When Are Popescu-Rohrlich Boxes and Random Access Codes Equivalent?

Andrzej Grudka,[1] Karol Horodecki,[2] Michał Horodecki,[3] Waldemar Kłobus,[1] and Marcin Pawłowski[3]

[1] *Faculty of Physics, Adam Mickiewicz University, 61-614 Poznań, Poland*
[2] *Institute of Informatics, University of Gdańsk, 80–952 Gdańsk, Poland*
[3] *Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80–952 Gdańsk, Poland*

(Received 31 July 2013; revised manuscript received 30 June 2014; published 2 September 2014)

We study a problem of interconvertibility of two supraquantum resources: one is the so-called Popescu-Rohrlich (PR) box, which violates Clauser-Horne-Shimony-Holt inequality up to the maximal algebraic bound, and the second is the so-called random access code (RAC). The latter is a functionality that enables Bob (receiver) to choose one of two bits of Alice. It is known that a PR box supplemented with one bit of communication can be used to simulate a RAC. We ask the converse question: to what extent can a RAC can simulate a PR box? To this end, we introduce a "racbox": a box such that when it is supplemented with one bit of communication it offers a RAC. As said, a PR box can simulate a racbox. The question we raise is whether any racbox can simulate a PR box. We show that a *nonsignaling* racbox, indeed, can simulate a PR box; hence, these two resources are equivalent. We also provide an example of a signaling racbox that cannot simulate a PR box. We give a resource inequality between racboxes and PR boxes and show that it is saturated.

DOI: 10.1103/PhysRevLett.113.100401 PACS numbers: 03.65.Ta, 03.65.Ud

Introduction.—Defining quantum mechanics by some information theoretic principles has been a hot topic recently. In the seminal paper by Popescu and Rohrlich (PR) [1], it was noted that the principle of nonsignaling does not forbid the violation of Bell inequalities stronger than quantum mechanics allows. Since then, much effort has been devoted to answer the question why systems that exhibit stronger than quantum-mechanical correlations do not exist in nature. The most nonlocal systems [which violate Clauser-Horne-Shimony-Holt (CHSH) inequality maximally] are called PR boxes. They exhibit a variety of strange properties. One of them is that they trivialize a problem of communication complexity, which is impossible both in quantum and in the classical worlds. The other property is that a PR box allows for a so-called random access code (RAC). Namely, suppose that Alice has two bits and can send to Bob only one bit. Suppose further that Bob cannot communicate to Alice. Then both in the quantum and classical worlds, it is not possible that Bob can choose which bit he wants to obtain and always get the right answer. However, the probability of getting it is higher if the parties have access to quantum resources.

In classical information theory, RACs are basic primitives for cryptography [2]. In the quantum counterpart, they were a basis of the first quantum protocols of Wiesner from circa 1970 (published 1983) [3]. Rediscovered in Ref. [4], where explicit connection with the classical case was made, they were exploited for semi-device-independent cryptography [5] and randomness expansion [6,7]. They also found application in studies on foundations of quantum mechanics. RACs relation to discrete Wigner functions was studied in Ref. [8] and their entanglement-based version [9] in the derivation of the Tsirelson bound from information-theoretic principles [10].

In Ref. [10], RACs became a basis for information causality, a principle that quantifies the success of decoding the right bit by means of mutual information. This is a new possible postulate to rule out systems that exhibit supraquantum correlations, saying that the sum of mutual informations about each bit cannot exceed the number of bits that are actually communicated. There have also been other possible postulates (see e.g., Refs. [11–13]). However, for a while none of those postulates was proven to be sufficient to ensure that a given system can be reproduced by quantum mechanics.

This development urges one to further investigate supraquantum resources in order to understand why quantum mechanics rules them out. The two mentioned phenomena exhibited by a PR box (trivializing communication complexity and simulating random access code) are both of the same kind: they show that a static resource which is a PR box can simulate some dynamical resources, RAC, or the possibility of computing any function with little communication. Therefore, to have a more complete understanding of supraquantum resources, there is a need to ask a converse question: suppose we are given some functionality; can it simulate a PR box? Thus, we ask about equivalence between resources. The question of interconvertibility between given resources is basic for any theory of resources, e.g., entanglement theory [14–17], quantum communication theory [18], or thermodynamics [19–21]. Notably, following the path paved by entanglement theory, there has been research done on the interconversion of nonsignaling boxes (see, e.g., Refs. [22,23]). Our present contribution

© 2014 American Physical Society

goes beyond that: namely, we want to establish (in) equivalence between nonsignaling systems (informally called "boxes") on one hand and a "functionality" such as RAC on the other hand.

In this Letter, we concentrate on a comparison of a PR box with a RAC. As said, a PR box can simulate a "racbox" (i.e., an arbitrary box which when supplemented with one bit of communication offers a RAC). The question we raise is whether any racbox can simulate a PR box. We show that a nonsignaling racbox, indeed, can simulate a PR box; hence, these two resources are equivalent. We also provide an example of a signaling racbox that cannot simulate a PR box. We give a resource inequality between racboxes and PR boxes and show that it is saturated. Our Letter opens a new field of study: boxes that are defined by specific tasks.

PR box, random access code, and racbox.—A PR box is a bipartite system shared by two distant parties Alice and Bob. Each of the parties can choose one of two inputs: Alice $x = 0, 1$ and Bob $y = 0, 1$. The parties have two binary outputs a, b [see Fig. 1(a)]. The box is defined by a family of joint probability distributions $p(ab|xy)$ that satisfy

$$p(ab|xy) = \begin{cases} \frac{1}{2} & \text{for } a \oplus b = xy, \\ 0 & \text{else}. \end{cases} \tag{1}$$

The condition

$$a \oplus b = xy, \tag{2}$$

will be called "PR correlations."

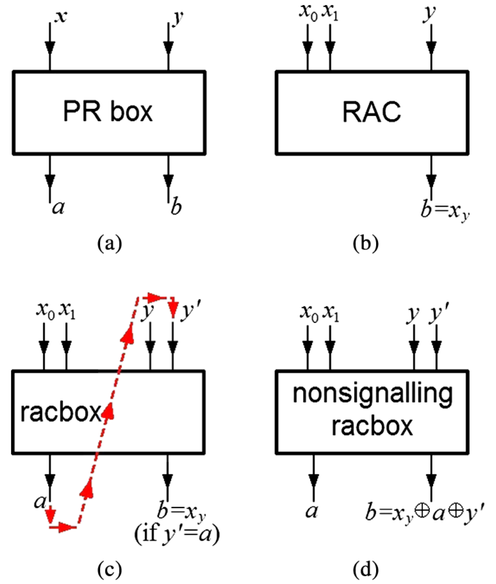

FIG. 1 (color online). (a) PR box. (b) RAC. (c) Racbox acts as RAC, provided that the input y' is equal to a. Thus, in particular, if the output a is sent to Bob and he inputs it to y' (as depicted by dashed line), then $b = x_y$. (d) Nonsignaling racbox satisfies $b = x_y \oplus a \oplus y'$.

Let us now define a RAC. This is a box which has two inputs on Alice's side (where Alice will put two bits x_0 and x_1) and no output. On Bob's side, it has an input y to decide which bit Bob wants to get, x_0 or x_1, and the output b. Such a box is a RAC when $b = x_y$ for all possible inputs [see Fig. 1(b)].

It is known [24] that a RAC can be simulated by a PR box assisted with one classical bit of communication. In this context, one may ask whether there are other boxes of that property designed for this specific task. To this end, let us define a new type of box as in the following.

Consider a box that has, in addition, an output a on Alice's side and one more input y' on Bob's side [see Fig. 1(c)], and suppose that it is nonsignaling from Bob to Alice. Such box we call racbox when the following holds: if $a = y'$, then it acts as a RAC on the rest of the outputs or inputs, i.e., $b = x_y$. When $a \neq y'$, we do not place any restrictions. A racbox is, thus, designed in such a way that when supplemented with a bit of communication, it offers a RAC.

A PR box is nonsignaling. It means that for any choice of Bob's setting, the probability distribution of his output does not depend on Alice's input and vice versa. However, in the case of a racbox, there is a freedom of defining the probability distribution associated with it as long as it can be turned into a RAC. This makes it possible to have both signaling and nonsignaling racboxes (where signaling can be possible only from Alice to Bob).

It is possible to simulate a nonsignaling racbox with a PR box as illustrated in Fig. 2(a).

Now we may ask the converse question: can we simulate a PR box using a racbox? If the answer is true, then the two resources are strictly equivalent. As we shall see, a PR box can be simulated by a nonsignaling racbox. However, we shall further present a signaling racbox that cannot simulate a PR box. Furthermore, we will derive a general resource

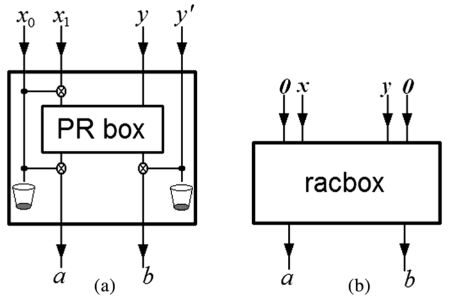

FIG. 2. (a) Simulation of a nonsignaling racbox with a PR box. (b) Simulation of a PR box with a nonsignaling racbox. We set inputs as $x_0 = 0, x_1 = x, y' = 0$, while leaving y and the outputs a and b unchanged. This simulation precisely cancels the actions of CNOT gate in the previous one so that we get a PR box again.

inequality for all racboxes and show that the signaling racbox saturates it, thus, proving that the inequality is tight, which reflects the fact that the signaling racbox can be considered a weaker resource than a nonsignaling one. Thus, all nonsignaling boxes that can perform a RAC if supplemented with 1 bit of communication are equivalent to a PR box, whereas if we allow signaling, there are boxes that still perform this functionality but cannot simulate a PR box.

PR box is equivalent to nonsignaling racbox.—First, let us characterize nonsignaling racboxes by the following lemma (for the proof, see the Supplemental Material [25]).

Lemma 1: A nonsignaling racbox for $a \neq y'$ operates as an anti-RAC; i.e., it satisfies

$$b = x_y \oplus a \oplus y'. \tag{3}$$

Below, we will show that a nonsignaling racbox can simulate a PR box [see Fig. 2(b)]. Namely, Alice inputs $x_0 = 0$, while Bob $y' = 0$. This choice is actually very natural, if one looks at the converse protocol, of simulating a racbox with a PR box in Fig. 2(a). The chosen fixed inputs regain the original PR-box; i.e., they cancel the action of CNOT gates. Thus, in our present simulation, the PR-box conditions (2) read as

$$a \oplus b = x_1 y. \tag{4}$$

Assuming that Eq. (3) holds, we proceed to show the equivalence between a PR-box and a nonsignaling racbox. The PR-box condition of Eq. (4) then reads as $a \oplus x_y \oplus a \oplus y' = x_1 y$. Recalling that in our simulation $y' = 0$, we obtain a relation

$$x_y = x_1 y, \tag{5}$$

which since in the simulation we set also $x_0 = 0$, holds for arbitrary x_1 and y (indeed, for $y = 1$ we have $x_1 = x_1$ and for $y = 0$ we have $x_0 = 0$). Therefore, our simulation, indeed, gives a PR box.

Resource inequality between a PR box and a racbox.—We show that the following inequality holds for *any* racboxes:

$$\text{racbox} + 1\text{c-bit} + 1\text{sr-bit} \geq \text{PR} + \mathcal{E}, \tag{6}$$

which means that having access to any racbox (signaling or nonsignaling), one bit of communication (c-bit), and one shared random bit (sr-bit) we can simulate a PR box and additionally obtain erasure channel ($\mathcal{E}$) with probability of erasure $\epsilon = p(y = 1)$, where $p(y = 1)$ is the probability that Bob will choose input $y = 1$.

We shall prove inequality

$$\text{RAC} + 1\text{sr-bit} \geq \text{PR} + 1\mathcal{E}, \tag{7}$$

which implies Eq. (6), since by definition racbox plus 1 bit of communication offers a RAC.

Let us note that to reproduce PR correlations (2) in the case when $y = 0$, one can use just shared randomness, since the condition says that Alice and Bob's input are the same. Thus, RAC is not used up and can be utilized to communicate the bit x_0. When $y = 1$, Bob will need to use a RAC to reproduce PR correlations, and in this case no communication will be performed.

Let us present the protocol that does the job (see Fig. 3). We denote by z the bit to be sent. Alice puts z to input x_0 and x to input x_1, while Bob leaves y unchanged. Regarding outputs, Alice and Bob use a shared random bit. When $y = 0$, Bob uses the random bit without any other action and, as said above, the PR correlations are obtained in this case. When $y = 1$, Bob performs a CNOT gate on his output b and the shared random bit with b being the control bit and shared random bit being the target bit. Let us see that again the PR correlations are reproduced. To this end, for $y = 1$ we need to have correlations when $x = 0$ and anticorrelations when $x = 1$. From the definition of a RAC, when $y = 1$, we have $b = x_1 = x$. Hence, when $x = 0$, the shared random bit is not flipped, and Alice and Bob have correlations, whereas for $x = 0$, the bit is flipped, and they have anticorrelations, as it should be. Thus, the protocol perfectly simulates a PR box.

Let us now check how good it is regarding communication. When $y = 0$, Bob's output b is equal to $x_0 = z$; hence, the message was perfectly transmitted, whereas for $y = 1$, the output is equal to x; hence, the message is lost. Thus, we obtain an erasure channel with probability of erasure $\epsilon = p(y = 1)$.

Tightness of the resource inequality.—Notice that the resource inequality of Eq. (6) is trivial for the case of a nonsignaling racbox. As we shall see, however, using a specific signaling racbox we can tighten the inequality (see Theorem 1 below).

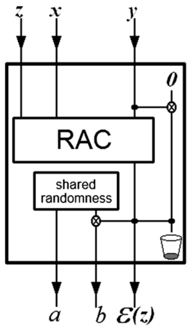

FIG. 3. A protocol for achieving resource inequality (7). The bit to be transmitted is denoted by z. $\mathcal{E}$ is the erasure channel: with probability $\epsilon = p(y = 1)$ the message is lost, whereas with probability $1 - \epsilon$ the message is delivered intact. The receiver knows which is the case. The inputs x, y and the outputs a, b satisfy Eq. (2).

We shall now present a "bad" racbox which, even though it performs its duty regarding RAC (i.e., when supplemented with a bit of communication performs RAC), cannot simulate a PR box. Such a racbox is defined as follows: when $a = y'$, it operates as RAC (hence it is a legitimate racbox); however, for $a \neq y'$, it produces a random bit at output b, uncorrelated with anything else. It is signaling, because by inputting $y' = 0$, $y = 0$, Bob obtains with probability $3/4$ Alice's input x_0. (A particular implementation of such a racbox is presented in the Supplemental Material, Fig. IV [25].)

Theorem 1: Assume that x and y are generated uniformly at random. Let us suppose that for the signaling racbox described above, a channel Λ satisfies the following inequality:

$$\text{racbox} + 1\text{c-bit} \geq \text{PR-correlations} + \Lambda. \qquad (8)$$

Then the channel can be obtained from the $1/2$-erasure channel by postprocessing.

For the proof, see the Supplemental Material [25]. The theorem shows that in order to simulate PR correlations by such a signaling racbox, we need, in addition, at least $1/2$ bit of communication. Thus, in that particular instance the signaling racbox is in some respects weaker than a nonsignaling one.

Conclusions.—We have introduced a new functionality called a racbox. We have proved that a nonsignaling racbox is equivalent to a PR box. We have also considered an exemplary signaling racbox, which, interestingly, can be a weaker resource: in the cycle "racbox + channel → PR box + channel" the capacity of the channel drops at most by a half. We have required that the output of the PR box is perfect. It seems, though, possible to derive a quantitative trade-off between quality of PR box and capacity of the channel (see Theorem 2 in the Supplemental Material for further details [25]). As an example, we can consider a more robust version where we do not aim to obtain a strict PR correlation. In such a case, one might expect a possible trade-off between quality of PR box and quality of a channel $z \to b$.

Our work opens a new area of studies, as similar analysis can be performed not only for more general RACs but also for any other communication complexity task where nonlocal resources provide an advantage.

The most general $n_d \to m_k$ RAC is a task in which Alice gets n numbers from 1 to d and sends one of m possible messages to Bob, who has to guess a subset of k numbers. For the simplest case studied here, $n = d = 2$ and $m = k = 1$. If these numbers are larger, the problem becomes much richer because of the freedom of which the nonlocal box has to compare with a particular racbox. One option is to consider the relation between a racbox and some number of PR boxes. In this case, $n_2 \to 1_1$ RAC requires $n - 1$ PR boxes for simulation while being able to simulate only 1 PR box. Another possibility is to define a generalization of a PR box that is naturally implied by the RAC. For such an entity, resource inequalities analogous to the ones presented here hold. The results will be proved rigorously in Ref. [26].

Linking nonlocal resources to RACs has proven to be a very powerful tool in studies on the foundations of quantum mechanics and quantum information processing protocols. Linking them to other tasks could be equally enlightening. One can, e.g., consider a "crypto-box" which gives the parties N bits of a secure key if augmented with $\mathcal{O}(N)$ bits of communication or a "cc box" which gives an answer to some communication complexity problem, i.e., allows the parties to find a value of a function when each of them has only a part of its input, again when augmented with some amount of two-way communication. Studies on these resources could help us understand the role of nonlocality in information processing tasks.

We thank members of the Gdansk QIT group for discussion, during which the problem was posed. This work is supported by ERC Advanced Grant QOLAPS, NCN Grant No. 2013/08/M/ST2/00626, and the FNP TEAM. Part of this work was done in the National Quantum Information Centre of Gdańsk. K. H. also acknowledges Grant BMN No. 538-5300-B162-13.

[1] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[2] J. Kilian, *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC 88)* (ACM, New York, 1988), pp. 20–31.
[3] S. Wiesner, SIGACT News **15**, 78 (1983).
[4] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM **49**, 1 (2002).
[5] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302 (2011).
[6] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).
[7] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).
[8] A. Casaccino, E. F. Galvao, and S. Severini, Phys. Rev. A **78**, 022310 (2008).
[9] M. Pawłowski and M. Żukowski, Phys. Rev. A **81**, 042326 (2010).
[10] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature (London) **461**, 1101 (2009).
[11] W. van Dam, arXiv:quant-ph/0501159.
[12] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, Phys. Rev. Lett. **96**, 250401 (2006).
[13] M. Navascues and H. Wunderlich, Proc. R. Soc. A **466**, 881 (2009).
[14] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[15] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[16] M. Horodecki, J. Oppenheim, and R. Horodecki, Phys. Rev. Lett. **89**, 240403 (2002).

[17] F. G. Brandao and M. B. Plenio, Nat. Phys. **4**, 873 (2008).

[18] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, Proc. R. Soc. A **465**, 2537 (2009).

[19] D. Janzing, P. Wocjan, R. Zeier, R. Geiss, and T. Beth, Int. J. Theor. Phys. **39**, 2717 (2000).

[20] M. Horodecki and J. Oppenheim, Nat. Commun. **4**, 2059 (2013).

[21] F. G. S. L. Brandão, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Phys. Rev. Lett. **111**, 250404 (2013).

[22] J. Allcock, N. Brunner, N. Linden, S. Popescu, P. Skrzypczyk, and T. Vértesi, Phys. Rev. A **80**, 062107 (2009).

[23] N. Brunner, D. Cavalcanti, A. Salles, and P. Skrzypczyk, Phys. Rev. Lett. **106**, 020402 (2011).

[24] S. Wolf, J. Wullschleger, arXiv:quant-ph/0502030.

[25] See the Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.113.100401 for a detailed proof of Theorem 1. We also present another result, which is in a sense weaker than Theorem 1, but it is more robust to possible generalizations.

[26] M. Pawłowski and W. Kłobus (unpublished).