Simulating Maximal Quantum Entanglement without Communication

Cerf, N. J.; Gisin, Nicolas; Massar, S.; Popescu, S.

How to cite

CERF, N. J. et al. Simulating Maximal Quantum Entanglement without Communication. In: Physical review letters, 2005, vol. 94, n° 22. doi: 10.1103/PhysRevLett.94.220403

This publication URL: https://archive-ouverte.unige.ch/unige:36755
Publication DOI: 10.1103/PhysRevLett.94.220403

Simulating Maximal Quantum Entanglement without Communication

N. J. Cerf
Centre for Quantum Information and Communication, Ecole Polytechnique, CP 165/59, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium

N. Gisin
GAP-Optique, University of Geneva, 20 rue de l'Ecole-de-Médecine, CH-1211 Geneva, Switzerland

S. Massar
Laboratoire d'Information Quantique and Centre for Quantum Information and Communication, Ecole Polytechnique, CP 165/59, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium

S. Popescu
H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom and Hewlett-Packard Laboratories, Stoke Gifford, Bristol BS12 6QZ, United Kingdom
(Received 14 October 2004; published 7 June 2005)

It is known that all causal correlations between two parties which output each 1 bit, a and b, when receiving each 1 bit, x and y, can be expressed as convex combinations of local correlations (i.e., correlations that can be simulated with local random variables) and nonlocal correlations of the form $a + b = xy \bmod 2$. We show that a single instance of the latter elementary nonlocal correlation suffices to simulate exactly all possible projective measurements that can be performed on a maximally entangled state of two qubits, with no communication needed at all. This elementary nonlocal correlation thus defines some unit of nonlocality, which we call a *nl* bit.

DOI: 10.1103/PhysRevLett.94.220403 PACS numbers: 03.65.Ud, 03.67.-a

The importance of quantum entanglement is by now widely appreciated [1]. Historically, entanglement has first been viewed mainly as a source of paradoxes, most noticeably the Einstein-Podolsky-Rosen (EPR) paradox, which is at the origin of the concept of quantum nonlocality [2]. Today, however, entanglement is viewed rather as the resource that makes quantum information science so successful [3–5]. Indeed, based on entanglement, various informational tasks become feasible while they would be impossible using classical physics only.

Following this new trend in quantum information science, a growing community of physicists and computer scientists has started to investigate the resource "entanglement." Questions, such as how to manipulate it, e.g., how to concentrate or dilute it [6], or how to transform it into secret bits [7,8], were addressed. Also, a unit of entanglement has been identified, named e bit; it consists of a pair of maximally entangled qubits, e.g., a singlet as used in Bohm's version of the EPR paradox. A few years ago, connections with communication complexity started to be studied [9], with questions like how much classical communication is required to simulate an e bit?

Simulating an e bit means the following. Two parties, Alice and Bob, each receive a normalized vector $\vec{\nu}_A$ and $\vec{\nu}_B$ that characterizes their measurement on the Poincaré sphere, and each has to output a bit, A and B [10]; see Fig. 1. The statistics of the output bits should exactly reproduce the quantum predictions for all values of $\vec{\nu}_A$ and $\vec{\nu}_B$ if Alice and Bob were actually sharing a singlet state $(|01\rangle - |10\rangle)/\sqrt{2}$. For instance, if the vectors are antiparallel, $\vec{\nu}_A = -\vec{\nu}_B$, the output bits should always be equal, $A = B$. From Bell's theorem, we know that it is impossible to simulate a singlet without any communication. This is so even if one assumes that both parties share local hidden variables or, in modern terminology, local randomness (that is, they share an infinite list of random bits λ_j). Of course, if an unlimited amount of communication is allowed, then Alice could simply send her measurement setting $\vec{\nu}_A$ to Bob with arbitrary precision, so the simulation of a singlet would become straightforward. But whether such an unlimited amount of communication is

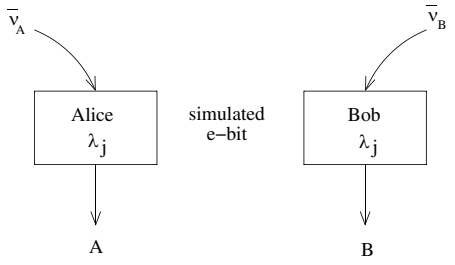

FIG. 1. Principle of e-bit simulation. The statistics of the output bits A and B should coincide with that predicted by quantum physics for the measurements defined by $\vec{\nu}_A$ and $\vec{\nu}_B$. The λ_j denote random data that Alice and Bob can share beforehand, when they jointly agree on a strategy. The inputs $\vec{\nu}_A$ and $\vec{\nu}_B$ are given to Alice and to Bob, respectively, after they separate. Note that each party is oblivious of the other party's input.

necessary was unknown. First answers to this question were given by Brassard, Cleve, and Tapp [11] in Montreal, and by Steiner [12] from the NSA. The Canadian group showed that, quite surprisingly, 8 bits of communication suffice for a perfect (analytic) simulation of the quantum predictions. Steiner, followed by [13], showed that if one allows the number of bits to vary from one instance to another, then 2 bits suffice on average. It was also shown that, if many singlets must be simulated in parallel, then block coding may be used to reduce the number of communicated bits to 1.19 bits on average [14]. A few years later, Toner and Bacon [15] improved on these results and showed that a single bit of communication suffices for perfect simulation of a singlet (again, with block coding, the communication may be reduced slightly below 1 bit per singlet).

Independently of the above developments, Popescu and Rohrlich raised the following question: can there be stronger correlations than the quantum mechanical correlations that remain causal (i.e., that do not allow signaling) [16]? Recall that the quantum correlations violate the Bell inequality, but do not allow any faster than light signaling. Popescu and Rohrlich answered by exhibiting a conceptual machine that does not allow signaling, yet violates the Clauser-Horne-Shimony-Holt (CHSH) [17] inequality more than quantum mechanics. They concluded by wondering why Nature is not *maximally* nonlocal, where this maximum would be limited only by the no-signaling constraint.

In this Letter, we push this investigation even further by showing that a maximally entangled (singlet) state *can* actually be perfectly simulated by using one instance of this nonlocal Popescu-Rohrlich (PR) machine and *no* communication at all. Since, as we shall see, one instance of the PR machine is a weaker resource than 1 bit of communication, this is the strongest known result today on entanglement simulation.

Nonlocal PR machine.—The nonlocal PR machine works as follows; see Fig. 2. It admits two input bits x and y, and yields two output bits a and b. The bits x and a are in Alice's hands, while y and b are on Bob's side. The machine is such that a and b are correlated according to the simple relation (equality modulo 2):

$$a + b = xy. \tag{1}$$

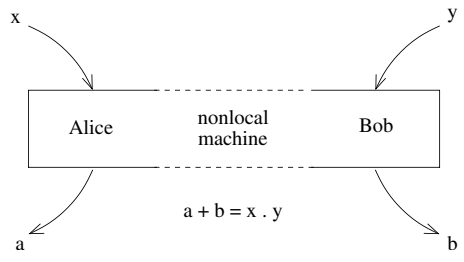

FIG. 2. Scheme of the nonlocal PR machine, where x, y and a, b denote the input and output bits, respectively.

Marginally, a and b are unbiased random bits. For example, if $x = y = 0$, then the outputs are random but identical bits: $a = b = 0$ or $a = b = 1$ with equal probabilities $1/2$. This implies that the PR machine cannot be used to signal: since the output a is locally random, its value cannot convey any information about the input y of the other party, and conversely. This machine is such that the CHSH inequality is violated by the algebraic maximum value of 4, while quantum correlations achieve at most $2\sqrt{2}$ [18]. (Remember that with shared randomness only, the maximum allowed value in a local theory is 2.) To see this, let us change the bit values 0 and 1 to the values ± 1 traditionally used in Bell inequalities. Define $a' = 1 - 2a$ and $b' = 1 - 2b$ and note that

$$a' \cdot b' = \begin{cases} 1 & \text{if } a + b = 0 \bmod 2, \\ -1 & \text{if } a + b = 1 \bmod 2. \end{cases} \tag{2}$$

Denoting by E the expectation value, the CHSH inequality reads $E(a' \cdot b'|x = 0, y = 0) + E(a' \cdot b'|x = 0, y = 1) + E(a' \cdot b'|x = 1, y = 0) - E(a' \cdot b'|x = 1, y = 1) = 4 \leq 2$. The violation of the CHSH inequality implies that this PR machine is nonlocal (even more than quantum physics), so that it cannot be simulated with local variables. Yet, it is causal, like quantum mechanics.

Let us emphasize that the PR machine is, up to elementary symmetries such as bit flips, the unique binary causal *maximally* nonlocal machine. Indeed, it can be shown that all binary causal correlations can be expressed as convex combinations of local machines (i.e., those that can be simulated with local random variables) and maximally nonlocal PR machines [19,20]. The PR machines also have the surprising property that, given an unlimited supply of them, any communication complexity problem can be solved with a single bit of communication [21]. In this sense, the PR machine is a very useful conceptual tool, although it should not be viewed as an actual physical device.

Finally, note that it is straightforward to simulate a PR machine with shared randomness (i.e., local hidden variables) augmented by 1 bit of communication: the hidden variable λ should then be a random unbiased bit, $a = \lambda$, and x should be communicated by Alice to Bob who should output $b = xy + \lambda \bmod 2$. But the converse is false: a PR machine cannot be used to communicate since it is causal. Therefore, the PR machine is a strictly weaker resource than a bit of communication, that is

$$1\ nl \text{ bit} \prec 1 \text{ bit (supraluminal communication)}, \tag{3}$$

where we have denoted as nl bit the unit of nonlocal correlations effected by the PR machine.

Simulation of a singlet with a nonlocal PR machine.—We now show that any projective measurements on a singlet can be perfectly simulated using a single instance of this nonlocal PR machine, with no communication being necessary. As a consequence of (3), this is a stronger result than the simulation of a singlet with one communicated bit

[15]. This result may appear straightforward at first sight since the PR correlations are stronger than the quantum correlations. Note, however, that we can simulate an infinite number of possible measurements, while the PR machine has only one input bit on each side. Consider that Alice and Bob shave a nonlocal PR machine as well as shared randomness in the form of pairs of normalized vectors $\vec{\lambda}_1$ and $\vec{\lambda}_2$, randomly and independently distributed over the Poincaré sphere. Denote $\vec{\nu}_A$ and $\vec{\nu}_B$ the vectors that determine Alice and Bob measurements, respectively.

The model goes as follows. Alice inputs

$$x = \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_1) + \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_2) \tag{4}$$

into the machine, where

$$\mathrm{sgn}\,(x) = \begin{cases} 1 & \text{if } x \geq 0, \\ 0 & \text{if } x < 0. \end{cases} \tag{5}$$

(Here and from now on, all equalities involving bits are taken modulo 2.) She then receives the bit a out of the machine, and outputs

$$A = a + \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_1) \tag{6}$$

as the *simulated* measurement outcome. Similarly, Bob inputs

$$y = \mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_+) + \mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_-) \tag{7}$$

into the machine, where $\vec{\lambda}_\pm = \vec{\lambda}_1 \pm \vec{\lambda}_2$, receives b out of the machine, and then outputs

$$B = b + \mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_+) + 1. \tag{8}$$

Note that since the machine's outputs a and b are random unbiased bits, the simulated measurement outcomes A and B are equally random, exactly as for actual measurements on a singlet. But the outputs a and b are correlated according to relation (1); hence A and B are also correlated. The surprising and interesting result is that this correlation is precisely the one predicted by quantum mechanics for the singlet state.

Theorem.

$$E(A + B|\vec{\nu}_A, \vec{\nu}_B) = \frac{1 + \vec{\nu}_A \vec{\nu}_B}{2}. \tag{9}$$

Proof: First, compute

$$\begin{aligned} A + B &= a + b + \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_1) + \mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_+) + 1 \\ &= xy + \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_1) + \mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_+) + 1 \\ &= z + \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_1) + \mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_+) + 1, \end{aligned} \tag{10}$$

where

$$\begin{aligned} z = &[\mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_1) + \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_2)] \\ &\times [\mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_+) + \mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_-)]. \end{aligned} \tag{11}$$

Next, note that (10) corresponds precisely to the 1-bit communication model [15]. Indeed, in this model, Alice outputs $A = \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_1)$, communicates the bit $c = \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_1) + \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_2)$ to Bob who outputs $B = (1 - c)\,\mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_+) + c\,\mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_-) + 1$. The latter can be reexpressed as $B = z + \mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_+) + 1$, so that $A + B = z + \mathrm{sgn}(\vec{\nu}_A \cdot \vec{\lambda}_1) + \mathrm{sgn}(\vec{\nu}_B \cdot \vec{\lambda}_+) + 1$. Thus, since the expressions for $A + B$ in our model and the 1-bit communication model are identical and since the latter model satisfies (9), so does our model [22]. Q.E.D.

Analogue of entanglement monogamy: the nonlocal PR machine cannot be shared.—Given the analogy between the entanglement contained in a singlet (1 *e* bit) and the nonlocal but causal correlations produced by the PR machine (1 *nl* bit), it is tempting to investigate how deep this analogy can be pushed. One of the key features of entanglement is its *monogamy* [1]. By this one means that if a quantum system A is strongly entangled with another system B, then A cannot simultaneously share much entanglement with any third system C. This property is, for example, at the basis of the quantum no-cloning theorem [23], the monogamy of CHSH inequalities [24], or the security of quantum cryptography [25]. We shall see that the exact same property holds for causal nonlocal machines. This can also be viewed as a consequence of the fact that the PR machine is an extremal causal machine (it cannot be obtained as a mixture of other causal machines); see [20] Sec. IIID.

First, let us summarize the argument of [23] underlying the monogamy of entanglement in order to emphasize the analogy with our result for causal nonlocal machines. Consider that Alice and Bob share a pair of maximally entangled qubits. Suppose that Bob is able to perfectly duplicate his qubit and make two clones (one that he keeps for himself, and the other one that he passes to Charles), so that Alice's qubit is now part of a singlet state both with Bob and Charles. Then, by measuring her qubit either in the computational basis or in the dual basis, Alice would prepare the 2-qubit system shared by Bob and Charles in two distinguishable mixtures, which would allow instantaneous signaling between Alice and Bob/Charles. Hence, perfect cloning is impossible, and entanglement must be monogamous. Now, coming back to the monogamy of

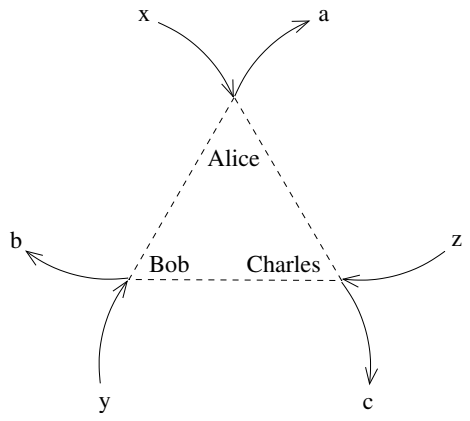

FIG. 3. Scheme of a 3-party nonlocal machine.

causal nonlocal machines, suppose that Alice holds the two halves of two PR machines, one shared with Bob, the other one shared with Charles (see Fig. 3). Denote by z and c Charles's input and output bits. One has

$$a + b = xy \quad \text{and} \quad a + c = xz. \tag{12}$$

Therefore, we have $b + c = x(y + z)$. Assume now that Bob and Charles sit next to each other, at a long distance from Alice. Then if Bob enters $y = 0$ and Charles enters $z = 1$ in their respective machines, they have $b + c = x$. This means that, by checking whether their outputs are equal or not, Bob and Charles can know instantaneously whether Alice entered $x = 0$ or $x = 1$ into the machine. Such a tripartite PR machine would thereby provide a means for supraluminal signaling between Alice and Bob or Charles; hence, it cannot exist, and causal nonlocal machines must be monogamous.

Conclusion.—Quantum nonlocality is one of the most important and amazing discoveries of the 20th century physics. It took a long time to be appreciated, and actually it is still believed to contain deep mysteries. However, today, with the progress in quantum information science, entanglement has become much better understood. Probably its most remarkable manifestation is quantum teleportation [26], a protocol that allows one to transport the characteristics of an object embedded in some energy and matter localized ''here'' to another piece of energy and matter located at a distance. In this Letter, we contributed to ''disentangle'' the nonlocality inherent to quantum mechanics into its elementary constituent, a *unit of nonlocality* or *nl* bit. Surprisingly, the quantum nonlocality of a singlet boils down to a rather simple machine, encapsulated by relation (1). We showed that one instance of this nonlocal machine is sufficient to perfectly simulate a singlet. Since this machine defines a resource that is strictly weaker than any communication while it is sufficient to simulate a singlet, we have in short

$$1\ e \text{ bit (simulation of)} \prec 1\ nl \text{ bit} \prec 1 \text{ bit}. \tag{13}$$

If we assume that Nature is sparing with resources, it is therefore tempting to conclude that, conceptually, it may use something like these nonlocal machines. This conclusion should be understood within the broader perspective of our general research program aiming at a better understanding of quantum nonlocality. This goal is achieved first by decomposing nonlocality into elementary constituents such as the PR machine, and next by considering quantum correlations as a particular subclass of the wider class of all nonsignaling correlations. In this way, it should be possible to study quantum correlations from an ''external'' viewpoint, i.e., to see quantum physics from a wider conceptual frame and answer questions about its limitations instead of the traditional questions about its differences with classical local physics.

We acknowledge financial support from the EU under Project RESQ (IST-2001-37559), from the Communauté Française de Belgique under Grant No. ARC 00/05-251, and from the IUAP program of the Belgian government under Grant No. V-18.

[1] B. M. Terhal, M. M. Wolf, and A. C. Doherty, Phys. Today **56**, No. 4, 46–52 (2003).
[2] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy* (Cambridge University Press, Cambridge, 1987).
[3] H. K. Lo, S. Popescu, and T. P. Spiller, *Introduction to Quantum Computation and Information* (World Scientific, Singapore, 1998).
[4] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information* (Springer-Verlag, Berlin, 2000).
[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[6] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[7] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[8] A. Acin, L. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003); **94**, 020501 (2005).
[9] For a survey, see G. Brassard, Found. Phys. **33**, 1593 (2003).
[10] We adopt the computer science terminology: bit values 0 and 1 instead of the spin values $\pm\frac{1}{2}$ or the values ± 1 often used in the context of Bell inequalities.
[11] G. Brassard, R. Cleve, and A. Tapp, Phys. Rev. Lett. **83**, 1874 (1999).
[12] M. Steiner, Phys. Lett. A **270**, 239 (2000).
[13] B. Gisin and N. Gisin, Phys. Lett. A **260**, 323 (1999).
[14] N. J. Cerf, N. Gisin, and S. Massar, Phys. Rev. Lett. **84**, 2521 (2000).
[15] B. F. Toner and D. Bacon, Phys. Rev. Lett. **91**, 187904 (2003).
[16] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994); see also quant-ph/9709026.
[17] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[18] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).
[19] B. S. Cirel'son, Hadronic J. Suppl. **8**, 329 (1993).
[20] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).
[21] W. van Dam, Ph.D. thesis, University of Oxford, 2000, available at http://web.mit.edu/vandam/www/publications.html.
[22] Note that, conditionally on $\vec{\lambda}_1$ and $\vec{\lambda}_2$, the bit c that is communicated in the model of [15] is not equiprobable. Therefore, by using block coding, less than 1 bit must be communicated on average to simulate a singlet. In our model, this translates into the fact that we do not fully use the nonlocality of the PR machine to simulate a singlet.
[23] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[24] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001).
[25] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[26] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).