PHYSICAL REVIEW LETTERS

Nonlocality Distillation and Postquantum Theories with Trivial Communication Complexity

Nicolas Brunner* and Paul Skrzypczyk

H.H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol, BS8 1TL, United Kingdom

We first present a protocol for deterministically distilling nonlocality, building upon a recent result of Forster *et al.* [Phys. Rev. Lett. **102**, 120401 (2009)]. Our protocol, which is optimal for two-copy distillation, works efficiently for a specific class of postquantum nonlocal boxes, which we term correlated nonlocal boxes. In the asymptotic limit, all correlated nonlocal boxes are distilled to the maximally nonlocal box of Popescu and Rohrlich. Then, taking advantage of a result of Brassard *et al.* [Phys. Rev. Lett. **96**, 250401 (2006)] we show that all correlated nonlocal boxes make communication complexity trivial, and therefore appear very unlikely to exist in nature. Astonishingly, some of these nonlocal boxes are arbitrarily close to the set of classical correlations. This result therefore gives new insight to the problem of why quantum nonlocality is limited.

By performing measurements on an entangled quantum state, two distant observers can establish correlations that are nonlocal, in the sense of violating a Bell inequality [1]. The nonlocality of these correlations is what makes them so powerful for processing information. Nevertheless quantum nonlocality is bounded, as found by Tsirelson [2]. In a seminal paper, Popescu and Rohrlich [3] showed that, surprisingly, this bound is not a consequence of relativity, i.e., there exist correlations respecting the no-signaling principle that are more nonlocal than those of quantum mechanics. Identifying what physical principle limits quantum nonlocality is an important problem in the foundations of quantum mechanics.

Recently, it was suggested that Tsirelson's bound could be a consequence of the information-theoretic properties of general nonsignalling theories [4–6], and several works underwent the task of demonstrating a separation between quantum mechanics and postquantum theories. In particular, van Dam [7] showed that the availability of Popescu-Rohrlich (PR) boxes [3,8], the paradigmatic nonlocal box, makes communication complexity trivial, while quantum mechanics does not [9]. More generally, it is strongly believed that theories in which communication complexity is trivial are very unlikely to exist. The result of [7] was subsequently extended by Brassard *et al.* [10], to a set of postquantum models known as isotropic nonlocal boxes. However a gap subsisted, in the sense that their proof applied only to isotropic boxes violating the Clauser-Horne-Shimony-Holt (CHSH) [11] inequality by more than $\mathcal{B}_{cc} \equiv 4\sqrt{2/3} \approx 3.266$; whereas quantum correlations are limited by Tsirelson's bound $\mathcal{B}_Q \equiv 2\sqrt{2} \approx 2.828$. Moreover, Linden *et al.* [12] showed that all postquantum isotropic boxes allow for nonlocal computation, thus indicating the first tight separation with quantum correlations. Finally, Tsirelson's bound was also found to appear (in a very unexpected way) in the study of the

dynamical process of nonlocality swapping [13,14], and in theories with relaxed uncertainty relations [15].

From a more general perspective, the problem of finding why quantum nonlocality is bounded does not reduce only to recovering Tsirelson's bound, but more generally to recovering the full boundary of the quantum set of correlations [16,17]. Indeed it is not so that all correlations below Tsirelson's bound are attainable in quantum mechanics (see Fig. 1); in fact there exist postquantum correlations that are arbitrarily close to the set of classical correlations. Again, it is a very natural question to ask why such correlations would be unlikely to exist in nature.

In the present Letter, we partially answer this question by showing that a particular class of postquantum correlations, which we term "correlated nonlocal boxes", make communication complexity trivial. Astonishingly, some of these correlated nonlocal boxes give an arbitrarily small
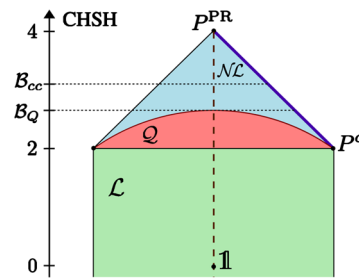

FIG. 1 (color online). The set of quantum nonlocal correlations $\mathcal{Q}$ is a strict subset of the correlations constrained solely by the nonsignaling principle $\mathcal{NL}$. In particular, there are postquantum correlations above, but also below Tsirelson's bound $\mathcal{B}_Q = 2\sqrt{2}$. Postquantum correlations violating the CHSH inequality by more than $\mathcal{B}_{cc} \approx 3.266$, are very unlikely to exist, since they make communication complexity trivial. Here we show that a similar conclusion holds for correlated nonlocal boxes (bold line). The dashed vertical line represents isotropic nonlocal boxes.

160403-1

violation of the CHSH inequality, and are arbitrarily close to the set of classical and quantum correlations. To demonstrate this result we construct a protocol for deterministically distilling nonlocality.

We build upon a recent breakthrough of Forster *et al.* [18], who presented the first nonlocality distillation protocol. The key element in their study was to look beyond isotropic boxes [19,20]. However, since their protocol can distill only up to CHSH = 3, it does not allow one to reach the bound $\mathcal{B}_{cc}$. Here we present a protocol that distills any correlated nonlocal box (in the asymptotic limit) to the maximally nonlocal box, i.e., to the PR box (CHSH = 4). Thus our protocol, which happens to be optimal for two-copy distillation, can distill above the bound $\mathcal{B}_{cc}$ and therefore implies that all correlated nonlocal boxes collapse communication complexity.

Preliminaries.—Our study focuses on the case of the CHSH scenario, which we will describe here in terms of nonlocal boxes. Two distant parties, Alice and Bob, share a nonlocal box. Each party is allowed to input one bit into the box and gets one output bit: Alice inputs $x \in \{0, 1\}$ and gets outcome $a \in \{0, 1\}$; Bob inputs $y \in \{0, 1\}$ and gets outcome $b \in \{0, 1\}$. Every nonlocal box is then characterized by a set of 16 joint probabilities $P(ab|xy)$. Here we will focus on the situation where the output bits a, b are unbiased.

The PR box is characterized by the following probability distribution:

$$P^{\mathrm{PR}}(ab|xy) = \begin{cases} \frac{1}{2} & \text{if } a \oplus b = xy \\ 0 & \text{otherwise} \end{cases}, \qquad (1)$$

where $\oplus$ is addition modulo 2. Moreover we will also consider the "correlated local state", for which the outputs are always perfectly correlated (independent of the inputs), i.e.,

$$P^{c}(ab|xy) = \begin{cases} \frac{1}{2} & \text{if } a \oplus b = 0 \\ 0 & \text{otherwise} \end{cases}. \qquad (2)$$

Next, we will mainly focus on the family of "correlated nonlocal boxes", defined as follows:

$$P^{\mathrm{PR}}_{\epsilon} = \epsilon P^{\mathrm{PR}} + (1 - \epsilon)P^{c}, \qquad (3)$$

where $0 \leq \epsilon \leq 1$. The box $P^{\mathrm{PR}}_{\epsilon}$ has a CHSH value of $\mathrm{CHSH}_i = 2(\epsilon + 1)$. Here the CHSH polynomial is given by $E_{00} + E_{01} + E_{10} - E_{11}$, where $E_{xy} = P(a = b|xy) - P(a \neq b|xy)$ is the correlator for the pair of measurements x, y.

Distillation protocol.—Now we present a nonlocality distillation protocol that works deterministically for correlated nonlocal boxes (3). More precisely our protocol takes two copies of any box $P^{\mathrm{PR}}_{\epsilon}$ with $0 < \epsilon < 1$ to a correlated nonlocal box $P^{\mathrm{PR}}_{\epsilon'}$ with $\epsilon' > \epsilon$, thus distilling nonlocality. Moreover in the asymptotic regime of many copies, any box $P^{\mathrm{PR}}_{\epsilon}$ with $\epsilon > 0$ is distilled arbitrarily close to the PR box. This protocol is optimal for deterministic two-copy distillation.

The protocol works as follows (see Fig. 2). Alice and Bob share two boxes. Let us denote x_i the value that Alice inputs into box i, and similarly y_j the value Bob inputs into box j. The output bits of box number k are then denoted a_k, b_k. Alice proceeds as follows: $x_1 = x$, $x_2 = xa_1$, and she outputs finally $a = a_1 \oplus a_2$. Bob proceeds in a similar way: $y_1 = y$, $y_2 = yb_1$, and he outputs finally $b = b_1 \oplus b_2$.

Now we prove that the protocol distills two copies of any box $P^{\mathrm{PR}}_{\epsilon}$ with $0 < \epsilon < 1$. The initial two box state is

$$P^{\mathrm{PR}}_{\epsilon} P^{\mathrm{PR}}_{\epsilon} = \epsilon^2 P^{\mathrm{PR}} P^{\mathrm{PR}} + \epsilon(1 - \epsilon)(P^{\mathrm{PR}} P^{c} + P^{c} P^{\mathrm{PR}})$$
$$+ (1 - \epsilon)^2 P^{c} P^{c}. \qquad (4)$$

Let us now compute the final box, after the above distillation protocol has been applied. It is convenient to proceed step by step. The notation $P_i P'_i \rightarrow P_f$ means that the protocol takes two initial boxes, P_i and P'_i, to one copy of the final box P_f. (i) $P^{\mathrm{PR}} P^{\mathrm{PR}} \rightarrow P^{\mathrm{PR}}$. For the first box we have $a_1 \oplus b_1 = xy$, implying $b_1 = a_1 \oplus xy$. For the second box, we have $a_2 \oplus b_2 = xa_1 yb_1 = xya_1(a_1 \oplus xy) = 0$. So the outputs satisfy the relation $a \oplus b = a_1 \oplus a_2 \oplus b_1 \oplus b_2 = xy$. (ii) $P^{\mathrm{PR}} P^{c} \rightarrow P^{\mathrm{PR}}$. For the first box we have $a_1 \oplus b_1 = xy$. For the second box we have $a_2 \oplus b_2 = 0$ independent of the inputs. So finally the outputs satisfy $a \oplus b = xy$. (iii) $P^{c} P^{\mathrm{PR}} \rightarrow \frac{1}{2}(P^{\mathrm{PR}} + P^{c})$. For the first box we have $a_1 \oplus b_1 = 0$, implying $b_1 = a_1$. For the second box, we have $a_2 \oplus b_2 = xya_1 b_1 = xya_1$, where a_1 is random. When $a_1 = 0$, one gets $a \oplus b = 0$; when $a_1 = 1$, one gets $a \oplus b = xy$. (iv) $P^{c} P^{c} \rightarrow P^{c}$. Here we have that $a_1 \oplus b_1 = 0$ and $a_2 \oplus b_2 = 0$. Therefore $a \oplus b = 0$.

So the final box, after distillation, is given by

$$P^{\mathrm{PR}}_{\epsilon'} = \frac{\epsilon}{2}(3 - \epsilon)P^{\mathrm{PR}} + \left[1 - \frac{\epsilon}{2}(3 - \epsilon)\right]P^{c}. \qquad (5)$$

Its CHSH value is $\mathrm{CHSH}_f = 3\epsilon - \epsilon^2 + 2$. Imposing that $\mathrm{CHSH}_f > \mathrm{CHSH}_i$ implies that $\epsilon - \epsilon^2 > 0$, a condition always satisfied for $0 < \epsilon < 1$. Therefore the protocol distills any box in the family (3), as shown in Fig. 3.

Note that it is convenient to view this distillation protocol as a discrete map. Starting with 2^n copies of a box $P^{\mathrm{PR}}_{\epsilon}$, the final box $P^{\mathrm{PR}}_{\epsilon_n}$ is characterized by the parameter ϵ_n which is the nth iteration of the map

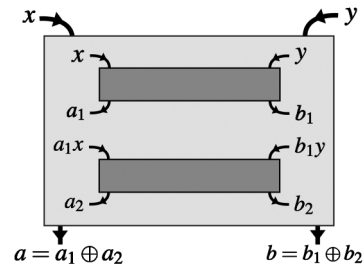$$T(\epsilon) = \epsilon' = \frac{\epsilon}{2}(3 - \epsilon). \qquad (6)$$

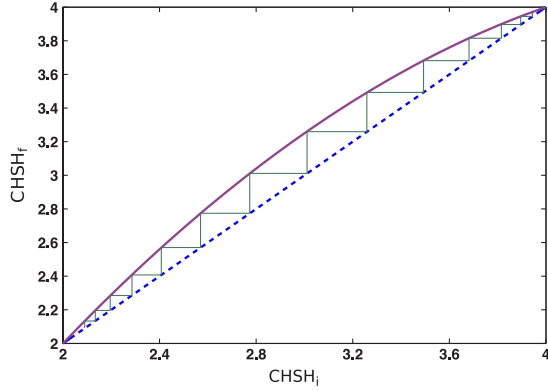FIG. 2. Protocol for two-copy deterministic nonlocality distillation.

FIG. 3 (color online). Nonlocality distillation of correlated nonlocal boxes with our protocol. The graph shows the CHSH_f value of the final box as a function of its initial CHSH_i value. The dashed straight line, $\mathrm{CHSH}_f = \mathrm{CHSH}_i$, is given as a reference. In the asymptotic regime, any nonlocal box P_ϵ^{PR} is distilled arbitrarily close to the PR box (CHSH = 4). The thin line (steps) shows the distillation of an initial box under successive iterations of the protocol.

Notably the fixed points of the map (i.e., the asymptotic behavior) are $\epsilon = 0$, i.e., the local box P^c, and $\epsilon = 1$, i.e., the PR box. The stability of both of these points can be checked by finding the eigenvalues of the Jacobian at the fixed points. Here the problem being one dimensional, this reduces to calculating $\lambda = \frac{dT}{d\epsilon}$. For the first fixed point, $\epsilon = 0$ (P^c), we find $\lambda = \frac{3}{2}$, indicating that the point is repulsive. For the second fixed point, $\epsilon = 1$ (P^{PR}), we find $\lambda = \frac{1}{2}$, indicating that the point is attractive.

In general, a distillation protocol can be viewed as a way of (classically) wiring the boxes together. In Ref. [21], a classification of all possible wirings has been given. It was shown that (consistent) wirings form a convex set, a polytope. There are 82 extremal wirings, which can be classified in five classes: deterministic, one-sided, XOR, AND, and sequential. A distillation protocol is then a choice of four wirings; one for each input of Alice and Bob. Our protocol mixes sequential and XOR wirings. We checked that it is optimal for deterministic two-copy distillation (with classical wirings). Note that the protocol of [18] is based solely upon XOR wirings, of which all are suboptimal for two-copy distillation. These protocols can distil nonlocality only up to CHSH = 3, and therefore do not allow one to reach the bound $\mathcal{B}_{cc}$.

Distillation in a section of the polytope.—In this section, we study how our distillation protocol works for more general nonlocal boxes, of the form

$$P_{\xi,\gamma}^{\mathrm{PR}} \equiv \xi P^{\mathrm{PR}} + \gamma P^c + (1 - \xi - \gamma) P^{\overline{\mathrm{PR}}} \quad (7)$$

with $\xi, \gamma \geq 0$ and $\xi + \gamma \leq 1$, and where $P^{\overline{\mathrm{PR}}}$ denotes the anti-PR box, given by the relation $a \oplus b = xy \oplus 1$. Note that the family of boxes $P_{\xi,0}^{\mathrm{PR}}$ are the isotropic PR boxes; the family of boxes $P_{\xi,1-\xi}^{\mathrm{PR}}$ are the correlated nonlocal boxes (3).

In order to compute the final box after distillation of two initial boxes $P_{\xi,\gamma}^{\mathrm{PR}}$, the following relations are needed: $P^{\mathrm{PR}} P^{\overline{\mathrm{PR}}} \to P^{\overline{\mathrm{PR}}}$, $P^{\overline{\mathrm{PR}}} P^{\mathrm{PR}} \to \frac{1}{2}(P^{\overline{\mathrm{PR}}} + P^a)$, $P^{\overline{\mathrm{PR}}} P^c \to P^{\overline{\mathrm{PR}}}$, $P^{\overline{\mathrm{PR}}} P^{\overline{\mathrm{PR}}} \to \frac{1}{2}(P^{\mathrm{PR}} + P^c)$, $P^c P^{\overline{\mathrm{PR}}} \to \frac{1}{2}(P^{\overline{\mathrm{PR}}} + P^a)$, where P^a is the anticorrelated (local) box given by $a \oplus b = 1$ for all x, y. Here it is convenient to use the nonconvex decomposition $P^a = P^{\mathrm{PR}} + P^{\overline{\mathrm{PR}}} - P^c$, since P^a lies in the plane defined by P^{PR}, $P^{\overline{\mathrm{PR}}}$ and P^c, but is not contained in their convex hull. Note that from now on we must have $-1 \leq \gamma \leq 1$ and $0 \leq \xi + \gamma \leq 1$.

The distillation protocol then implements the map

$$T_1(\xi, \gamma) = \xi' = \xi^2 + \frac{3}{2}\xi\gamma + \frac{1}{2}(1 - \xi - \gamma)$$
$$T_2(\xi, \gamma) = \gamma' = \xi^2 + 2\gamma^2 + \frac{5}{2}\xi\gamma - \frac{3}{2}(\xi + \gamma) + \frac{1}{2} \quad (8)$$

and the final box is given by $P_{\xi',\gamma'}^{\mathrm{PR}}$. This map has three fixed points: $P_{1,0}^{\mathrm{PR}} = P^{\mathrm{PR}}$, $P_{0,1}^{\mathrm{PR}} = P^c$, and $P_{1/2,0}^{\mathrm{PR}} = \mathbb{1}$, where $\mathbb{1}$ is the fully mixed box given by $a \oplus b = c$ and c is a random bit. Again, the stability of these points can be studied by computing the eigenvalues of the Jacobian at each fixed point. We find that $\mathbb{1}$ is an attractor, P^c is an unstable point, and P^{PR} is an unstable saddle point. For the correlated nonlocal boxes (3), P^{PR} is indeed an attractive point, but in all other directions it becomes repulsive. This implies that the only boxes which are distilled in the asymptotic regime are correlated nonlocal boxes. In Fig. 4, we highlight the set of boxes that are distilled in a single iteration of the protocol; note that these do not include the isotropic boxes,
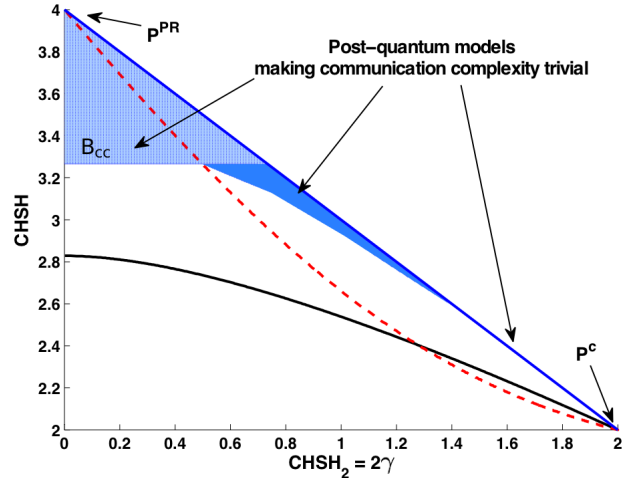

FIG. 4 (color online). Section of the nonsignaling polytope given by nonlocal boxes $P_{\xi,\gamma}^{\mathrm{PR}}$. The blue line and the shaded (blue) areas represent the set of postquantum boxes that collapse communication complexity. The area shaded in light blue was identified in [10], while the area in dark blue has been identified in the present Letter. Astonishingly, some of the correlated nonlocal boxes are arbitrarily close to the local state P^c, yet they still collapse communication complexity. Nonlocal boxes above the dashed (red) curve are distilled in one iteration of the protocol. The solid curve is the quantum boundary [16].

since they cannot be deterministically distilled by a two-copy protocol [20].

Trivial communication complexity.—It was shown in Ref. [10] that isotropic nonlocal boxes violating the CHSH inequality by more than $\mathcal{B}_{cc} \approx 3.266$ make communication complexity trivial. In fact this result also holds for nonisotropic boxes violating the CHSH inequality by more than $\mathcal{B}_{cc}$, since there exists a depolarizing protocol, found by Masanes *et al.* [22] and independently by Short [20]. This protocol, which can be performed locally and without communication, maps any nonisotropic box to an isotropic one, leaving its CHSH value unchanged. The protocol works as follows. Alice and Bob generate three random bits α, β, γ, and modify their inputs and outputs as follows: $x \rightarrow x \oplus \alpha$, $y \rightarrow y \oplus \beta$, $a \rightarrow a \oplus \beta x \oplus \alpha\beta \oplus \gamma$, $b \rightarrow b \oplus \alpha y \oplus \gamma$.

Now it is clear that any correlated nonlocal box P_ϵ^{PR} (3) violating the CHSH inequality by less than $\mathcal{B}_{cc}$ can be distilled using our protocol to a box giving a violation above this bound. Therefore, any box P_ϵ^{PR} with $\epsilon > 0$ makes communication complexity trivial. This result is indeed astonishing since a box P_ϵ^{PR} can be arbitrarily close to the local set (and consequently also to the quantum set). This shows again that the CHSH violation is an inadequate measure of nonlocality [18,23].

More generally, all nonlocal boxes $P_{\xi,\gamma}^{\mathrm{PR}}$ that can be distilled (in any number of iteration of the protocol) above $\mathcal{B}_{cc}$ make communication complexity trivial. These boxes form a region highlighted in Fig. 4. Importantly this region is not singular; it has always a finite (nonzero) width, so that it is robust against small perturbations. Indeed, the amount of tolerable perturbation depends on the CHSH value, and the system becomes more sensitive to perturbation as we get closer to the CHSH limit of 2, but even there, for small enough, yet finite, perturbations, the system is robust.

Conclusion.—We started by presenting a protocol for distilling nonlocality, that works for the family of correlated nonlocal boxes. All of these boxes, even those giving arbitrarily small violation of the CHSH inequality, can be distilled to the PR box in the asymptotic limit. Furthermore, the existence of this protocol has important implications from the point of view of communication complexity in postquantum theories: all nonlocal boxes that can be distilled above CHSH $= \mathcal{B}_{cc} \approx 3.266$ using our protocol make communication complexity trivial. Astonishingly, some of these nonlocal boxes are arbitrarily close to the set of local (and quantum) boxes, yet they still collapse communication complexity. In this sense, these boxes appear to be as nonlocal as the PR box, and therefore seem very unlikely to exist in nature. This result provides a partial answer to the question of why quantum nonlocality is also bounded below Tsirelson's bound, in regions of the polytope close to the local set of correlations.

In the future it would be interesting to find better distillation protocols, which might witness a larger set of postquantum nonlocal boxes that make communication complexity trivial. Of particular interest would be protocols based on generalized joint measurements, so-called couplers [13,14], which may enhance distillation, in analogy to the advantage given by joint measurements in quantum mechanics. Indeed the ultimate goal of this line of research would be to obtain a tight separation between quantum and any postquantum correlations, eventually leading to a new information-theoretic axiom for quantum mechanics [5].

*n.brunner@bristol.ac.uk

[1] J. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[2] B. S. Tsirelson, Lett. Math. Phys. **4**, 93 (1980).
[3] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[4] J. Barrett, Phys. Rev. A **75**, 032304 (2007).
[5] G. Brassard, Nature Phys. **1**, 2 (2005).
[6] S. Popescu, Nature Phys. **2**, 507 (2006).
[7] W. van Dam, arXiv:quant-ph/0501159.
[8] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).
[9] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, *Quantum Computing and Quantum Communication, Lecture Notes in Computer Science* (Springer-Verlag, Heidelberg, 1999), Vol. 1509.
[10] G. Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp, and F. Unger, Phys. Rev. Lett. **96**, 250401 (2006).
[11] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[12] N. Linden, S. Popescu, A. J. Short, and A. Winter, Phys. Rev. Lett. **99**, 180502 (2007).
[13] P. Skrzypczyk, N. Brunner, and S. Popescu, Phys. Rev. Lett. **102**, 110402 (2009).
[14] P. Skrzypczyk and N. Brunner, arXiv:0812.0758.
[15] G. Ver Steeg and S. Wehner, arXiv:0811.3771.
[16] B. S. Tsirelson, J. Sov. Math. **36**, 557 (1987); L. Landau, Found. Phys. **18**, 449 (1988); L. Masanes, arXiv:quant-ph/0309137.
[17] M. Navascues, S. Pironio, and A. Acin, Phys. Rev. Lett. **98**, 010401 (2007).
[18] M. Forster, S. Winkler, and S. Wolf, Phys. Rev. Lett. **102**, 120401 (2009).
[19] D. D. Dukaric and S. Wolf, arXiv:0808.3317.
[20] A. J. Short, arXiv:0809.2622.
[21] A. J. Short, S. Popescu, and N. Gisin, Phys. Rev. A **73**, 012101 (2006).
[22] L. Masanes, A. Acin, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).
[23] A. A. Méthot and V. Scarani, Quantum Inf. Comput. **7**, 157 (2007); A. Cabello and J.-A. Larsson, Phys. Rev. Lett. **98**, 220402 (2007); N. Brunner, N. Gisin, V. Scarani, and C. Simon, Phys. Rev. Lett. **98**, 220403 (2007).