PHYSICAL REVIEW A **80**, 040103(R) (2009)

Recovering part of the boundary between quantum and nonquantum correlations from information causality

Jonathan Allcock,[1,*] Nicolas Brunner,[2] Marcin Pawlowski,[3] and Valerio Scarani[4]
[1]*Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*
[2]*H.H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom*
[3]*Institute of Theoretical Physics and Astrophysics, University of Gdansk, 80-952 Gdansk, Poland*
[4]*Centre for Quantum Technologies and Department of Physics, National University of Singapore, 3 Science Drive 2, 117543 Singapore, Singapore*

(Received 16 July 2009; published 14 October 2009)

Recently, the principle of information causality has appeared as a good candidate for an information-theoretic principle that would single out quantum correlations among more general nonsignaling models. Here, we present results going in this direction, namely, we show that part of the boundary of quantum correlations actually emerges from information causality.

DOI: 10.1103/PhysRevA.80.040103 PACS number(s): 03.65.Ud

I. INTRODUCTION

Nonlocality is a central feature of quantum mechanics (QM) and a powerful resource for processing information. However, as Tsirelson [1] first proved, the amount of nonlocality allowed by QM is limited. In a seminal paper, Popescu and Rohrlich (PR) [2] showed that this limitation is not a consequence of relativity. Indeed, there exist theories which are more nonlocal than QM yet do not allow for superluminal signaling. Identifying the physical principles underlying the limits to quantum nonlocality is now a central problem in foundational QM.

Recently, several works have studied the physical and information-theoretic properties of general nonsignaling models. Surprisingly, it appears that these models have numerous properties in common with QM, such as no-cloning [3,4], no-broadcasting [5], monogamy of correlations [3], and information-disturbance trade-offs [6]. General nonsignaling models also allow for secure key distribution [7,8] as well as quantumlike dynamical processes [9]. Therefore, none of these properties, usually thought of as being typically quantum, are useful for separating quantum from postquantum correlations.

On the other hand, it is known that some particular postquantum correlations have extremely powerful communication properties. For instance, the availability of PR boxes—the paradigmatic example of postquantum correlations—makes communication complexity trivial [10]. However, communication complexity is not trivial in QM [11], and it is strongly believed not to be trivial in nature. Therefore, correlations which collapse communication complexity, such as PR box correlations, appear unlikely to exist. More recently, a similar conclusion has been shown to hold for two classes of noisy PR boxes [12,13]. However, there is a large class of postquantum correlations for which it is still unknown whether communication complexity collapses or not.

In parallel, nonlocality has also been studied from the point of view of nonlocal computation [14]. Remarkably, here Tsirelson's bound (of quantum nonlocality) naturally appears since all postquantum correlations violating this bound offer an advantage over classical and quantum correlations. It is also known that part of the quantum boundary emerges from nonlocality swapping [9,15] (an analog of entanglement swapping), although the origin of this connection is still not understood. Finally Tsirelson's bound also appears in theories with relaxed uncertainty relations [16].

More recently, Pawlowski *et al.* [17] introduced a new physical principle, the principle of information causality (IC), which is satisfied by both classical and quantum correlations. The essence of IC is that the communication of m classical bits can cause a potential information gain of at most m bits. As is the case for nonlocal computation, Tsirelson's bound naturally emerges since all correlations exceeding Tsirelson's bound violate the principle of IC. Therefore, IC is a potential candidate for separating quantum from postquantum correlations. However, Tsirelson's bound identifies only one point on the boundary of the set of quantum correlations. There are also postquantum correlations which lie below Tsirelson's bound. Thus, while the emergence of Tsirelson's bound from IC is a remarkable feature, it is not sufficient for singling out quantum correlations. More generally, one aims at finding a principle underlying the full quantum boundary.

In the present Rapid Communication, we show that part of the quantum boundary actually emerges from IC. More precisely, we show that in two two-dimensional slices of the binary-input–binary-output nonsignaling polytope, the IC criterion analytically coincides with the quantum boundary.

The organization of the Rapid Communication is the following. In Sec. II we review the geometrical approach to nonsignaling correlations, while in Sec. III we review IC. In Sec. IV, we study the link between IC and the quantum boundary.

II. GEOMETRY OF NONSIGNALING BOXES

It will be convenient to describe bipartite nonsignaling correlations in terms of black boxes shared between two parties: Alice and Bob. Alice and Bob input variables x and y at

*jon.allcock@bristol.ac.uk

their ends of the box, respectively, and receive outputs a and b. The behavior of a given correlation box is fully described by a set of joint probabilities $P(ab|xy)$. We focus on the case of binary inputs and outputs $(a,b,x,y\in\{0,1\})$, for which

$$P(ab|xy)=\tfrac{1}{4}[1+(-1)^a C_x+(-1)^b C_y+(-1)^{a\oplus b}C_{xy}],$$

where $\oplus$ is addition modulo 2, the correlators are given by $C_{xy}=\Sigma_{a'=b'}P(a'b'|xy)-\Sigma_{a'\neq b'}P(a'b'|xy)$, and the marginals are given by $C_x=\Sigma_{b'}[P(0b'|x0)-P(1,b'|x0)]$ and $C_y=\Sigma_{a'}[P(a'0|0y)-P(a'1|0y)]$. In this case, which corresponds to the famous Clauser-Horne-Shimony-Holt (CHSH) [18] scenario, the full set of nonsignaling boxes forms an eight-dimensional polytope [19] which has 24 vertices: eight extremal nonlocal boxes and 16 local deterministic boxes. The extremal nonlocal correlations have the form

$$P_{\mathrm{NL}}^{\mu\nu\sigma}(ab|xy)=\begin{cases}\frac{1}{2} & \text{if } a\oplus b=xy\oplus\mu x\oplus\nu y\oplus\sigma\\ 0 & \text{otherwise,}\end{cases}$$

where $\mu,\nu,\sigma\in\{0,1\}$ and the canonical PR box corresponds to $\mathrm{PR}=P_{\mathrm{NL}}^{000}$. Similarly, the local deterministic boxes are described by

$$P_{\mathrm{L}}^{\mu\nu\sigma\tau}(ab|xy)=\begin{cases}1 & \text{if } a=\mu x\oplus\nu,\quad b=\sigma y\oplus\tau\\ 0 & \text{otherwise.}\end{cases}$$

The set of local boxes forms a subpolytope of the full nonsignaling polytope and has facets which correspond to Bell inequalities—here, the CHSH inequality

$$C_{00}+C_{01}+C_{10}-C_{11}\leq 2, \tag{1}$$

and its symmetries. Note that there are eight symmetries of the CHSH inequality [any odd number of terms on the left-hand side of (1) can have a minus sign], and that each CHSH inequality is violated by one of the extremal nonlocal boxes.

The set of quantum boxes, i.e., correlations obtainable by performing local measurements on a quantum state (of any dimension), is sandwiched between the local polytope and the full nonsignaling polytope. In particular, quantum correlations satisfy a variant of inequality (1), where the right-hand side is replaced with $2\sqrt{2}$, a value known as Tsirelson's bound. The quantum set is a convex body, although it is not a polytope. Thus, its boundary is described by a smooth curve. For binary inputs and outputs, Tsirelson, Landau, and Masanes (TLM) [20] (independently) derived a necessary and sufficient criterion for a set of correlators C_{xy} to admit a quantum description. In the form of Landau, C_{xy} must satisfy

$$|C_{00}C_{10}-C_{01}C_{11}|\leq\sum_{j=0,1}\sqrt{(1-C_{0j}^2)(1-C_{1j}^2)}. \tag{2}$$

However, when considering the full probability distribution (including the marginals), this criterion remains necessary but is no longer sufficient. Recently, a refinement of Eq. (2) has been derived by Navascues, Pironio, and Acin (NPA) [21]. Their work improves Eq. (2) in that it incorporates the marginals of the probability distribution. The NPA criterion reads

$$|\arcsin D_{00}+\arcsin D_{01}+\arcsin D_{10}-\arcsin D_{11}|\leq\pi, \tag{3}$$

where $D_{xy}=(C_{xy}-C_xC_y)/\sqrt{(1-C_x^2)(1-C_y^2)}$. Note that, for vanishing marginals, Eq. (3) is equivalent to Eq. (2). Note also that Eq. (3) is in general not sufficient for a probability distribution to be quantum realizable; to determine whether a probability distribution is quantum or not, one has to test a hierarchy of semidefinite programming conditions [22].

III. INFORMATION CAUSALITY

Let us now briefly review the principle of IC. The authors of [17] considered the following communication task, which is similar to random access coding [23] and oblivious transfer [24,25]. Alice and Bob, who are separated in space, have access to nonsignaling resources such as shared randomness, entanglement, or (in principle) PR boxes. Alice receives N i.i.d. random bits $\vec{a}=(a_1,a_2,\ldots,a_N)$, while Bob receives a random variable $b\in\{1,2,\ldots,N\}$. Alice then sends m classical bits to Bob, who must output a single bit β with the aim of guessing the value of Alice's bth bit a_b. Their degree of success at this task is measured by

$$I\equiv\sum_{K=1}^{N}I(a_K:\beta|b=K),$$

where $I(a_K:\beta|b=K)$ is the Shannon mutual information between a_K and β. The principle of IC states that physically allowed theories must have $I\leq m$. Indeed, it was proved in [17] that both classical and quantum correlations satisfy this condition. Moreover, suppose that Alice and Bob share arbitrary binary-input–binary-output nonsignaling correlations corresponding to conditional probabilities $P(ab|xy)$. A condition under which IC is violated was derived in [17]—based on a construction by van Dam [10] and Wolf and Wullschleger [25]—for a specific realization of the Alice-Bob channel. It goes as follows. Define P_I and P_{II},

$$\begin{aligned}P_I&=\tfrac{1}{2}[P(a\oplus b=0|00)+P(a\oplus b=0|10)]\\&=\tfrac{1}{4}[2+C_{00}+C_{10}],\\ P_{II}&=\tfrac{1}{2}[P(a\oplus b=0|01)+P(a\oplus b=1|11)]\\&=\tfrac{1}{4}[2+C_{01}-C_{11}].\end{aligned} \tag{4}$$

Then, the IC condition $(I\leq m)$ is violated for all boxes for which

$$E_I^2+E_{II}^2>1, \tag{5}$$

where $E_j=2P_j-1$. It follows from this that all nonsignaling correlations which violate Tsirelson's bound also violate IC. To see this, it suffices to consider "isotropic" correlations of the form $\alpha\mathbf{PR}+(1-\alpha)\mathbf{I}$, where $\mathbf{I}$ is the correlation box given by $P(ab|xy)=1/4$ $(\forall\ a,b,x,y)$. For such boxes, $E_1=E_2=\alpha$ and Eq. (5) is satisfied when $\alpha>1/\sqrt{2}$, which corresponds to violating Tsirelson's bound. However, as previously mentioned, there are correlations which lie below Tsirelson's bound which are nonetheless unobtainable in QM. For such correlations, it was not known whether the principle of IC singles out exactly those allowed by quantum physics. We now offer a partial answer to this question.

IV. IC AND THE QUANTUM BOUNDARY

Here, we investigate the link between IC and the set of correlations achievable in QM. We would like to determine whether the entire quantum boundary can be recovered from the principle of IC. It will be convenient to re-express condition (5) for the violation of IC in terms of the correlators C_{xy} as follows:

$$(C_{00}+C_{10})^2+(C_{01}-C_{11})^2>4. \tag{6}$$

Interestingly, this is equivalent to a violation of Uffink's quadratic inequality [26]; note that Uffink's inequality is known to be strictly weaker than the TLM criterion [27].

In the following, we compare Eq. (6) with the TLM and NPA criteria for quantumness. We shall investigate several two-dimensional slices of the nonsignaling polytope, which can be grouped into two families. More precisely, we consider noisy PR boxes of the form

$$\mathbf{PR}_{\alpha,\beta}=\alpha\mathbf{PR}+\beta\mathbf{B}+(1-\alpha-\beta)\mathbf{I}, \tag{7}$$

where $\mathbf{B}$ is an extremal nonlocal box in the first family and an extremal local deterministic box in the second. Remarkably, in the first family we find two different slices of the polytope where boxes that satisfy IC coincide analytically with the set of quantum boxes. In other words, in these slices IC exactly singles out quantum correlations in that all postquantum correlations violate IC. Note that, because of the symmetry of the polytope, it is sufficient here to focus on nonsignaling boxes violating the CHSH inequality (1), and not those which violate the seven other symmetries of CHSH; basically, a nonsignaling box can never violate more than one symmetry of CHSH.

Family 1. We first consider correlations of form (7), where $B=P_{\mathrm{NL}}^{\mu\nu\sigma}$ and $\mu\nu\sigma$ can take any values except for 000 and 001 (since these are collinear with **PR** and **I**). The corresponding correlators are given by $C_{00}=\alpha+(-1)^{\sigma}\beta$, $C_{01}=\alpha+(-1)^{\nu\oplus\sigma}\beta$, $C_{10}=\alpha+(-1)^{\mu\oplus\sigma}\beta$, and $C_{11}=-\alpha+(-1)^{\mu\oplus\nu\oplus\sigma\oplus1}\beta$.

We see from Eq. (2) that if boxes of this form are to be quantum realizable then we require that $\alpha^2+\beta^2\leq\frac{1}{2}$. Note that here the TLM criteria are necessary and sufficient for quantumness since the probability distribution given by boxes in this family has a specific form [28]. On the other hand, we see from Eq. (6) that, if $B=PR_2=P_{\mathrm{NL}}^{010}$, then IC is violated when

$$\alpha^2+\beta^2>\tfrac{1}{2}. \tag{8}$$

Thus, in this particular slice of the nonsignaling polytope, a box violates IC if and only if it is postquantum (Fig. 1). Note that here we could have chosen $B=\overline{\mathbf{PR}}_2=P_{\mathrm{NL}}^{011}$ as well.

The above proof is easily adapted to another slice. By exchanging the roles of Alice and Bob, the same can also be seen to hold in the slice where $B=PR_3=P_{\mathrm{NL}}^{100}$ (or equivalently $B=\overline{\mathbf{PR}}_3=P_{\mathrm{NL}}^{101}$).

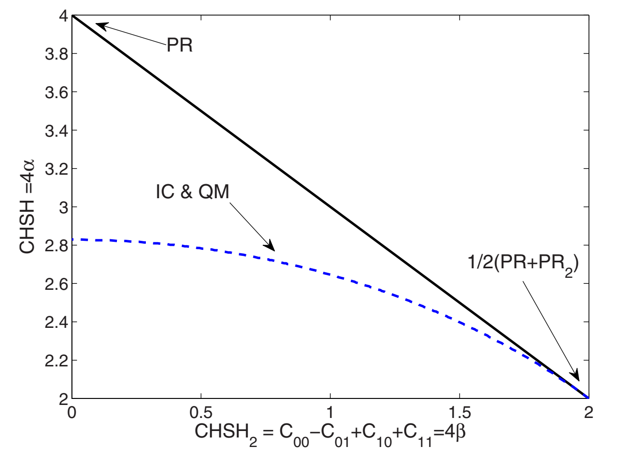

FIG. 1. (Color online) A slice of the nonsignaling polytope where correlations violate IC if and only if they are postquantum. Above the blue dashed curve, IC is violated; below, correlations are quantum realizable.

Finally, note that in the case where $B=PR_4=P_{\mathrm{NL}}^{111}$, the criterion for violating IC reduces to $\alpha>\frac{1}{\sqrt{2}}$. Thus, boxes below Tsirelson's bound are not known to violate IC in this slice (Fig. 2). We stress that this does not imply that there exist postquantum boxes lying below Tsirelson's bound which do not violate IC. The fact that boxes which satisfy Eq. (6) also violate IC follows from considering a particular strategy for using the boxes, found in [17]. It remains possible that a different strategy could be used to show that all postquantum correlations violate IC in this slice as well.

Family 2. Next, we consider correlations of form (7), where $B=P_{\mathrm{L}}^{\mu\nu\sigma\tau}$ with $\mu\sigma\oplus\nu\oplus\tau=0$; note that these are the local deterministic boxes sitting on the CHSH facet below the PR box. For simplicity, we will focus here on $B=P_{\mathrm{L}}^{0000}$. In this case, the correlators are given by $C_{00}=C_{01}=C_{10}=\alpha+\beta$, $C_{11}=\beta-\alpha$, and the marginals are given by $C_0^a=C_1^a=C_0^b=C_1^b=\beta$. It follows from Eq. (6) that IC is violated whenever

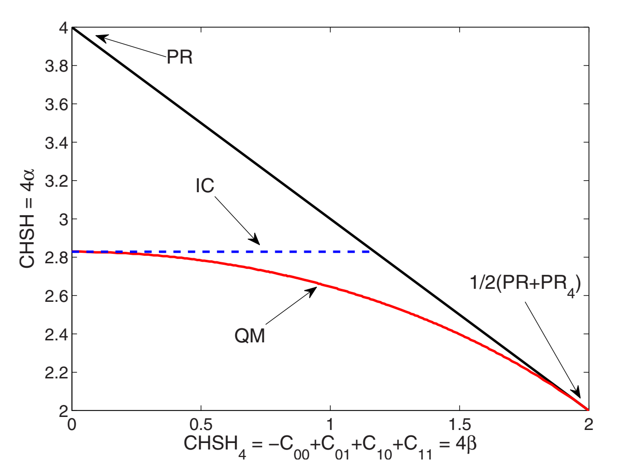

FIG. 2. (Color online) A slice of the nonsignaling polytope where postquantum boxes which lie below Tsirelson's bound (CHSH=$2\sqrt{2}$) are not known to violate IC. The red solid line is the quantum boundary.

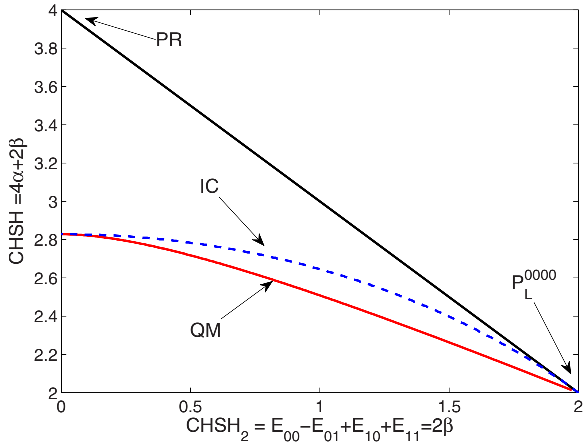

FIG. 3. (Color online) A slice of the nonsignaling polytope where IC does not single out quantum correlations. The red solid line is the upper limit on quantum correlations, as given by the NPA criteria.

$$(\alpha+\beta)^2+\alpha^2>1. \tag{9}$$

However, this does not coincide with the NPA criterion (3). Figure 3 shows clearly the discrepancy between the quantum boundary, or more precisely the upper bound given by NPA, and the IC condition (9). Let us reiterate that the bound (9) follows from a particular strategy in [17] for using boxes to violate IC. Thus, it might still be the case that a better strategy would single out quantum correlations in this particular slice.

V. CONCLUSION

We have shown that in the binary-input–binary-output nonsignaling polytope, part of the quantum boundary emerges from the principle of IC. The central question is now whether this connection can be extended to the full nonsignaling polytope, which would establish IC as the information theoretic principle singling out quantum correlations.

ACKNOWLEDGMENTS

We thank M. Seevinck for pointing out the equivalence of Eq. (6) to Uffink's inequality. J.A. acknowledges support from the Dorothy Hodgkins Foundation, N.B. from the Swiss National Science Foundation, M.P. from the EU program QAP, and V.S. from the National Research Foundation and the Ministry of Education, Singapore.

[1] B. S. Tsirelson, Lett. Math. Phys. **4**, 93 (1980).
[2] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[3] L. Masanes, A. Acin, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).
[4] J. Barrett, Phys. Rev. A **75**, 032304 (2007).
[5] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, Phys. Rev. Lett. **99**, 240501 (2007).
[6] V. Scarani *et al.*, Phys. Rev. A **74**, 042339 (2006).
[7] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[8] A. Acin, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).
[9] P. Skrzypczyk, N. Brunner, and S. Popescu, Phys. Rev. Lett. **102**, 110402 (2009).
[10] W. van Dam, e-print arXiv:quant-ph/0501159.
[11] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, *Quantum Computing and Quantum Communication*, Lecture Notes in Computer Science Vol. 1509 (Springer-Verlag, Heidelberg, 1999).
[12] G. Brassard *et al.*, Phys. Rev. Lett. **96**, 250401 (2006).
[13] N. Brunner and P. Skrzypczyk, Phys. Rev. Lett. **102**, 160403 (2009).
[14] N. Linden, S. Popescu, A. J. Short, and A. Winter, Phys. Rev. Lett. **99**, 180502 (2007).
[15] P. Skrzypczyk and N. Brunner, New J. Phys. **11**, 073014 (2009).
[16] G. Steeg and S. Wehner, Quantum Inf. Comput. **9**, 0801 (2009).
[17] M. Pawlowski *et al.*, e-print arXiv:0905.2292.
[18] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[19] J. Barrett *et al.*, Phys. Rev. A **71**, 022101 (2005).
[20] B. Tsirelson, J. Sov. Math. **36**, 557 (1987); L. Landau, Found. Phys. **18**, 449 (1988); L. Masanes, e-print arXiv:quant-ph/0309137.
[21] M. Navascues, S. Pironio, and A. Acin, Phys. Rev. Lett. **98**, 010401 (2007).
[22] S. Wehner, Phys. Rev. A **73**, 022110 (2006); M. Navascues, S. Pironio, and A. Acin, New J. Phys. **10**, 073013 (2008); A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner, *Proceedings of the IEEE Conference on Computational Complexity* (IEEE, New York, 2008), Vol. 199.
[23] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM **49**, 496 (2002).
[24] M. Rabin, Harvard Aiken Computation Laboratory Technical Report No. TR-81, 1981 (unpublished).
[25] S. Wolf and J. Wullschleger, e-print arXiv:quant-ph/0502030.
[26] J. Uffink, Phys. Rev. Lett. **88**, 230406 (2002).
[27] M. Seevinck (private communication); see also A. Cabello, Phys. Rev. A **72**, 012113 (2005).
[28] Tsirelson and Masanes [20] proved that if a given set of correlators satisfies the TLM criterion (2), there exists a probability distribution admitting a quantum description that has this set of correlators. Here, the question is whether this quantum probability distribution could have the form of correlations in family 1. This is indeed the case since any probability distribution can be brought to a form where the marginals are unbiased and the joint probabilities satisfy $P(a,b|x,y)=P(a\oplus 1,b\oplus 1|x,y)$. Importantly, this can be done by local operations without modifying the value of the correlators; Alice and Bob share a random bit α and subsequently modify their output according to $a\rightarrow a\oplus\alpha$ and $b\rightarrow b\oplus\alpha$. Thus, the TLM criterion is necessary and sufficient for quantumness in the slices of the polytope in family 1.