

Combinatorics and Quantum Nonlocality

Harry Buhrman*

CWI and University of Amsterdam, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands

Peter Høyer†

Dept. of Comp. Sci., University of Calgary, 2500 University Drive N.W., Calgary AB, Canada T2N 1N4

Serge Massar‡

*Service de Physique Théorique, Université Libre de Bruxelles,
C.P. 225, Bvd. du Triomphe, 1050 Bruxelles, Belgium*

Hein Röhrig*

CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands

(Dated: February 4, 2003)

We use techniques for lower bounds on communication to derive necessary conditions (in terms of detector efficiency or amount of super-luminal communication) for being able to reproduce the quantum correlations occurring in EPR-type experiments with classical local hidden-variable theories. As an application, we consider n parties sharing a GHZ-type state and show that the amount of super-luminal classical communication required to reproduce the correlations is at least $n(\log_2 n - 3)$ bits and the maximum detector efficiency η_* for which the resulting correlations can still be reproduced by a local hidden-variable theory is upper bounded by $\eta_* \leq 8/n$ and thus decreases with n .

PACS numbers: 03.67.Hk, 03.65.Ta

I. INTRODUCTION

Some 40 years ago Bell showed that entangled quantum states are nonlocal [1]. Although much is known about nonlocality in the simplest cases, there are few clear results when the number n of systems or the dimension d of the systems is large. In this paper we show how combinatorial techniques can be used to study quantum nonlocality, particularly in the asymptotic cases.

We consider two ways in which the nonlocality of the quantum correlation can be measured: 1) the minimum efficiency η of detectors required for the correlations to exhibit nonlocality (this is the so-called “detection loophole”[2]); 2) the amount of classical communication required to reproduce the quantum correlations [3, 4]. (Note that if the measurements that are carried out on the entangled state are spatially separated events, this communication would have to occur faster than the speed of light, which is impossible. If the events are timelike separated, this communication can occur without contradicting relativity.) It has been shown that these two measures are closely related [5, 6]. In this paper we further explore this connection.

The amount of (possibly super-luminal) classical communication required to reproduce the quantum correlations, is related to the question examined in [7, 8] of whether entanglement could decrease the amount of communication required to compute a distributed function. This is the subject of the field of computer science called “communication complexity.” Special combinatorial techniques have been developed to prove lower bounds on the amount of communication required to solve such problems, see [9] for an overview. Here we show that the same combinatorial techniques can be used to provide bounds on the minimum detector efficiency required to close the detection loophole.

As an application of our method we obtain new results concerning how nonlocality scales with the number of systems. We consider a specific case in which n parties each possess a two-dimensional system. The state of the overall system is a GHZ-type state. We show that the amount of communication required to reproduce these correlations classically is at least $n(\log_2 n - 3)$ bits and that the minimum detector efficiency η_* required to close the detection loophole in this case *decreases* as $1/n$ where n is the number of parties. This bound on η_* is a significant improvement over previous results, which could only show that the threshold detector efficiency stays constant as the number of parties increases [10, 11, 12]. We discuss possible experimental tests of these correlations.

II. DEFINITIONS

Consider the following situation. There are n spatially separated parties; party i receives an input $X_i \in$

*Supported in part by the EU fifth framework projects QAIP, IST-1999-11234, and RESQ, IST-2001-37559.

†Supported in part by the Alberta Ingenuity Fund and the Pacific Institute for the Mathematical Sciences.

‡Also at Ecole Polytechnique, C.P. 165, Université Libre de Bruxelles, 1050 Brussels, Belgium; supported in part by the EU fifth framework projects EQUIP, IST-1999-11053, and RESQ, IST-2001-37559.

$\{1, \dots, k\}$ and produces an output $a_i \in \{1, \dots, d\}$. With $X = (X_1, \dots, X_n)$ and $a = (a_1, \dots, a_n)$, let $P(a|X)$ denote the probability of output a given input X . We formalize this situation as follows.

Definition 1 An (n, k, d) correlation problem with promise $D \subseteq \{1, \dots, k\}^n$ is a family of probability distributions $P(\cdot|X)$ on the “outputs” $\{1, \dots, d\}^n$, for each “input” $X \in D$.

In an experimental setup, we would configure the random-number generators for the inputs to produce settings only from D and thus an adversary constructing a classical model would be “promised” that he only has to reproduce the conditional probabilities for inputs from D . A restriction of this type often simplifies the analysis of what quantum and classical models can or cannot achieve.

Of particular interest are correlation problems obtained from quantum mechanical experiments in which the parties share an entangled state $|\psi\rangle$; each input X_i determines a von Neumann measurement \hat{X}_i . The measurement of \hat{X}_i produces result a_i . The probability $P_{\text{QM}}(a|X)$ to obtain outcome a given input X is easily computed using the standard rules of quantum mechanics.

In the case of inefficient detectors we enlarge the space of outputs to $a_i \in \{1, \dots, d\} \cup \{\perp\}$, where $a_i = \perp$ is the event that the i th detector does not produce an output (“click”). We suppose that each measurement \hat{X}_i has probability η of giving a result and a probability $1 - \eta$ of not giving a result. We are interested in the case where all n detectors give a result. This occurs with probability η^n .

Let us consider classical models in which the parties cannot communicate after they have received the inputs (such models are called *local*). The best the parties can do in this case is to randomly select in advance a deterministic strategy. This motivates the following definition.

Definition 2 A deterministic local hidden variable (lhv) model is a family of functions $\lambda = (\lambda_1, \dots, \lambda_n)$ from the inputs to the outputs: $\lambda_i : \{1, \dots, k\} \rightarrow \{1, \dots, d, \perp\}$. Each party outputs $a_i = \lambda_i(X_i)$.

A probabilistic lhv model (or just lhv model) is a probability distribution $\nu(\lambda)$ over all deterministic lhv models for given (n, k, d) .

Thus in probabilistic lhv models the parties first randomly choose a deterministic lhv model λ using the probability distribution ν . Each party then outputs $a_i = \lambda_i(X_i)$. In general, lhv models cannot reproduce the quantum correlations P_{QM} except if the detector efficiency η is sufficiently small. For a fixed correlation problem (based on the quantum correlations P_{QM}), we denote by $\eta_* = \eta_*(P_{\text{QM}})$ the maximum detector efficiency for which a lhv model exists. Our aim is to obtain upper bounds on η_* .

We also consider classical models with communication. In such models, the parties may communicate over a

(possibly super-luminal) classical broadcast channel in order to reproduce the quantum correlations P_{QM} . Different communication models exist depending on whether the parties do not have access to randomness, possess local randomness only, or possess shared randomness.

Definition 3 For a correlation problem P , denote by $R(P)$, and $R^{\text{pub}}(P)$, respectively, the minimum number of bits that must be broadcast in order to perfectly reproduce the correlations P when the parties have local randomness only or have shared randomness, respectively.

Clearly, $R(P) \geq R^{\text{pub}}(P)$. $R(P)$ can be infinite [13]; in this work we derive lower bounds on R^{pub} .

Since the results of quantum measurements are inherently random, it is in general impossible to reproduce the quantum correlations using deterministic lhv models or using deterministic models with communication. However, deterministic models are a very useful tool for studying the probabilistic models. In particular, properties of *all* deterministic models necessarily also hold for *all* probabilistic models.

III. COMBINATORIAL BOUNDS

Our results are not based on the details of the probability distribution $P(\cdot|X)$, but only on whether a given output a has nonzero probability given an input X .

Definition 4 For a given correlation problem with promise D , we call output a admissible on input $X \in D$ if and only if $P(a|X) > 0$.

We call a lhv model error free if and only if it produces for all inputs only admissible outputs.

In the following we consider only error-free models. We now introduce some definitions and notation which allow us to state our main result.

For sets A_1, \dots, A_n , a subset R of the Cartesian product $A_1 \times \dots \times A_n$ is called a *rectangle* if there are $R_1 \subseteq A_1, \dots, R_n \subseteq A_n$ such that $R = R_1 \times \dots \times R_n$, i.e., R is a Cartesian product itself.

The importance of rectangles is that for a deterministic lhv model $\lambda = (\lambda_1, \dots, \lambda_n)$, the set $R_\lambda(a) = \{X : \lambda(X) = a\}$ of all inputs X leading to output a is a rectangle: $R_\lambda(a) = \lambda_1^{-1}(a_1) \times \dots \times \lambda_n^{-1}(a_n)$.

Let us consider outputs $a \in \{1, \dots, d\}^n$. We call a set $R \subseteq \{1, \dots, k\}^n$ *a-monochromatic* with respect to an (n, k, d) correlation problem P with promise D if for all $X \in R \cap D$, $P(a|X) > 0$ (the term “monochromatic” derives from interpreting a as a color label of the points in X). Monochromatic rectangles play a central role in what follows because a deterministic lhv model λ produces only admissible outputs if and only if for all $a \in \{1, \dots, d\}^n$, $R_\lambda(a)$ is *a-monochromatic*.

Our results are stated in terms of maximum size of monochromatic rectangles. Specifically, for a correlation problem P with promise D , we will denote the

size of the largest overlap of the promise D with an a -monochromatic rectangle (with $a \in \{1, \dots, d\}^n$) by

$$r(P) := \max\{|R \cap D| : R \text{ monochromatic rectangle}\}.$$

This allows us to bound the minimum number $\text{cov}(P)$ of monochromatic rectangles required to cover D : $\text{cov}(P) \geq |D|/r(P)$. Our main results can now be stated with precision.

Theorem 1 *The maximum detection efficiency η_* for which an (n, k, d) correlation problem P with promise D can be explained by a lhv theory is bounded by*

$$\eta_* \leq d \left(\frac{r(P)}{|D|} \right)^{1/n}.$$

Theorem 2 *In the communication model where the parties have shared randomness, the minimum amount of communication required to reproduce the correlations for an (n, k, d) correlation problem P with promise D is*

$$R^{\text{pub}}(P) \geq \log_2 \left(\frac{\text{cov}(P)}{d^n} \right) \geq \log_2 \left(\frac{|D|}{d^n r(P)} \right).$$

Thus the same quantities provide a bound for the minimum amount of classical communication required to reproduce the quantum correlations and the minimum detector efficiency η_* required for the correlations to be nonlocal.

Proof of Theorem 1. A general lhv model without error can be interpreted as a probability distribution $\nu(\lambda)$ over all deterministic error-free lhv models λ : for each run, a deterministic lhv model λ is chosen according to the distribution ν before the inputs are received. Let $A_{\lambda, X} = 1$ if $\lambda_i(X_i) \neq \perp$ for all $i = 1, \dots, n$, and $A_{\lambda, X} = 0$ otherwise; i.e., $A_{\lambda, X} = 1$ if and only if all n detectors “click” in the deterministic lhv model λ on input X . With this notation, the probability that the probabilistic lhv model produces an output for inputs drawn uniformly at random from D is $q := \sum_X 1/|D| \sum_\lambda \nu(\lambda) A_{\lambda, X}$. If the detector efficiency is η , then the probability of all detectors clicking is $\eta^n = q$.

If we can show that any deterministic lhv model produces an admissible output for at most $d^n r(P)$ inputs, then no probabilistic lhv model can produce an admissible output with probability $q > d^n r(P)/|D|$, because $q = \sum_\lambda \nu(\lambda) \sum_X A_{\lambda, X}/|D| \leq \sum_\lambda \nu(\lambda) d^n r(P)/|D| = d^n r(P)/|D|$.

A deterministic lhv model λ that produces only admissible outputs can give an output with all detectors clicking for at most $d^n r(P)$ input settings, because for each of d^n possible outputs a , $R_\lambda(a)$ is a monochromatic rectangle of size $|R_\lambda(a)| \leq r(P)$.

In conclusion, if $d^n r(P)/|D| < q = \eta^n$ no lhv model can reproduce the correlations. \square

Proof of Theorem 2. We now consider classical models with a limited amount of communication and perfect

detector efficiency. As in the previous proof, any such model can be interpreted as a probability distribution $\nu(\lambda)$ over deterministic models λ with communication and perfect detector efficiency. Since there are no errors, the models λ with nonzero probability $\nu(\lambda) > 0$ in this decomposition must produce only admissible outputs. We now show that deterministic models that produce only admissible outputs require at least $\log_2(\text{cov}(P)/d^n)$ bits of communication. Hence probabilistic models also require at least $\log_2(\text{cov}(P)/d^n)$ bits of communication.

Consider a deterministic model with at most c bits of communication producing only admissible outputs. This model can be represented by a tree where each node is labeled by the party whose turn it is to send a message, and the edges to children are labeled by which message was sent; a run of the model corresponds to a path from the root of the tree to a leaf. The communication tree has at most 2^c leaves; with each leaf l we associate d^n sets $R(l, a) \subseteq \{1, \dots, k\}^n$ of the inputs leading to this leaf and producing output a . The deterministic model produces only admissible outputs, hence, $R(l, a)$ is a monochromatic rectangle for each l and a . Furthermore, the $R(l, a)$ must cover D since every input produces an output (the detector efficiency is 1), therefore we have $2^c d^n \geq \text{cov}(P)$ or, equivalently, $c \geq \log_2(\text{cov}(P)/d^n)$. \square

The proofs of Theorems 1 and 2 show the close relation between the detection loophole and the amount of communication required in the shared randomness model. In both cases the size of the largest monochromatic rectangle yields bounds on the detector efficiency and the amount of communication, respectively.

We can map any communication model with c bits of communication with shared randomness into a model with inefficient detectors with efficiency $\eta^n = 2^{-c}$: the shared randomness is used to randomly select a conversation between the parties and each party i checks whether its input X_i is compatible with the conversation and, if yes, produces output a_i according to the communication model and otherwise produces no output. The probability that all detectors click is equal to the probability that X belongs to the conversation. Since each input belongs to one and only one conversation, the probability that all detectors click is equal to one over the number of conversations. Note that in this model the probability that a specific detector, say detector i , clicks may depend on the input X_i (however, the probability that all detectors click remains independent of the input).

Theorem 3 *Consider lhv models where the probability that all detectors click is independent of the input, but where the probability that each detector clicks, say detector i , may depend on its input X_i . Then there exists a lhv model if the probability η^n that all detectors click is at most $2^{-R^{\text{pub}}}$. This implies that in these models,*

$$\eta_*^n \geq 2^{-R^{\text{pub}}}. \quad (1)$$

Theorem 1 also applies to the models considered in Theorem 3. Observe that together with Theorem 2, this im-

plies that in models where the bounds on R^{pub} coming from rectangles are almost tight, eq. (1) also is almost tight. This is for instance the case in the model considered below (see the discussion in [8]).

IV. AN APPLICATION

We now apply Theorems 1 and 2 to an example inspired by [8].

Theorem 4 *For each $n \geq 3$, there is a correlation problem P with n parties, $k = 2^{\lceil \log_2 n \rceil} \in \Theta(n)$ possible inputs per party, and $d = 2$ possible outputs per party with the following properties,*

- *it can be perfectly reproduced by a quantum mechanical system sharing a GHZ-type state $|\psi\rangle = (|0^n\rangle + |1^n\rangle)/\sqrt{2}$;*
- *it cannot be reproduced by an error-free lhw model for detector efficiency $\eta > 8/n$ or with less than $n(\log_2 n - \text{constant})$ bits of communication.*

Proof. Consider n parties, each of which possesses a two-dimensional quantum system. The entangled state of the n systems is a GHZ-type state, $|\psi\rangle = (|0^n\rangle + |1^n\rangle)/\sqrt{2}$. Each party i receives as input a l bit string: $X_i \in \{0, \dots, 2^l - 1\}$. The measurements carried out by the parties are the following. Each party carries out the unitary transformation $|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto \exp(2\pi\sqrt{-1}X_i/2^l)|1\rangle$. Each party then measures an operator whose eigenstates are $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$. The first outcome is assigned the value $a_i = 0$, the second the value $a_i = 1$, so $d = 2$.

In this measurement scenario, we have that if

$$\left(\sum_{i=1}^n X_i\right) \bmod 2^{l-1} = 0, \quad (2)$$

then

$$\left(\sum_{i=1}^n a_i\right) \bmod 2 = \frac{1}{2^{l-1}} \left\{ \left(\sum_{i=1}^n X_i\right) \bmod 2^l \right\}. \quad (3)$$

The promise D is taken to be the set of X that satisfy (2); the size of D is $|D| = 2^{(n-1)l}$ (since in eq. (2) $n-1$ of the X_i can be freely chosen and the last is then fixed). We say $S \subseteq \{0, \dots, 2^l - 1\}^n$ is b -monochromatic if

$$\frac{1}{2^{l-1}} \left\{ \left(\sum_{i=1}^n X_i\right) \bmod 2^l \right\} = b$$

for all $X \in S \cap D$. Reference [8] shows using addition theorems for finite groups that for $b \in \{0, 1\}$ any b -monochromatic rectangle R has size bounded by

$$r \leq \left(\frac{2^l - 2}{n} + 1\right)^n$$

whenever $R \cap D \neq \emptyset$. By eq. (3), for all $a \in \{0, 1\}^n$, any a -monochromatic set is also $(\sum_i a_i \bmod 2)$ -monochromatic. Therefore $r(P) \leq r$. Substituting these values into the bound of Theorem 1, we obtain

$$\eta_* \leq 2 \cdot 2^{l/n} \left(\frac{1}{n} - \frac{2}{n2^l} + \frac{1}{2^l}\right) \leq \frac{4}{n} n^{1/n} \leq \frac{8}{n}, \quad (4)$$

where l is taken so that $\log_2 n \leq l < \log_2 n + 1$ and the last inequality is valid when $n \geq 3$. Similarly, Theorem 2 yields $R^{\text{pub}} \geq n(\log_2 n - 3)$. \square

GHZ-type states involving three parties have been realized experimentally in cavity QED [14], in optics using spontaneous parametric down-conversion [15], and in NMR [16]. Optimizing eq. (4) shows that only a moderate number of parties is required for the super-luminal communication cost R^{pub} to increase and the threshold detection efficiency to decrease significantly. For example, for $n = 8$, $\eta_* \leq 0.46$ and $R^{\text{pub}} \geq 9$ bits, and for $n = 12$, $\eta_* \leq 0.29$ and $R^{\text{pub}} \geq 22$ bits. Therefore it should be feasible to realize experimentally the states and measurements required for these tests of quantum non-locality, using either extensions of the techniques above, ion traps [17] (up to four ions have been entangled), or atomic ensembles following a recent proposal [18]. However, in experiments noise is inevitable, whereas we have considered here only noiseless correlations. In an upcoming paper we will show how Theorem 4 can be generalized in the presence of noise.

In summary, we show that the combinatorial techniques developed to study communication complexity can be used to quantify the amount of (super-luminal) communication required to reproduce the quantum correlations or the minimum detection efficiency required to close the detection loophole. We apply this approach to multipartite entanglement: building on a result of [8] we show that in a precise and operational way the non-locality increases with the number of parties.

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

[2] P. Pearle, Phys. Rev. D **2**, 1418 (1970).

[3] G. Brassard, R. Cleve, and A. Tapp, Physical Review

Letters **83**, 1874 (1999).

[4] M. Steiner, Physics Letters A **270**, 239 (2000).

[5] N. Gisin and B. Gisin, Phys. Lett. A **260**, 323 (1999).

- [6] S. Massar, *Physical Review A* **65**, 032121 (2002).
- [7] R. Cleve and H. Buhrman, *Physical Review A* **56**, 1201 (1997).
- [8] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp, *Physical Review A* **60**, 2737 (1999).
- [9] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, 1997).
- [10] N. D. Mermin, *Physical Review Letters* **65**, 1838 (1990).
- [11] M. Zukowski, *Physics Letters A* **177**, 290 (1993).
- [12] J.-Å. Larsson and J. Semitecolos, *Physical Review A* **63**, 022117 (2001).
- [13] S. Massar, D. Bacon, N. J. Cerf, and R. Cleve, *Phys. Rev. A* **63**, 052305 (2001).
- [14] A. Rauschenbeutel, G. Nogués, S. Osnaghi, P. Bertet, M. Brune, J.-M. Raimond, and S. Haroche, *Science* **288**, 2024 (2000).
- [15] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, *Nature* **403**, 515 (2000).
- [16] R. J. Nelson, D. G. Cory, and S. Lloyd, *Physical Review A* **61**, 022106 (2000).
- [17] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, et al., *Nature* **404**, 256 (2000).
- [18] L.-M. Duan, *Physical Review Letters* **88**, 170402 (2002).