice and Bob to maximize the probability of success of their nonlocal computation, given either (a) classical resources, (b) quantum resources, or (c) stronger-than-quantum nonlocal resources.

We allow the inputs z to be given by an arbitrary probability distribution $\tilde{p}(z)$. However, as mentioned above, in order to prevent Alice and Bob learning something about z, it is necessary to take all inputs x and y satisfying $z = x \oplus y$ with equal probability, i.e.,

$$p(x, y|z) = \begin{cases} \frac{1}{2^n} & \text{if } x \oplus y = z \\ 0 & \text{otherwise} \end{cases}. \tag{3}$$

The average success probability P for Alice and Bob to satisfy Eq. (2) is therefore given in terms of the success probability for particular inputs, $P_{x,y}$, by

$$P = \sum_{x,y,z} \tilde{p}(z) p(x, y|z) P_{x,y} = \frac{1}{2^n} \sum_{x,y} \tilde{p}(x \oplus y) P_{x,y}. \tag{4}$$

Nonlocal computation with quantum resources.— Consider the nonlocal computation of a function f, given quantum resources. In the most general quantum protocol,

Alice and Bob share an entangled quantum state $|\psi\rangle$ and perform projective measurements on their subsystem dependant on their inputs, given by Hermitian operators $\hat{a}_x$ and $\hat{b}_y$ respectively, with eigenvalues 0 and 1. They then output their measurement results. Note that protocols involving initially mixed states or generalized measurements (involving ancillas) can all be represented in this form by expanding the dimensionality of the initial state. The success probability $P_{x,y}$ is the expectation value of the projector onto the eigenstates of $\hat{a}_x$ and $\hat{b}_y$ whose eigenvalues satisfy (2), which can be expressed as

$$P_{x,y} = \langle\psi|\left(\frac{1 + (-1)^{f(x\oplus y)+\hat{a}_x+\hat{b}_y}}{2}\right)|\psi\rangle. \quad (5)$$

Hence, using (4), the total probability of success is

$$P_Q = \frac{1}{2} + \frac{1}{2^{n+1}}\sum_{xy}\tilde{p}(x\oplus y)\langle\psi|(-1)^{f(x\oplus y)+\hat{a}_x+\hat{b}_y}|\psi\rangle. \quad (6)$$

Extending the Hilbert space from $\mathcal{H}$ to $\mathcal{H}\otimes\mathbb{C}^{2^n}$, we define normalized states $|\alpha\rangle$ and $|\beta\rangle$ and a Hermitian operator $\hat{\Phi}$ as follows (Note that this is to aid in the analysis, and does not correspond to any physical change)

$$|\alpha\rangle = \frac{1}{\sqrt{2^n}}\sum_x (-1)^{\hat{a}_x}\otimes\mathbb{1}|\psi\rangle\otimes|x\rangle, \quad (7)$$

$$|\beta\rangle = \frac{1}{\sqrt{2^n}}\sum_y (-1)^{\hat{b}_y}\otimes\mathbb{1}|\psi\rangle\otimes|y\rangle, \quad (8)$$

$$\hat{\Phi} = \sum_{xy}(-1)^{f(x\oplus y)}\tilde{p}(x\oplus y)|x\rangle\langle y|, \quad (9)$$

where $|x\rangle$ and $|y\rangle$ are computational basis states in $\mathbb{C}^{2^n}$. Equation (6) can then be reexpressed in the simple form

$$P_Q(f) = \frac{1}{2}(1 + \langle\alpha|\mathbb{1}\otimes\hat{\Phi}|\beta\rangle), \quad (10)$$

from which it follows that

$$P_Q(f) \le \frac{1}{2}(1 + |\langle\alpha||\,\|\,\mathbb{1}\otimes\hat{\Phi}\,\|\,||\beta\rangle|) = \frac{1}{2}(1+\|\,\hat{\Phi}\,\|), \quad (11)$$

where $\|\,\hat{\Phi}\,\|$ is the operator norm of $\hat{\Phi}$ (the largest modulus eigenvalue).

To investigate the eigenstates and eigenvalues of $\hat{\Phi}$, we first rewrite it in the Fourier-transform basis

$$|\tilde{u}\rangle = \frac{1}{\sqrt{2^n}}\sum_x (-1)^{u\cdot x}|x\rangle \quad (12)$$

where $u\cdot x$ is the inner product modulo 2 of the bit strings u and x, $u\cdot x = u_1x_1\oplus u_2x_2\oplus\ldots\oplus u_nx_n$. This gives

$$\begin{aligned}\hat{\Phi} &= \left(\sum_u|\tilde{u}\rangle\langle\tilde{u}|\right)\hat{\Phi}\left(\sum_v|\tilde{v}\rangle\langle\tilde{v}|\right)\\ &= \frac{1}{2^n}\sum_{uvxy}(-1)^{f(x\oplus y)+u\cdot x+v\cdot y}\tilde{p}(x\oplus y)|\tilde{u}\rangle\langle\tilde{v}|\\ &= \frac{1}{2^n}\sum_{uvyz}[(-1)^{f(z)+u\cdot z}\tilde{p}(z)][(-1)^{(u+v)\cdot y}]|\tilde{u}\rangle\langle\tilde{v}|\\ &= \sum_u\left(\sum_z(-1)^{f(z)+u\cdot z}\tilde{p}(z)\right)|\tilde{u}\rangle\langle\tilde{u}|, \end{aligned} \quad (13)$$

where in the second line we have replaced the sum over x by one over $z = x\oplus y$. The eigenstates of $\hat{\Phi}$ are therefore $|\tilde{u}\rangle$, and inserting the modulus of the largest eigenvalue in (11), we obtain the quantum bound

$$P_Q(f) \le \frac{1}{2}\left(1 + \max_u\left|\sum_z(-1)^{f(z)+u\cdot z}\tilde{p}(z)\right|\right). \quad (14)$$

Nonlocal computation with classical resources.—We now consider the optimal classical strategy for the nonlocal computation of f. Obviously, this is a problem that can be addressed without any reference to quantum theory. However, as quantum theory includes all classical strategies as special cases, the quantum bound (14) is also a bound on the classical probability. We might expect, however, that the best quantum strategy would perform better than the best classical one. We show now that this is not the case, by explicitly giving a classical strategy that achieves the quantum bound.

The probability of success for a (deterministic) classical strategy is given by

$$P_C = \frac{1}{2} + \frac{1}{2^{n+1}}\sum_{xy}\tilde{p}(x\oplus y)(-1)^{f(x\oplus y)+a_x+b_y} \quad (15)$$

where a_x and b_y are the outputs of Alice and Bob for the given input strings x and y. (Note that this can be obtained from the quantum probability (6) by replacing the operators $\hat{a}_x$ and $\hat{b}_y$ by the numbers a_x and b_y.)

Let us now consider the particular classical strategy (parameterized by an n-bit string u, and a single -bit δ)

$$a_x = u\cdot x, \qquad b_y = u\cdot y\oplus\delta. \quad (16)$$

Inserting these a_x and b_y in (15), we obtain

$$P_C = \frac{1}{2}\left(1 + (-1)^{\delta}\sum_z(-1)^{f(z)+u\cdot z}\tilde{p}(z)\right). \quad (17)$$

Choosing δ to equal the sign of the summation, and maximizing over different choices of u, we achieve a classical success probability equal to the bound obtained in (14). It follows that this strategy is optimal and no other classical or quantum strategy can do better. Hence, we have proven that quantum physics provides no advantage over classical physics for the nonlocal computation of f.

Moreover, the optimal strategy actually produces the output $c = u \cdot z \oplus \delta$ (since $c = a_x \oplus b_y$); hence, all that is achieved is the optimal linear approximation of f. Since nonlinearity is essential for universal computation, we could say that nonlocal computation is impossible in both classical and quantum theory.

Nonlocal computation using stronger-than-quantum nonlocal correlations.—In [2], Popescu and Rohrlich discovered the existence of nonlocal correlations that are consistent with relativity (i.e., that do not allow signalling), yet which are not achievable within quantum theory. A great deal of research has been undertaken recently into such stronger-than-quantum nonlocal correlations [5–9], with the aim of better characterizing the differences between them and quantum correlations, and hence better understanding the nature and limits of quantum nonlocality. Here, we consider the power of stronger-than-quantum nonlocal correlations for nonlocal computation.

The first question we address is: Do there exist stronger-than-quantum nonlocal correlations that allow nonlocal computation beyond the linear approximation (i.e., quantum) limit? To investigate this, we allow Alice and Bob access to an extended black box, for which the inputs (x and y) and outputs (a and b) can be related by any nonsignalling probability distribution $P(a, b|x, y)$ [10]. In fact, with such correlations, we can solve any nonlocal problem with perfect success, simply by setting

$$P(a, b|x, y) = \begin{cases} \frac{1}{2} & \text{if } a \oplus b = f(x \oplus y) \\ 0 & \text{otherwise} \end{cases}. \quad (18)$$

This probability distribution gives both possible sets of outputs fulfilling (2) with equal probability (e.g., $a = 0b = 0[50\%]a = 1, \quad b = 1[50\%]$ when $f(x \oplus y) = 0$). Each party individually obtains a random bit and learns nothing about the other party's input, so the distribution is nonsignalling. Furthermore, as the outputs generated satisfy (2) perfectly, we obtain the maximal success probability $P_S^{\max}(f) = 1$ (where here the index S stands for "stronger-than-quantum correlations"). In fact, each nonlocal computation that goes beyond the linear approximation limit and yields maximally random outputs for Alice and Bob (individually) is by itself a stronger-than-quantum nonlocal correlation.

Having established that some stronger-than-quantum nonlocal correlations help in nonlocal computation, we now come to the crucial question: Do *all* stronger-than-quantum nonlocal correlations help in (at least some) nonlocal computation? In general, this remains an open and intriguing question. However, the following section indicates that perhaps this is the case.

Nonlocal computation of AND using PR-boxes.—The simplest and most fundamental stronger-than-quantum nonlocal correlation has a 1 bit input and 1 bit output for each party and is, in that context, a "maximally nonlocal" correlation [2,6,7]. It is

$$P_{\mathrm{PR}}(a, b|x, y) = \begin{cases} \frac{1}{2} & \text{if } a \oplus b = xy \\ 0 & \text{otherwise} \end{cases} \quad (19)$$

where x, y, a, and b are single bits. Although similar to the distribution given by (18), note that this correlation does not correspond to a nonlocal computation problem because its governing equation $a \oplus b = xy$ is not of the form $a \oplus b = f(x \oplus y)$. Fictitious devices yielding such correlations have become known as PR-boxes [2].

Similarly, the AND function (AND$(z_1, z_2) = z_1 z_2$) represents the simplest case in which nonlocal computation is not trivial. In order to implement this gate nonlocally, Alice and Bob's outputs must obey [5]

$$a \oplus b = (x_1 \oplus y_1)(x_2 \oplus y_2). \quad (20)$$

When the different values of the input bits z_1 and z_2 are given with uniform probability ($\tilde{p}(z) = \frac{1}{4}$), it follows from (14) that the maximal success probabilities obey

$$P_C^{\max}(\mathrm{AND}) = P_Q^{\max}(\mathrm{AND}) = \frac{3}{4} < P_S^{\max}(\mathrm{AND}) = 1.$$

A strategy that achieves the classical or quantum bound is for Alice and Bob to give the output zero in all cases [$u = \delta = 0$ in (16)], which only fails when $z_1 = z_2 = 1$.

It is possible to compute nonlocal-AND perfectly using two PR-boxes (to generate the $x_1 y_2$ and $x_2 y_1$ terms) and local operations (to generate the $x_1 x_2$ and $y_1 y_2$ terms). In fact, because PR-boxes allow a perfect implementation of nonlocal-AND and it is easy to implement nonlocal-NOT using only local operations (e.g., $a = x$, $b = y \oplus 1$), we can build any nonlocal computation perfectly using only PR-boxes and local operations. This also follows straightforwardly from van Dam's result [8] that any distributed computation can be performed perfectly using PR-boxes and 1 bit of communication.

Now suppose we consider noisy PR-boxes, i.e., PR-boxes that give a correct result with probability q and an incorrect result with probability $1 - q$. Implementing the same scheme as before with two noisy PR-boxes, the success probability is given by $P_G = q^2 + (1 - q)^2$, which will be greater than $3/4$ (the classical and quantum bound) whenever $q > (2 + \sqrt{2})/4$. Tantalizingly, $q = (2 + \sqrt{2})/4$ is the maximal value of success probability for PR-boxes constructed via quantum-mechanical means [this is equivalent to the Tsirelson [11] bound for the standard Clauser-Horne-Shimony-Holt (CHSH) [3] inequality]. Hence noisy PR-boxes help for computing nonlocal-AND if and only if they are better than quantum mechanical.

Discussion.—We have shown that quantum nonlocality gives no advantage over classical resources for nonlocal computation, and indeed both can only do as well as simple linear approximations. However, generalized nonlocal correlations can allow perfect success in such tasks. For any nonlinear function f, we therefore find that

$$P_C^{\max}(f) = P_Q^{\max}(f) < P_S^{\max}(f) = 1. \quad (21)$$

This is the main result of the Letter and gives an intriguing insight into the nature of quantum nonlocality. We now consider several extensions and open questions.

Note that in the definition of success probability above, we assumed a fixed prior distribution $\tilde{p}$. One could equally well ask for the maximum success probability *in the worst case* (i.e., when each strategy is evaluated using its worst z). Fortunately, the minimax theorem of game theory [12] tells us that in the classical case, when Alice and Bob can use shared randomness, the optimal worst-case success probability is equal to the maximal success probability ($P_C^{\max}$) for some particular prior distribution $\tilde{p}$. That quantum strategies can do no better then follows from the fact that $P_Q^{\max} = P_C^{\max}$ for the chosen $\tilde{p}$. Hence, even in this scenario, the identity of classical and quantum optimal performance is preserved.

It is also straightforward to extend the above results to the nonlocal computation of $f(z)$ by any number of parties. In the multiparty case, the function's inputs and output are encoded in the modulo 2 sum of m separate inputs $x^{(r)}$ and outputs $a^{(r)}$ (with all sets of $x^{(r)}$ consistent with z equally probable). Note that this task cannot be easier than nonlocal computation with only two parties; hence, the bounds obtained above must still apply. Furthermore, it is easy to see that the classical strategy

$$a^{(r)}(x^{(r)}) = \begin{cases} u \cdot x^{(r)} + \delta & : r = 0 \\ u \cdot x^{(r)} & : r = 1, \ldots, m-1 \end{cases} \tag{22}$$

yields the same success probability as the 2-party strategy (16), and therefore achieves the quantum bound (14).

We also note that each choice of $f(z)$ and $\tilde{p}(z)$ corresponds to a Bell-type inequality:

$$\sum_{x,y} C(x,y)\langle \hat{A}_x \hat{B}_y \rangle \leq K, \tag{23}$$

where $C(x,y) = (-1)^{f(x \oplus y)} \tilde{p}(x \oplus y)$, the observables $\hat{A}_x$ and $\hat{B}_y$ have outcomes ± 1, and $K = 2^n[2P_C^{\max}(f) - 1]$. Our results imply that there is also a Tsirelson-type inequality with exactly the same coefficients constraining quantum measurements. It would be interesting to discover if any of these inequalities generate facets of the Bell-polytope of classically attainable probability distributions $P(ab|xy)$ [13] (and consequently a facet of the set of attainable quantum probability distributions). In any case, we find that the Bell-polytope and the convex Tsirelson body have many (potentially lower-dimensional) faces in common which are not trivially inherited from the probability or nonsignalling constraints.

This also leads us to a considerable generalization of the nonlocal tasks described so far. Consider any Bell expression of the form given by (23), for which the largest singular value of the matrix $C(x,y)$ corresponds to an operator $|\tilde{u}\rangle\langle\tilde{v}|$ [where $|\tilde{u}\rangle, |\tilde{v}\rangle$ are as defined in (12)]. Then it follows from our analysis that quantum resources do not offer a benefit over classical resources for that task. However, note that not all nonlocal tasks for which quantum resources give no benefit are of this type [14].

Although functions with a single-bit output are very important (as they encapsulate all decision problems), it would also be interesting to extend these results to functions with a multibit output, or with different input and output alphabets (e.g., ternary rather than binary). In both cases, it is important to consider how success will be measured, as in addition to the total success probability used above, one could reasonably measure success by the average "distance" between the output and the correct answer. For functions with a multibit output, where success is measured by the number of correct output bits, our results still imply that quantum strategies provide no advantage over classical (because the best strategy is to optimally compute each output bit independently).

Perhaps the most interesting open question is whether all stronger-than-quantum correlations are helpful in performing some nonlocal computation. We have already shown that an interesting class of nonlocal correlation has this property (noisy PR-boxes). If this could be shown to hold generally, we would obtain a powerful and intuitive characterization of *quantum* nonlocality, as those correlations which do not help in nonlocal computation, and a deeper insight into why stronger nonlocal correlations (apparently) do not occur in nature.

We thank Harry Buhrman for helpful conversations and the U.K. EPSRC "QIP IRC" and EC QAP projects for support.

[1] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[2] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[3] J. F. Clauser *et al.*, Phys. Rev. Lett. **23**, 880 (1969).
[4] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).
[5] G. Brassard *et al.*, Phys. Rev. Lett. **96**, 250401 (2006).
[6] J. Barrett *et al.*, Phys. Rev. A **71**, 022101 (2005).
[7] J. Barrett, Phys. Rev. A **75**, 032304 (2007).
[8] W. van Dam, Ph.D. thesis, University of Oxford, 2000; see also arXiv:quant-ph/0501159.
[9] A. J. Short, S. Popescu, and N. Gisin, Phys. Rev. A **73**, 012101 (2006).
[10] Nonsignalling from Alice to Bob is ensured by demanding that $\sum_a P(ab|xy)$ is independent of x, and an analogous condition prevents signalling from Bob to Alice.
[11] B. S. Tsirelson, Lett. Math. Phys. **4**, 93 (1980).
[12] O. Morgenstern and J. von Neumann, *Theory of Games and Economic Behavior* (Princeton, Princeton, NJ, 1944).
[13] R. F. Werner *et al.*, Quantum Information Problems (1 and 26), http://www.imaph.tu-bs.de/qi/problems/.
[14] N. Linden and S. Popescu (to be published).