PHYSICAL REVIEW A, VOLUME 65, 032121

Nonlocality, closing the detection loophole, and communication complexity

Serge Massar
Service de Physique Théorique, Université Libre de Bruxelles, Code Postal 225, Boulevard du Triomphe, B1050 Bruxelles, Belgium
(Received 10 September 2001; published 1 March 2002)

It is shown that the detection loophole that arises when trying to rule out local realistic theories as alternatives for quantum mechanics can be closed if the detection efficiency $\eta \geqslant Cd^{3/4}2^{-0.0035d}$ where d is the dimension of the bipartite entangled system and C is a positive constant. Furthermore it is argued that such an exponential decrease of the detector efficiency required to close the detection loophole is almost optimal. This optimality argument is based on a close connection that exists between closing the detection loophole and the amount of classical communication required to simulate quantum correlations when the detectors are perfect.

DOI: 10.1103/PhysRevA.65.032121 PACS number(s): 03.65.Ud, 03.67.−a

Experimental tests of the entanglement of quantum systems are important for several reasons. They provide an experimental check of the validity of quantum mechanics, and in particular the surprising "nonlocality" exhibited by quantum mechanics. Furthermore they can be viewed as primitives from which one can build more complicated protocols of interest for quantum information processing and they provide a benchmark with which to compare the performance of different quantum systems, such as ion traps, photons, etc.

To test the entanglement of a quantum system one carries out measurements on each particle, and compares the correlations between the results of these measurements with the predictions of quantum mechanics. A crucial check of the quantumness of these correlations is whether they exhibit "nonlocality," that is, whether it is impossible to reduce them by a classical local-variable theory (also called local-realistic theory) [1]. Formally, this is done by inserting the joint probabilities of outcomes into an inequality, called a "Bell inequality," which must be satisfied in the case of local-variable theories but can be violated by quantum mechanics.

During the past decades successively more sophisticated tests of Bell inequalities have been carried out (for a review see [2]). Most experiments so far have involved entangled photons. By letting the photons propagate a large distance from their emission point it has been possible to spatially separate the two measurements and thereby close the so-called "locality loophole." However, in optical experiments, because of losses and small detector efficiency, all tests of Bell inequalities so far leave open the so-called "detection loophole." This means that all experimental results that use pairs of photons can be explained by a classical local-variable theory if the local-variable theory can instruct the detectors either to click, i.e., register the presence of a particle, or not. The strongest theoretical result so far is that the detection loophole can be closed in the efficiency is $\eta > 2/3$ [3], but this is too stringent for optical experiments. Recently an experiment that closes the detection loophole has been carried out using trapped ions [4]. But in this experiment the ions were separated by a very small distance and the locality loophole was not closed.

In almost all experiments on entangled systems each system belongs to a Hilbert space of dimension 2. (One recent experiment tested the entanglement of systems of dimension 3 [5].) However, when pairs of photons are produced (for instance by parametric down conversion), the photons are entangled in position-momentum and time-energy in addition to a possible entanglement in polarization. Thus entangled systems of large dimensionality can easily be produced in the laboratory. Can one exploit the large dimensionality of these entangled photons to carry out stronger tests of quantum nonlocality? This has been the subject of several recent theoretical works [6–10] in which it has been shown that using entangled systems of large dimensionality can be advantageous, but no spectacular improvements have been found.

In the present work it will be shown that using entangled systems of large dimensionality allows in principle a dramatic decrease in the detector efficiency required to close the detection loophole. More precisely, the minimum detector efficiency required to close the detection loophole decreases exponentially with the dimension d. This is particularly relevant to possible experiments involving momentum or energy-entangled photons since in this case it may be possible to devise an experiment in which photon losses and detector efficiency decrease only slowly with the dimension.

This result is obtained by explicitly describing a set of measurements carried out by Alice and Bob on an entangled system of large dimension and writing a Bell inequality adapted to this measurement scenario. It will be shown that this Bell inequality is violated even for exponentially small detector efficiencies. However, this Bell inequality is extremely sensitive to noise and therefore does not constitute a realistic experimental proposal. A noteworthy feature of this measurement scenario is that the number of measurements between which Alice and Bob must choose is exponentially large.

In the second part of this paper we consider whether it is possible to improve this Bell inequality. Can one decrease the number of measurements between which Alice and Bob must choose, or decrease the dimensionality of the entangled system, while keeping the same low sensitivity to detector inefficiency? We argue that this is not the case and that our Bell inequality is close to optimal.

These latter results follow from a close connection between the detection loophole and the minimum amount of classical communication required to perfectly simulate measurements on an entangled quantum system. Suppose measurements are carried out on an entangled quantum system (with perfect detectors $\eta = 1$). The correlations exhibited by such measurements will in general violate a Bell inequality and therefore cannot be reproduced by local variable theories. However, by supplementing the local-variable theory by classical communication one can reproduce the quantum correlations. Recently there have been several works that attempted to understand how much classical communication is necessary to bridge the gap between quantum mechanics and local-variable theories [11,13,14]. Intuitively one would expect that the greater the amount of communication required to recover the quantum correlations, the stronger is the nonlocality of the quantum-correlation test. This intuition will be made precisely below in the context of the detection loophole. It will be shown that the minimum amount of classical communication C^{min} required to recover the quantum correlations is anticorrelated to the minimum detection efficiency η^* required to close the detection loophole.

We begin with some definitions.

Definition 1. A measurement scenario is defined by a bipartite quantum state ψ belonging to the tensor product of two Hilbert spaces $H_A \otimes H_B$, and by two ensembles of measurements, M_A acting on H_A and M_B acting on H_B. For instance $\psi = \sum_{k=1}^{d} |k\rangle_A |k\rangle_B / \sqrt{d}$ can be the maximally entangled state of d dimensions. The elements $x \in M_A$ are a basis of H_A: $x = \{|x_1\rangle, \ldots, |x_d\rangle\}$ with $\langle x_i | x_j \rangle = \delta_{ij}$. Similarly the elements $y \in M_B$ are a basis of H_B. Party A is given a random element $x \in M_A$ as input and party B is given a random element $y \in M_B$ as input.

Definition 2. In a measurement scenario with perfect detectors ($\eta = 1$), both parties must give as output one of d possible outcomes. Denote Alice's output by a and Bob's output by b. The joint probabilities of the outcomes are $P(a=i, b=j | x,y) = |\langle \psi | x_i \rangle | y_j \rangle|^2$.

Defintion 3. In a measurement scenario with detectors of finite efficiency η, both parties must give as output one of $d+1$ possible outcomes. Output 0 occurs with probability $1-\eta$ and corresponds to the detector not detecting the particle whereas outcomes 1 to d occur with probability η and correspond to a specific result of the measurement when the particle is detected. The probability that one of the detectors gives outcome 0 is independent of the other detector. Thus the joint probabilities of outcomes are

$$P(a=0, b=0 | x,y) = (1-\eta)^2,$$

$$P(a=i, b=0 | x,y) = \eta(1-\eta) \mathrm{Tr} |x_i\rangle\langle x_i| \otimes \mathbb{1}_B |\psi\rangle\langle\psi|,$$

$$P(a=0, b=j | x,y) = \eta(1-\eta) \mathrm{Tr}\, \mathbb{1}_A \otimes |y_j\rangle\langle y_j| |\psi\rangle\langle\psi|,$$

$$P(a=i, b=j | x,y) = \eta^2 |\langle \psi | x_i \rangle | y_j \rangle|^2. \tag{1}$$

Definition 4. In a local-variable theory for the measurement scenario $\{\psi, M_A, M_B\}$ with detector efficiency η, Alice and Bob are both given the same element $\lambda \in \Lambda$ drawn with probability $p(\lambda)$ (often called the "local-hidden variable"). Alice knows x but does not know y. From her knowledge of λ and x, Alice selects an outcome $a = f(x,\lambda)$. Similarly Bob knows y but does not know x and chooses an outcome $b = g(y,\lambda)$. We can suppose that the functions f and g are deterministic since all local randomness can be put in λ. The joint probabilities

$$P(a,b|x,y) = \int_\Lambda d\lambda\, p(\lambda)\, \delta(f(x,\lambda) - a)\, \delta(g(y,\lambda) - b)$$

are identical with the predictions of quantum mechanics Eq. (1).

A local-variable theory will only exist if the detector efficiency is sufficiently small. The maximum detector efficiency for which a local-variable theory exists will be denoted $\eta^*(\psi, M_A, M_B)$.

We are now in a position to state our main result.

Theorem 1. There exists a measurement scenario for which the state is the maximally entangled state of dimension $d = 2^n$ with $n \geqslant 2$ an integer, and for which the number of measurements carried out by Alice and Bob are exponentially large $|M_A| = |M_B| = 2^d$, and such that the detection loophole is closed if $\eta \geqslant C d^{3/4} 2^{-0.0035d}$ where C is a positive constant.

Proof. We consider the same measurement scenario as that described in Theorem 4 of [11] that itself is inspired by the Deutch-Jozsa problem, see [12]. The state is $\psi = \sum_{k=1}^{d=2^n} |k\rangle |k\rangle / \sqrt{d}$. The sets of measurements M_A and M_B are identical. The measurements $x \in M_A$ are parametrized by a string of d bits: $x = x_1 x_2 \ldots x_d$ where $x_i \in \{0,1\}$ and similarly for $y \in M_B$. Hence $|M_A| = |M_B| = 2^d$. The measurements are described in detail in [11].

They have the following properties: (1) if $x = y$, then Alice and Bob's outcomes are identical ($a = b$); (2) if the Hamming distance $\Delta(x,y)$ between x and y is $\Delta(x,y) = d/2$, then Alice and Bob's outcomes are always different ($a \neq b$).

Let us define

$$\alpha(x,y) = \delta(x-y) - \delta(\Delta(x,y) - d/2),$$

which is equal to $+1$ if $x = y$, equal to -1 if $\Delta(x,y) = d/2$, and equal to zero otherwise. Consider the following Bell expression:

$$I = \sum_{x=1}^{2^d} \sum_{y=1}^{2^d} P(a=b \;\; \text{AND} \;\; a \neq 0)\, \alpha(x,y). \tag{2}$$

It is immediate to compute the value of I predicted by quantum mechanics for the above measurement scenario since from properties 1 and 2 above, only the term proportional to $\delta(x=y)$ contributes,

$$I(QM) = \eta^2 2^d. \tag{3}$$

It is more difficult to compute the maximum value of I in the case of local-variable theories. Let Z be the largest subset of $\{0,1\}^d$ such that if $z, z' \in Z$, then $\Delta(z,z') \neq d/2$ (i.e. no two elements of Z are Hamming distance $d/2$ one from the other). We shall show below that

$$I(\text{local variable}) \leqslant d|Z| \tag{4}$$

independently of η. Frankl and Rödl have given bounds on $|Z|$. Theorem 1.10 of [15] states that when d is divisible by 4, then $|Z|<(2-\epsilon)^d$ for some universal constant $\epsilon>0$. Combining this with Eq. (3) implies that one can close the detection loophole if

$$\eta \geqslant d^{1/2}\left(1-\frac{\epsilon}{2}\right)^{d/2}. \tag{5}$$

In order to obtain a more precise result we introduce a slightly different Bell expression. We denote by R the set of all strings of d bits $x_1 \ldots x_d$, such that exactly $d/2$ of the bits are equal to 1 and $d/2$ of the bits are equal to 0. The number of such strings is

$$|R| = \binom{d}{d/2} = \frac{\sqrt{2}}{\sqrt{\pi d}} 2^d [1+o(1)]. \tag{6}$$

The second Bell expression is

$$J = \sum_{x\in R}\sum_{y\in R} P(a=b \text{ AND } a\neq 0)\,\alpha(x,y). \tag{7}$$

It is immediate to compute the value of J predicted by quantum mechanics for the above measurement scenario

$$J(QM) = \eta^2 |R|. \tag{8}$$

It is more difficult to compute the maximum value of J in the case of local-variable theories. Let Q be the largest subset of R such that if $z,z' \in Q$, then $\Delta(z,z') \neq d/2$ (i.e., no two elements of Q are Hamming distance $d/2$ one from the other). In analogy with Eq. (4) one has

$$J(\text{local variable}) \leqslant d|Q| \tag{9}$$

independent of η. Frankl and Rödl have given bounds on $|Q|$. Corollary 1.2 of [15] implies that when d is divisible by 4, then $|Q| \leqslant 1.99^d < 2^{0.993d}$. Combining this with Eq. (8) implies that one can close the detection loophole if

$$\eta \geqslant \sqrt{\frac{d|Q|}{|R|}} \geqslant \frac{d^{3/4}\pi^{1/4}}{2^{1/4}} 2^{0.0035d}[1+o(1)]. \tag{10}$$

We now prove Eq. (4). The proof of Eq. (9) is exactly the same and will not be given. Recall that in the case of local-variable model, Alice's output is a function $a(\lambda,x)$ of the local variable and of her measurement, and similarly for Bob. Using $P(a=b \text{ AND } a\neq 0) = \Sigma_{k=1}^{d} P(a=k \text{ AND } b=k)$, the value of I for a local-variable model can be written as

$$\begin{aligned} I(\text{lv}) &= \sum_{\lambda} p(\lambda) \sum_x \sum_y \sum_{k=1}^{d} \\ &\quad \times P[a(\lambda,x)=k \text{ AND } b(\lambda,y)=k]\,\alpha(x,y) \\ &= \sum_{\lambda} p(\lambda) \sum_{k=1}^{d} \sum_{x\in X_{k\lambda}} \sum_{y\in Y_{k\lambda}} \alpha(x,y), \end{aligned} \tag{11}$$

where $X_{k\lambda}$ is the set of x such that $a(\lambda,x)=k$ and $Y_{k\lambda}$ is the set of y such that $b(\lambda,y)=k$.

Let us denote by $Z_{k\lambda}$ the largest set such that: (1) $Z_{k\lambda} \subset X_{k\lambda}$; (2) $Z_{k\lambda} \subset Y_{k\lambda}$; (3) if $z,z' \in Z_{k\lambda}$ then $\Delta(z,z') \neq d/2$. The third defining property of $Z_{k\lambda}$ implies that $|Z_{k\lambda}| \leqslant |Z|$.

Consider the sum $\beta(x) = \Sigma_{y\in Y_{k\lambda}} \alpha(x,y)$. From the definition of α, it follows that $\beta(x)$ is an integer less than or equal to 1. Let us show that if $x \notin Z_{k\lambda}$, then $\beta(x) \leqslant 0$. Suppose this is not true [i.e., $x \notin Z_{k\lambda}$ and $\beta(x)=1$], then necessarily $x \in Y_{k\lambda}$ and there is no $y \in Y_{k\lambda}$ such that $\Delta(x,y)=d/2$. But then we could increase $Z_{k\lambda}$ by adding x to $Z_{k\lambda}$. But $Z_{k\lambda}$ is maximal, hence there is a contradiction. We therefore obtain that $\Sigma_{x\in X_{k\lambda}} \beta(x) \leqslant \Sigma_{x\in Z_{k\lambda}} \beta(x) \leqslant |Z_{k\lambda}| \leqslant |Z|$. Inserting this in Eq. (11) yields Eq. (4). ■

Note that the Bell expressions Eqs. (2) and (7) are extremely sensitive to noise. This is because in the presence of noise the term in α proportional to $\delta(\Delta(x,y)=d/2)$ receives a very large contribution, and therefore leads to a much reduced value of I.

We now turn to the relation between the detection loophole and communication complexity. We begin with a definition.

Definition 5 In a local-variable theory supplemented by C bits of classical communication for the measurement scenario $\{\psi, M_A, M_B\}$ with perfect detectors ($\eta=1$), the parties, in addition to sharing the random variable λ, are allowed to communicate C bits before choosing their output.

Note that one should distinguish whether C is the absolute bound on the amount of communication, or whether C is the average amount of communication between the parties, where the average is taken over many repetitions of the protocol, see [14]. For a given measurement scenario $\{\psi, M_A, M_B\}$ with perfect detectors one can try to minimize the amount of communication required to reproduce the quantum probabilities. The minimum amount of communication required to simulate the measurement scenario in the average communication model will be denoted $C^{min}(\psi, M_A, M_B)$.

We shall now show that the minimum detector efficiency η^* required to close the detection loophole and the minimum amount of communication C^{min} required to simulate a measurement scenario with perfect detectors are closely related. We begin by showing that if a measurement scenario is difficult to simulate classically, then the minimum detector efficiency required to close the detection loophole is small. In fact this result was the inspiration for Theorem 1: the measurement scenario considered in Theorem 1 is difficult to simulate classically [11], hence η^* must be small. Further investigations led to the strong result of Theorem 1.

Theorem 2. For all measurement scenarios $\{\psi, M_A, M_B\}$, the relation $\eta^*(\psi, M_A, M_B) \leqslant \sqrt{2/C^{min}(\psi, M_A, M_B)}$ holds.

Proof. It will be shown that any local-variable model with detector efficiency η can be mapped into a communication protocol with an average of $2/\eta^2$ bits of communication. Therefore $C^{min} \leqslant 2/\eta^2$ for all detector efficiencies for which a local-variable model exists, and this yields the upper bound on η^*.

Recall that a local-variable model is defined by the two functions f and g introduced above and the probability distribution p on the space Λ. Now suppose that initially the parties share an infinite number of independent identically distributed hidden variables $\lambda_1,\lambda_2,\lambda_3,\ldots$ each drawn from the space Λ with probability p. Consider the following protocol in which the two parties repeatedly simulate the local-variable model and communicate whether the model predicts that the detectors work or not: (1) Set the index $k=1$. (2) Alice computes $f(x,\lambda_k)$ and Bob computes $g(y,\lambda_k)$. (3) Alice tells Bob whether $f(x,\lambda_k)=0$ or $f(x,\lambda_k)\neq 0$ and Bob tells Alice whether $g(y,\lambda_k)=0$ or $g(y,\lambda_k)\neq 0$. (4) If $f(x,\lambda_k)=0$ or $g(y,\lambda_k)=0$, Alice and Bob increase the index k by 1 and go back to step 2. (5) If $f(x,\lambda_k)\neq 0$ and $g(y,\lambda_k)\neq 0$ then Alice outputs $f(x,\lambda_k)$ and Bob outputs $g(y,\lambda_k)$.

This protocol reproduces exactly the correlations exhibited by quantum mechanics. The mean number of iterations of the protocol is $1/\eta^2$. The number of bits communicated during each iteration is 2 (one bit from Alice to Bob and one from Bob to Alice). Hence the average amount of communication is $2/\eta^2$. ■

We now investigate the converse, namely, whether a model with finite communication and perfect detectors can be mapped into a local-variable model with inefficient detectors. We will give an argument, but not a proof, that suggests that such a mapping should exist.

Consider a measurement scenario. Suppose there is a classical protocol that simulates the quantum correlations with C bits of communication. In this protocol, Alice initially knows the local variable λ and her measurement x, and Bob initially knows the local variable λ and his measurement y. Denote the conversation by $\mathcal{C}(x,y,\lambda)=c_1c_2\ldots$ where $c_i\in\{0,1\}$ is the ith bit in the conversation. Alice and Bob's outputs are, therefore, given by functions $a=f(x,\lambda,\mathcal{C})$ and $b=g(y,\lambda,\mathcal{C})$.

Now suppose that in addition to the local variable λ, Alice and Bob share a second local variable $\mu=\mu_1\mu_2\ldots$ that consists of an infinite string of independent random bits $\mu_i\in\{0,1\}$. The basic idea is that Alice and Bob will check whether the local variable μ is a possible conversation $\mu=\mathcal{C}(x,y,\lambda)$. If it is they give the corresponding output. If it is not they give the outcome 0 corresponding to the detectors not working. The probability that $\mu=\mathcal{C}$ is 2^{-C}. This suggests that if $\eta\leqslant 2^{-C}$ a local-variable model should exist.

Making the above argument precise is difficult because one wants to recover exactly the probability distribution Eq. (1). For instance if some conversation are shorter than others, then they will be accepted with higher probability, yielding a skewed distribution. Nevertheless the above argument is very suggestive. For instance in [14] it was shown that if the entangled state has dimension d, then any measurement scenario can be simulated in the average communication model using less than $[6+3\log_2(d)]d+2$ bits on average. Combining this with the above argument suggests that if $\eta<O(2^{-6d}d^{-3d})$ a local-variable model should exist. This in turn suggests that Theorem 1 is close to optimal.

It is also interesting to combine the above argument with a result from [11] that states that it is always possible to simulate a measurement scenario with $C=\log_2|M_A|$ bits of communication. Combining this with the above argument suggests that if $\eta>1/|M_A|$ a local-variable model should exist. We now prove this result (in a slightly weaker form, since the result in [11] depends only on $|M_A|$, independently of $|M_B|$) by generalizing an argument of Gisin and Zbinden [16].

Theorem 3. Consider a measurement scenario in which the number of possible measurements is $|M_A|=|M_B|=M$. Then a local-hidden-variable model exists if the detector efficiency is $\eta=1/M$.

Proof. The local-hidden variable consists of the quadruple (x,i,y,j) where $x\in M_A$, $y\in M_B$, $i,j\in\{1,\ldots,d\}$ and i,j have joint probabilities $P(i,j)=|\langle\psi|x_i\rangle|y_j\rangle|^2$. The protocol is as follows. Alice checks whether her measurement is equal to x, if so she outputs i, if not she outputs 0, Bob checks whether his measurement is equal to y, if so he outputs j, if not he outputs 0. This reproduces exactly the correlations Eq. (1) with $\eta=1/M$. ■

In summary we have presented a measurement scenario that closes the detection loophole when the detector efficiency $\eta\simeq d^{3/4}2^{-0.0035d}$ is exponentially small. This should be contrasted to the best previous result that required $\eta>2/3$ [3]. Our measurement scenario requires an entangled system of large dimension d, and it requires that Alice and Bob choose between exponentially many measurements. We have argued that it is not possible to substantially improve this measurement scenario, either by decreasing the number of measurements, or by decreasing the dimension, while keeping the same resistance to inefficient detectors.

The results reported here are inspired by recent work in communication complexity. Indeed the measurement scenario we consider in our main theorem is also known to require a large amount of communication in order to be simulated classically [11]. And we present general arguments concerning bounds on the minimum detector efficiency required to close the detection loophole follow from mappings between communication models and local-variable models with inefficient detectors. This connection between two different approaches to entanglement, namely, the point of view of computer scientists and the more pragmatic considerations of experimentalists will, we hope, continue to prove fruitful.

I would like to thank Harry Buhrman, Nicolas Cerf, Richard Cleve, Thomas Durt, Nicolas Gisin, Jan-Åke Larsson, Noah Linden and Sandu Popescu for helpful discussions. Funding by the European Union under project EQUIP (IST-FET program) is gratefully acknowledged.

[1] J.S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[2] A. Aspect, Nature (London) **398**, 189 (1999).
[3] P.H. Eberhard, Phys. Rev. A **47**, R747 (1993).
[4] M.A. Rowe, D. Kielpinski, V. Meyer, C.A. Sackett, W.M.

Itano, C. Monroe, and D.J. Wineland, Nature (London) **409**, 791 (2001).
[5] J.C. Howell, A. Lamas-Linares, and D. Bowmeester, e-print quant-ph/0105132.
[6] D. Kaszlikowski, P. Gnacinski, M. Zukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).
[7] T. Durt, D. Kaszlikowski, and M. Zukowski, e-print quant-ph/0101084.
[8] J.-L. Chen, D. Kaszlikowski, L.C. Kwek, M. Zukowski, and C.H. Oh, e-print quant-ph/0103099.
[9] D. Kaszlikowski, L.C. Kwek, J.-L. Chen, M. Zukowski, and C.H. Oh, e-print quant-ph/0106010.
[10] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, e-print quant-ph/0106024.
[11] G. Brassard, R. Cleve, and A. Tapp, Phys. Rev. Lett. **83**, 1874 (1999).
[12] H. Buhrman, R. Cleve and A. Wigderson, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1998), pp. 63–68.
[13] M. Steiner, Phys. Lett. A **270**, 239 (2000).
[14] S. Massar, D. Bacon, N.J. Cerf, and R. Cleve, Phys. Rev. A **63**, 052305 (2001).
[15] P. Frankl and V. Rödl, Trans. Am. Math. Soc. **300**, 259 (1987).
[16] N. Gisin and H. Zbinden, Phys. Lett. A **264**, 103 (1999).