

No-broadcasting of non-signalling boxes via operations which transform local boxes into local ones

P. Joshi^{1,2}, A. Grudka³, K. Horodecki^{2,4}, M. Horodecki^{1,2}, P. Horodecki^{2,5} and R. Horodecki^{1,2}

¹*Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*

²*National Quantum Information Center of Gdańsk, 81-824 Sopot, Poland*

³*Faculty of Physics, Adam Mickiewicz University, 61-614 Poznań, Poland*

⁴*Institute of Informatics, University of Gdańsk, 80-952 Gdańsk, Poland and*

⁵*Technical University of Gdańsk, 80-233 Gdańsk, Poland*

We deal with families of probability distributions satisfying non-signalling condition, called non-signalling boxes and consider a class of operations that transform local boxes into local ones (the one that admit LHV model). We prove that any operation from this class cannot broadcast a bipartite non-local box with 2 binary inputs and outputs. We consider a function called anti-Robustness which can not decrease under these operations. The proof reduces to showing that anti-Robustness would decrease after broadcasting.

I. INTRODUCTION

Given a quantum bipartite state and a set of measurements on its both subsystems, one ends up with a family of probability distributions obtained from these measurement on the quantum state. Such a family can have interesting features, e.g. can violate some of the Bell inequalities [1]. Moreover such a family satisfies the so-called non-signalling condition: change of measurement by one party can not change statistics of the other party. One can then ask after Popescu and Rohrlich [2], if any set of non-signalling distributions (called a box), can be reproduced by measurement on quantum state. The answer is no, and the proof is given by the fact, that certain (called Popescu-Rohrlich) boxes violate CHSH inequality up to 4, while maximal violation via measurements on quantum states of this inequality is due to Cirel'son's limit $2\sqrt{2}$ [3].

Since this discovery by Popescu and Rohrlich, non-signalling boxes have been treated as a resource in different contexts [4]. In particular it has been shown, that they bear analogous features to those of entangled states [5] such as non-shareability [5], monogamy of correlations [6], offering secret key [7–9] which lead to the so called device independent security (see [10] and references therein). The distillation of PR-boxes and cost of non-locality has attracted recently much attention as well [11–14], as an analogue of distillation of entanglement.

Another context in which non-signalling principle was considered, are the well known no-goes of quantum theory: no-cloning [15] and no-broadcasting [16]. The first states that there is no universal machine which given an unknown input produces its copies, while the second is stronger: it states that there is no universal machine that given an unknown state ρ produces a state whose subsystems are in state ρ . Analogous results for non-signalling boxes were shown in [17].

There is also a bipartite version of no-cloning and no-broadcasting theorems. In case of bipartite quantum states one requires that the input state of machine is *known*, but the operations which machine uses are not

all quantum operations but *local operations* [18, 19] (see also [20]). It was shown later, that this kind of no-broadcasting is equivalent to the previous mentioned one, (with general operations) in [21, 22].

In this article, we consider a variant of 'local' broadcasting of bipartite non-signalling boxes with 2 binary inputs and outputs. (We will represent all such boxes as 2×2 for our convenience). Namely we assume that the input box is known, and it is processed by locality preserving operations. By locality preserving operations we mean here the ones that transform local boxes (those with local hidden variable model) into local ones. We show that any 2×2 non-local box cannot be broadcast in two copies (which excludes broadcasting in arbitrary n -copies), and prove it using idea of monotones, in analogy to entanglement theory. Namely we introduce monotone called anti-Robustness, which cannot decrease under locality preserving operations. For a related entanglement monotone see [23]. We then show that if broadcast were possible, anti-Robustness would increase under locality preserving operations, which gives desired contradiction. Our proof has two main parts: we first show this for states which are mixture of PR and anti-PR boxes and then show that broadcasting of any other non-local boxes implies broadcasting of the latter case. By symmetry, we then extend the argument to all 2×2 boxes. We begin however with analogous question in quantum case: can one broadcast a quantum bipartite state which is entangled by means of operations that transform separable states into separable ones, and answer in negative to this question in section II. The main tools are introduced in section IV and IV A. The two parts of the proof of main result are in sections IV B and IV C. Appendix contains proofs of some needed facts.

II. NO-BROADCASTING IN QUANTUM CASE

In this section we show that any entangled states can not be broadcast, which is in fact an immediate implication of known facts from entanglement theory.

Let ρ_{AB} be a state and Λ be a broadcast map which maps ρ_{AB} to $\rho_{ABA'B'}$ i.e.

$$\Lambda(\rho_{AB}) = \rho_{ABA'B'}, \quad (1)$$

and

$$Tr_{AB}(\rho_{ABA'B'}) = Tr_{A'B'}(\rho_{ABA'B'}) = \rho_{AB}. \quad (2)$$

We show now that such a map does not exist if ρ_{AB} is entangled and it preserves the set of separable states.

To this end, consider first cloning of known bipartite state by LOCC operations which is a smaller class of operations than the separability preserving ones. Cloning is nothing but creating independent copies i.e. in (1) demanding $\Lambda(\rho_{AB}) = \rho_{AB}^{\otimes 2}$. Such a problem was considered in [24] and entanglement measure defined by quality of cloning was suggested. Indeed, by LOCC one can clone any separable state, so if the quality of cloning is not perfect the state must be entangled. At that time it was not known whether any entangled state can be cloned. Note that, if we knew an entanglement measure E (a function that does not increase under LOCC), that for any entangled state

$$E(\rho_{AB} \otimes \rho_{A'B'}) > E(\rho_{AB}), \quad (3)$$

this would imply impossibility of cloning entangled state by LOCC. Indeed, by cloning we would increase the measure E , which is impossible by LOCC. Consider now broadcasting by LOCC. Again, if we knew entanglement measure E which satisfies even more, namely

$$E(\rho_{ABA'B'}) > E(\rho_{AB}), \quad (4)$$

for any entangled state ρ_{AB} and any state $\rho_{ABA'B'}$ being a broadcast copy of ρ_{AB} , i.e. $Tr_{AB}(\rho_{ABA'B'}) = \rho_{AB}$ and $Tr_{A'B'}(\rho_{ABA'B'}) = \rho_{AB}$, then broadcasting of known entangled state by LOCC would be impossible. Indeed, like in cloning case, by broadcasting, we would increase the measure E , which is impossible by LOCC.

Such a measure is actually known. Namely, in [25] it was shown that entanglement of formation satisfies this equation, and as a corollary, it was obtained that cloning of arbitrary entangled state by LOCC is impossible (and also broadcasting, as we now see).

One can strengthen the result by referring to a later analogous result by Marco Piani [26], who showed that relative entropy of entanglement satisfies equation (4) too for any entangled state. Now, since relative entropy of entanglement does not increase after action of arbitrary operations which preserve the set of separable states [27] (called non-entangling operations), we obtain

Corrolary 1 *Arbitrary entangled state cannot be broadcast by non-entangling operations.*

Finally, let us mention, that broadcasting by means of local operations was also considered, and it was shown in [18] that a state can be broadcast by means of local operations only when the state is classical (i.e. it is a state of two classical registers).

III. STATEMENT OF THE BROADCASTING PROBLEM IN BOX SCENARIO

By box X we mean a family of probability distributions that have support on Cartesian product of spaces $\Omega_A \times \Omega_B$. Each of the spaces may contain (the same number of) n systems i.e. it may be a product of spaces $\Omega_{A_1} \dots \Omega_{A_n}$. We will consider only boxes that satisfy certain non-signalling conditions. To specify this we need to define a general non-signalling [4, 28] condition between some partitions of systems.

Definition 1 *Consider a box of some number of systems $n + m$ and its partition into two sets: A_1, \dots, A_n and B_1, \dots, B_m . A box on these systems given by probability table $P(\mathbf{a}, \mathbf{b}|\mathbf{x}, \mathbf{y})$ is non-signalling in cut A_1, \dots, A_n and B_1, \dots, B_m if the following two conditions are satisfied:*

$$\forall_{\mathbf{a}, \mathbf{x}, \mathbf{x}', \mathbf{y}} \sum_{\mathbf{b}} P(\mathbf{a}, \mathbf{b}|\mathbf{x}, \mathbf{y}) = \sum_{\mathbf{b}} P(\mathbf{a}, \mathbf{b}|\mathbf{x}', \mathbf{y}) \quad (5)$$

$$\forall_{\mathbf{b}, \mathbf{x}, \mathbf{x}', \mathbf{y}} \sum_{\mathbf{a}} P(\mathbf{a}, \mathbf{b}|\mathbf{x}, \mathbf{y}) = \sum_{\mathbf{a}} P(\mathbf{a}, \mathbf{b}|\mathbf{x}', \mathbf{y}) \quad (6)$$

If the first condition is satisfied, we denote it as

$$A_1, \dots, A_n \not\rightarrow B_1, \dots, B_m,$$

if the second we write

$$B_1, \dots, B_m \not\rightarrow A_1, \dots, A_n,$$

and if both:

$$A_1, \dots, A_n \not\leftrightarrow B_1, \dots, B_m.$$

We say that a box of systems $A_1, \dots, A_n, B_1, \dots, B_m$ is fully non-signaling if for any subset of systems $A^I B^J \equiv A_{i_1}, \dots, A_{i_k} B_{j_1}, \dots, B_{j_l}$ with $I \equiv \{i_1, \dots, i_k\} \subseteq N \equiv \{1, \dots, n\}$ and $J \equiv \{j_1, \dots, j_l\} \subseteq M \equiv \{1, \dots, m\}$ such that not both I and J are empty, there is

$$A^I B^J \not\leftrightarrow A^{N-I} B^{M-J}. \quad (7)$$

By locally realistic box we mean the following ones:

Definition 2 *Locally realistic box of $2n$ systems $A_1, \dots, A_n, B_1, \dots, B_n$ is defined as*

$$\sum_{\lambda} p(\lambda) P(\mathbf{a}|\mathbf{x})_{A_1, \dots, A_n}^{(\lambda)} \otimes P(\mathbf{b}|\mathbf{y})_{B_1, \dots, B_n}^{(\lambda)} \quad (8)$$

for some probability distribution $p(\lambda)$, where we assume that boxes $P(\mathbf{a}|\mathbf{x})_{A_1, \dots, A_n}^{(\lambda)}$ and $P(\mathbf{b}|\mathbf{y})_{B_1, \dots, B_n}^{(\lambda)}$ are fully non-signaling. The set of all such boxes we denote as LR_{ns} . All boxes that are fully non-signaling but do not satisfy the condition (8), are called non- LR_{ns} .

Having defined relevant classes of boxes, we can define relevant class of operations. We consider a family \mathcal{L} of operations Λ on a box shared between Alice and Bob, which preserve locality, as defined below.

Definition 3 An operation Λ is called *locality preserving* if it satisfies the following conditions:

(i) *validity* i.e. transforms boxes into boxes.
(ii) *linearity* i.e. for each mixture $X = pP + (1-p)Q$, there is $\Lambda(X) = p\Lambda(P) + (1-p)\Lambda(Q)$

(iii) *locality preserving* i.e. transforms boxes from LR_{ns} into boxes from LR_{ns} .

(iv) transforms a *fully non-signalling* box as defined in the Def(1) into fully non-signalling one.

The set of all such operations we denote as \mathcal{L} .

The problem of broadcasting is then *if there exists* $\Lambda \in \mathcal{L}$ which makes a 2-copy broadcast of a 2×2 box P i.e.

$$\Lambda(P_{AB}) = P_{ABA'B'}^{(2)}, \quad (9)$$

where $P^{(2)}$ is arbitrary box with 4 inputs and 4 outputs whose marginal boxes on AB and A'B' are again box P. More generally, one can ask if there exists Λ which produces n broadcast copies, which is a problem of n -copy broadcast. The impossibility of 2-copy broadcast implies the impossibility of n -copy broadcast. Hence it is enough to deal with 2-copy broadcast. From now on by broadcast we mean 2-copy broadcast.

IV. NO-BROADCASTING THEOREM IN BOX SCENARIO

Our approach is like in entanglement theory (see in this context [30]). We pick up a monotone and show that it could be smaller after broadcasting which is not possible. Our monotone will be *anti-Robustness of a box*, defined as follows:

Definition 4 Let A be a NS and non- LR_{ns} box. *Anti-Robustness of A* , $\bar{R}(A)$ is defined as,

$$\bar{R}(A) = \max_X \{q|qA + (1-q)X \in LR_{ns}\}, \quad (10)$$

where X is arbitrary NS box.

The name anti-Robustness comes from the fact that if a given q is anti-Robustness of some box A, then $1-q$ is minimal weight with which one needs to admix some box X to make A local, i.e. $1-q$ reports how 'robust' is A against admixing of some other boxes in terms of non-locality. It is analogous to the robustness quantity defined in [23]. It would be measure of non-locality in the same way as the Robustness of entanglement is measure of entanglement (cf. other measures of nonlocality [14, 31]).

Observation 1 \bar{R} is non decreasing under locality preserving operations.

Proof.- Let us fix an arbitrary NS box A. Let Λ be linear operation taking LR_{ns} boxes into LR_{ns} boxes. Let also q_0 be the value of $\bar{R}(A)$. Then there exists box X such that $q_0A + (1-q_0)X \in LR_{ns}$. Let us apply Λ to $q_0A + (1-q_0)X$ by linearity of Λ it reads $q_0\Lambda(A) + (1-q_0)\Lambda(X)$, and by its locality, this box is LR, hence q_0 is a

candidate for value $\bar{R}(\Lambda(A))$, but by definition the latter can be at most higher, hence proving $\bar{R}(A) \leq \bar{R}(\Lambda(A))$. ■

In the following, we will need also a technical property of anti-Robustness, that can be viewed as connectivity: if it is attained at q , it could be attained at all $p < q$:

Observation 2 If there exists $L = qA + (1-q)X$ with $q > p$, then there exists also a box X' such that $L = pA + (1-p)X'$.

Proof.- The proof is straightforward with $X' = (q-p)/(1-p)A + (1-q)/(1-p)X$. ■

A. Extremal non-local boxes, twirlings and CHSH quantities

We will use numerously the operation of twirling of a box [29, 30], which maps all boxes into a smaller subset of boxes. In what follows we will consider 4 such twirlings and show that they preserve corresponding CHSH quantities.

Let us recall the geometry of two parties 2 binary inputs and outputs NS boxes. The set of such boxes forms an 8 dimensional polytope with 24 vertices [4]. 16 of these are deterministic boxes which span the set of LR_{ns} boxes that satisfy all the CHSH inequalities $4|-2 \leq \beta_{rst}(P) \leq 2$ for all choices of r, s and t with:

$$\beta_{rst}(P) \equiv (-1)^t \langle 00 \rangle + (-1)^{s+t} \langle 01 \rangle + (-1)^{r+t} \langle 10 \rangle + (-1)^{r+s+t+1} \langle 11 \rangle, \quad (11)$$

where $\langle ij \rangle = P(a=b|ij) - P(a \neq b|ij)$ and r, s, t takes values either 0 or 1. The rest of 8 vertices are equivalent to PR-boxes, which are defined as follows :

$$B_{rst}(ab|xy) = \begin{cases} 1/2 & \text{if } a \oplus b = xy \oplus rx \oplus sy \oplus t \\ 0 & \text{else.} \end{cases} \quad (12)$$

We describe now 4 twirling operations τ_{rs} , and show that they preserve corresponding CHSH quantities. The twirling τ_{00} is introduced in [29, 30].

Definition 5 A twirling operation τ_{rs} is defined by flipping randomly 3 bits δ, γ, θ and applying the following transformation to a 2×2 box $P(a, b|x, y)$:

$$\begin{aligned} x &\rightarrow x \oplus \delta \\ y &\rightarrow y \oplus \gamma \\ a &\rightarrow a \oplus \gamma x \oplus \delta \gamma \oplus \theta \oplus s \gamma \\ b &\rightarrow b \oplus \delta y \oplus \theta \oplus r \delta \end{aligned} \quad (13)$$

We then make the following observation, which is easy to check:



Observation 3 Twirling τ_{rs} maps all 2×2 boxes into line $pB_{rst} + (1-p)B_{rs\bar{t}}$; $\tau_{rs}(B_{rst}) = B_{rst}$ and $\tau_{rs}(B_{rs\bar{t}}) = B_{rs\bar{t}}$ where \bar{t} denotes binary negation of t .

We are ready to show that twirling preserves appropriate CHSH quantity, which is formulated in lemma below:

Lemma 1 The CHSH quantities β_{rst} satisfy:

$$\beta_{rst}(P) = \beta_{rst}(\tau_{rs}(P)). \quad (14)$$

Proof.- It is straightforward to check that $\beta_{rst}(P) = \langle 2(B_{rst} - B_{rs\bar{t}})|P \rangle$, where $\langle \cdot | \cdot \rangle$ denotes Euclidean scalar product and hence there is

$$\begin{aligned} \beta_{rst}(\tau_{rs}(P)) &= \langle 2(B_{rst} - B_{rs\bar{t}})|\tau_{rs}(P) \rangle = \\ &= \sum_i q_i \langle 2(B_{rst} - B_{rs\bar{t}})|\pi_i P \rangle. \end{aligned} \quad (15)$$

Here we use the fact that each twirling is a mixture of some permutations π_i . We have then

$$\begin{aligned} \beta_{rst}(\tau_{rs}(P)) &= \sum_i q_i \langle \pi_i 2(B_{rst} - B_{rs\bar{t}})|P \rangle = \\ &= \langle \tau_{rs}(2(B_{rst} - B_{rs\bar{t}}))|P \rangle \end{aligned} \quad (16)$$

which ends the proof, since $\tau_{rs}(B_{rst}) = B_{rst}$ and $\tau_{rs}(B_{rs\bar{t}}) = B_{rs\bar{t}}$ by observation 3. ■

B. No-broadcasting for mixtures of PR and anti-PR box

Here we show, for a subclass $\{B_\alpha\}$ of non- LR_{ns} boxes that they cannot be broadcast. These boxes are a family of convex combinations of $B_{000} \equiv B$ (PR-box) and $B_{001} \equiv \tilde{B}$ (anti-PR) boxes i.e.

$$B_\alpha = \alpha B + (1 - \alpha) \tilde{B}, \quad (17)$$

where $\alpha \in [1, \frac{3}{4})$, such that when $\alpha = 1 \Rightarrow B_\alpha = B$ (PR box). For $\alpha = \frac{3}{4}$, B_α becomes an LR box (say K)

$$K = \frac{3}{4}B + \frac{1}{4}\tilde{B} \quad (18)$$

One can express K in terms of B_α and \tilde{B} as follows:

$$K = p_\alpha B_\alpha + (1 - p_\alpha) \tilde{B}, \quad (19)$$

where $p_\alpha = \frac{3}{4\alpha}$. We show that for B_α in (17) broadcasting is not possible. Only when $B_\alpha = K$, it turns out that broadcasting can be possible which is known fact for LR_{ns} boxes.

Before passing to the main results there is an important observation required in the main proof:

Observation 4 $\bar{R}(B_\alpha) = p_\alpha$.

Proof.- Consider, two boxes C and X such that $\beta(X) \in [-4, \beta(C)]$ and $\beta(C) \in [-2, 2]$. These two boxes lie on

the line of convex combination of B and B' . Let us write C as follows,

$$C = qB_\alpha + (1 - q)X \quad (20)$$

Taking β values of (20) and rearranging terms we get

$$q = \frac{\beta(C) - \beta(X)}{\beta(B_\alpha) - \beta(X)} \quad (21)$$

By the definition of anti-Robustness, $\bar{R}(B_\alpha)$ is equal to maximum of q over all X such that (20) holds. So to maximize q we need to have maximum value of $\beta(C) = 2$.

$$q_{max} = \frac{2 - \beta(X)}{8\alpha - 4 - \beta(X)} \quad (22)$$

We find that for $\alpha \in (\frac{3}{4}, 1]$, $q_{max} = \frac{3}{4\alpha}$. Hence, $\bar{R}(B_\alpha) = \frac{3}{4\alpha} = p_\alpha$.

Theorem 1 For any broadcast copy \hat{B}_α of B_α , where $\alpha \in (\frac{3}{4}, 1]$, there is

$$\bar{R}(B_\alpha) > \bar{R}(\hat{B}_\alpha). \quad (23)$$

Proof.- Suppose we can broadcast B_α and consider \hat{B}_α be the broadcast of it. Let Λ be the operation that achieves broadcast. Since it transforms LR_{ns} boxes into LR_{ns} boxes, if applied to K it will transform it into some box $L \in LR_{ns}$. Thus using (19) we would obtain:

$$L = p_\alpha \hat{B}_\alpha + (1 - p_\alpha)X. \quad (24)$$

We will show however in lemma 2 below, that for any broadcast copy \hat{B}_α , any LR_{ns} box L and any box X the above equality does not hold. Now, if there does not exist an LR_{ns} box L satisfying the above equality, by definition of anti-Robustness $p_\alpha (= \bar{R}(B_\alpha))$ can not be anti-Robustness of \hat{B}_α . The latter can not be also higher than p_α or otherwise (24) would be satisfied, because we have the observation 2 which ends the proof. ■

Corrolary 2 The boxes B_α for $\alpha \in (\frac{3}{4}, 1]$ are not broadcastable.

Proof.- The proof follows from the above theorem and monotonicity of anti-Robustness (observation 1). ■

We can proceed now with the proof of crucial lemma mentioned in the proof of the theorem above:

Lemma 2 For any broadcast copy \hat{B}_α of B_α with $\alpha \in (\frac{3}{4}, 1]$, any LR_{ns} box L and any NS box X the equality

$$L = p_\alpha \hat{B}_\alpha + (1 - p_\alpha)X \quad (25)$$

does not hold.

Proof.- We define two random variables C_1 and C_2 in the following way: pick randomly independent 2 bits and according to it's values choose inputs x and y for the first box. Then compare the outputs a and b . If outputs

satisfy the condition $a \oplus b = xy$, the value of C_1 is set to 4 otherwise it is set to -4. It is straightforward to check that the average value of this random variable on a box equals the CHSH quantity β_{000} of the first box. We define C_2 in the same way on second box.

We will be interested now in joint probability distributions of the variables (C_1, C_2) applied to boxes L , \hat{B}_α and X . Note that this transformation of mapping the box to a probability distribution is linear. With a box we associate a corresponding probability distribution of (C_1, C_2) :

$$L \rightarrow \{p'_{11}, p'_{12}, p'_{21}, p'_{22}\}, \quad (26)$$

with $p'_{ij} = P(C_1 = (-1)^{i+1}4, C_2 = (-1)^{j+1}4)$, similarly for a broadcast copy:

$$\hat{B}_\alpha \rightarrow \{\tilde{p}_{11}, \tilde{p}_{12}, \tilde{p}_{21}, \tilde{p}_{22}\}, \quad (27)$$

and the X :

$$X \rightarrow \{p''_{11}, p''_{12}, p''_{21}, p''_{22}\}. \quad (28)$$

If there exists L and X such that (25) holds, then there also exists the one which is permutationally invariant w.r.t. to copies i.e. symmetric, because \hat{B}_α is such. Hence without loss of generality, we can assume that distribution L is symmetric, therefore we have $p'_{12} = p'_{21}$ and $\tilde{p}_{12} = \tilde{p}_{21}$.

Now, by assumption, the box L is LR_{ns} . Hence, if we perform operation defined by the random variable C_1 on first copy, given we observe value 4, the second copy is also an LR_{ns} box: it is a mixture of induced product boxes on the second system given input i, j and output a, b on the first system [32]. Analogous property holds if we ask how the second system looks like given the C_1 had value -4. Thus the CHSH inequality of conditional box on second system must hold in both cases. Recall that the average value of C_2 on a box equals the CHSH quantity β_{000} of this box, thus if the measured copy results 4 for C_1 , the CHSH inequality $-2 \leq \beta_{000} \leq 2$ for the second copy is

$$-2 \leq \frac{4p'_{11} + (-4)p'_{12}}{p'_{11} + p'_{12}} \leq 2, \quad (29)$$

and if the outcome is -4 then CHSH inequality is

$$-2 \leq \frac{4p'_{21} + (-4)p'_{22}}{p'_{21} + p'_{22}} \leq 2. \quad (30)$$

Using the fact that $p'_{12} = p'_{21}$, $\tilde{p}_{12} = \tilde{p}_{21}$ and normalization condition, we rewrite the above inequalities in simplified form as follows

$$0 \leq 6p'_{11} - 2p'_{12}, \quad (31)$$

$$2p'_{11} - 6p'_{12} \leq 0, \quad (32)$$

$$0 \leq 2p'_{11} + 10p'_{12} - 2, \quad (33)$$

$$6p'_{11} + 14p'_{12} - 6 \leq 0. \quad (34)$$

These inequalities give an LR_{ns} polytope.

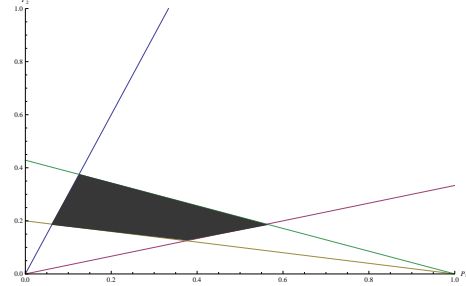


FIG. 1: A set of pairs of parameters (p'_{11}, p'_{12}) of box L (shaded region), satisfying locality conditions (31)-(34).

Let us consider constraints on \hat{B}_α , i) normalisation condition ii) symmetry of broadcast i.e. $\tilde{p}_{12} = \tilde{p}_{21}$ iii) if we trace out one copy of the broadcast copy then the second copy has to be B_α and hence

$$\tilde{p}_{11} + \tilde{p}_{21} = \alpha, \quad (35)$$

as α is probability of obtaining 4 (i.e. value 4 of C_1) on B_α box. We can rewrite eq.(25) as,

$$L - p_\alpha \hat{B}_\alpha = (1 - p_\alpha)X. \quad (36)$$

Thanks to linearity of the map giving (C_1, C_2) for a box, the same relation holds for the related probability distributions $\{p'_{ij}\}$, $\{\tilde{p}_{ij}\}$ and $\{p''_{ij}\}$. Since X is a box, the distribution $\{p''_{ij}\}$ should always have positive coefficients. We check if for any B_α it becomes negative. So, now we have a complete set of LR_{ns} boxes mapped on the shaded region as shown in fig.1 let us denote it S_1 . The image under mapping to distribution $\{\tilde{p}_{ij}\}$ of one copy of \hat{B}_α is nothing but a straight line given by the eq. (35). We draw this straight line scaled by the factor p_α , and denote resulting set of points as S_2 . Interestingly, for any $\alpha \in [\frac{3}{4}, 1]$, we get the same line, because $(p_\alpha \tilde{p}_{11}, p_\alpha \alpha - p_\alpha \tilde{p}_{11}) = (p_\alpha \tilde{p}_{11}, \frac{3}{4} - p_\alpha \tilde{p}_{11})$. Changing value of α , simply shifts points on the line since slope of the line $p_\alpha \hat{B}_\alpha$ is the same for all α .

In fig.2, we draw points of S_1 and S_2 and find that they only intersect at a point $(\frac{9}{16}, \frac{3}{16})$. For all other points, $(1 - p_\alpha)X$ turns out to be negative. At the intersection, since X is normalised and LHS in (36) is zero, p_α should be 1. Therefore, $\alpha = \frac{3}{4}$. This intersection point precisely corresponds to the case when $B_\alpha = K$, which we know can be broadcast. Hence for any $\alpha \in (\frac{3}{4}, 1]$ the eq. (36) does not hold with both positive X . This ends proof of the lemma 2. ■

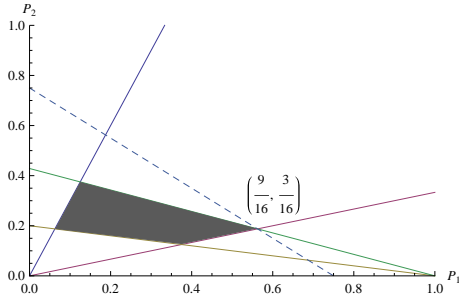


FIG. 2: A set of pairs of parameters (p'_{11}, p'_{12}) of box L, satisfying locality conditions (31)-(34) (shaded region) and the set of the parameters $(\tilde{p}_{11}, \tilde{p}_{21})$ of box \tilde{B}_α scaled by p_α (dashed line).

C. General Case - No-broadcasting for all 2×2 non- LR_{ns} boxes

In this section we show no-broadcasting for all 2×2 non- LR_{ns} boxes. To this end we will need the following crucial lemma, proved in Appendix.

Lemma 3 For any r, s, t in $\{0, 1\}$, and any box P_{AB} satisfying $\beta_{rst}(P_{AB}) \geq 2$ there is

$$\bar{R}(P_{AB}) = \bar{R}(\tau_{rs}(P_{AB})), \quad (37)$$

where τ_{rs} is twirling given in def 5.

We are ready to state our main result:

Theorem 2 Any non- LR_{ns} box in 2×2 can not be broadcast.

Proof.- We will show first that any box with $\beta_{000}(P) > 2$ is not broadcastable. Suppose by contradiction that they can be broadcast i.e. there exists a transformation Λ such that takes a box P_{AB} to a broadcast copy $P_{ABA'B'}$. We will use now monotonicity of anti-Robustness under linear operations that transform LR_{ns} boxes into LR_{ns} boxes (Observation 1). From monotonicity and the above Lemma 3 we get,

$$\bar{R}(\tau_{rs}P_{AB}) = \bar{R}(P_{AB}) \leq \bar{R}(P_{ABA'B'}) \leq \quad (38)$$

$$\bar{R} \left[(\tau_{rs}^{AB} \otimes \tau_{rs}^{A'B'}) (P_{ABA'B'}) \right]. \quad (39)$$

But this contradicts equation (23). This reduction argument proves no-broadcasting of boxes P satisfying $\beta_{000}(P) > 2$. The whole set of 2×2 non- LR_{ns} boxes can be written compactly as

$$\bigcup_{r,s,t=0}^1 \{P : \beta_{rst}(P) > 2\}, \quad (40)$$

hence we need to have proof for 7 other values of string rst . We prove that if boxes with $\beta_{000} > 2$ are non-broadcastable then so are those with $\beta_{r's't'} > 2$ for $r's't' \neq 000$. This is because by definition of B_{rst} there is local operation which maps B_{000} into $B_{r's't'}$ and B_{001}

into $B_{r's't'}$. Hence if boxes $\alpha B_{r's't'} + (1 - \alpha) B_{r's't'}$ were broadcastable for $\alpha \in [1, \frac{3}{4})$, then the corresponding box $\alpha B_{000} + (1 - \alpha) B_{001} = B_\alpha$ would be broadcastable, which is disproved in section IV B. Thus we have no-broadcasting on a line between $B_{r's't'}$ and $B_{r's't'}$ with $\beta_{r's't'} > 2$. To prove this for all $\beta_{r's't'} > 2$ boxes, we note, that reduction argument as shown above applies, with $r = r' s = s' t = t'$ in lemma 3. This proves the theorem. ■

V. CONCLUSIONS

We have shown that locality preserving operations do not broadcast 2×2 non-local boxes. Moreover, this result is general since impossibility of 2-copy broadcast implies impossibility of $n(>2)$ -copy broadcast. Indeed, if latter were true, we could simply trace out $n-2$ systems and obtain 2 copies of broadcast. It is intuitive in a sense that non-locality is a resource, and it can not be brought into for free, which broadcast would do. We developed an idea of monotone in boxes paradigm, introducing anti-Robustness (or equivalently Robustness), a quantity interesting on its own. The proof uses counter-intuitive property of this monotone: it does not change under irreversible operation of twirling, resembling the fact that CHSH value is preserved under twirling. In this proof we have used heavily some properties of 2×2 boxes. It would be interesting to show the same for arbitrary nonlocal box, which is an open question. In fact, we consider here exact broadcasting i.e. we do not allow errors in this process. It would be interesting to prove its non-exact version as well.

VI. APPENDIX

In this section we prove some results including proof of lemma 3.

A. Proof of the lemma 3

We first prove that $\bar{R}(P) = \bar{R}(\tau_{rs}P)$ with $\beta_{rst}(P) > 2$. We fix values r, s, t and omit them in the following proof as thanks to lemma 1 it goes the same way for all these indices.

To this end consider an arbitrary box $X \neq P$ and $Y = qP + (1-q)X$. Then,

$$\beta(Y) = q\beta(P) + (1-q)\beta(X). \quad (41)$$

To make Y local, we need clearly $\beta(X) \leq 2$. Let q_0^X be solution of

$$2 = q_0^X \beta(P) + (1 - q_0^X) \beta(X). \quad (42)$$

Let us observe that

$$\bar{R}(P) = \max_X \max_q \{q\beta(P) + (1-q)\beta(X) \in LR\}, \quad (43)$$

and denote

$$q_X(P) := \max_q \{q|qP + (1-q)X \in LR\}, \quad (44)$$

then $\bar{R}(P) = \max_X q^X(P)$. Now for $\beta(P) > 2, \beta(X) \leq 2$, any $q > q_0^X$ there is $Y \notin LR$. Thus $q^X(P) \leq q_0^X$ for any X .

However, we have a lemma 4 that if $\beta(A) = 2$, then $A \in LR$ (see section below). Hence for $q = q_0^X, \beta(Y) = 2$, and therefore $Y \in LR$. This implies that for any $X, q_X(P) = q_0^X$. Thus for $\beta(P) \geq 2$ we can equivalently write definition of anti-Robustness as

$$\bar{R}(P) = \max_X q_0^X \equiv \max_X \{q : q\beta(P) + (1-q)\beta(X) = 2\}, \quad (45)$$

but we know by lemma 1 that twirl of a box has same value of CHSH as that of the box for the same CHSH i.e. $\beta(P) = \beta(\tau P)$ [30] Hence,

$$\bar{R}(P) = \max_X \{q : q\beta(\tau P) + (1-q)\beta(X) = 2\}. \quad (46)$$

But according to (45) this is nothing but the definition of anti-Robustness of τP i.e. $\bar{R}(\tau P)$. And hence $\bar{R}(P) = \bar{R}(\tau P)$ for $\beta(P) > 2$. For $\beta(P) = 2$ we have $\beta(\tau(P)) = 2$ by lemma 1. Hence by lemma 4 we have that both P and $\tau(P)$ are local. It is easy to see, that for local boxes anti-Robustness is 1, hence the desired weak inequality. ■

B. locality of $\beta_{rst}(X) = 2$ hyperplane

The main result of this section is the lemma below. We first show the proof of this lemma, and then the proof of theorem (3) which is crucial to this proof.

Lemma 4 For any $r, s, t \in \{0, 1\}$ and any box $X, \beta_{rst}(X) = 2$ implies $X \in LR_{ns}$.

Proof Let us fix r, s, t . By theorem (3) there is $X \in \text{conv}\{x_0, \tilde{x}_1^{(rst)}, \dots, \tilde{x}_n^{(rst)}\}$ where $\tilde{x}_i^{(rst)}$ are points from the half plain defined by $\beta_{rst}(x) = 2$ which belongs to ray starting at $x_0 = B_{rst}$ and passing through x_i which is the i -th of 23 (apart from x_0) extremal point of the set of non-signalling boxes. In other words $\tilde{x}_i^{(rst)} = p_i B_{rst} + (1-p_i)x_i$ such that $\beta_{rst}(\tilde{x}_i^{(rst)}) = 2$. Thus $X = p_0 x_0 + \sum_{i=1}^n p_i \tilde{x}_i^{(rst)}$. Now, since $\beta_{rst}(X) = 2$ there is $X = \sum_i p_i \tilde{x}_i^{(rst)}$ i.e. the weight p_0 of x_0 is zero in the mixture. But it is easy to check that all $\tilde{x}_i^{(rst)}$ are local, hence X must be local itself. To see this we check that for all $r's't'$ there is

$$-2 \leq \beta_{r's't'}(\tilde{x}_i^{(rst)}) \leq 2, \quad (47)$$

i.e. that $\tilde{x}_i^{(rst)}$ belongs to the LR_{ns} in 2×2 . To this end we first compute from the assumption $\beta_{rst}(\tilde{x}_i^{(rst)}) = 2$ the probability p_i and check for all values $r's't' \neq r, s, t$ the value of $\beta_{r's't'}$ of $\tilde{x}_i^{(rst)}$. The last check is easy if we

observe that $\beta_{r's't'}(B_{rst}) \in \{-4, 0, 4\}$ and $\beta_{r's't'}(L) \in \{-2, 2\}$, where L stands for any locally realistic extremal box. This holds because both nonlocal boxes B_{rst} and locally realistic extremal ones L can be represented (not uniquely) as vectors v_i of 1s and -1 s (4 of them in total each corresponding to one pair of x and y), where 1 denotes maximal correlations of a distribution and -1 denotes maximal anticorrelations. Each value of $\beta_{r's't'}$ can be represented as an Euclidean scalar product of v_i with again vector of 4 1s and -1 s depending on sign of $\langle ij \rangle$ in definition (11) where the number of -1 is always odd. The numbers $\{-4, -2, 0, 2, 4\}$ follows from the fact that for each B_{rst} v_i has always odd number of -1 s, and each L has always even number of them. ■

1. geometrical theorem

Following Bengtsson and Życzkowski [33], by a cone with apex x_0 and some body such that $x_0 \notin$ body as a base we mean the set of points obtained by the following operation: taking rays (half lines) that connect x_0 and each point of the body.

Thus we consider operation *cone* which makes cone from the body defined in the following way: $\text{cone}(x_0, \text{conv}\{x_1, \dots, x_n\})$ where x_0 does not belong to $\text{conv}\{x_1, \dots, x_n\}$ and x_1, \dots, x_n are extremal points of the body. In our case, the apex will be any of the maximally non-local boxes B_{rst} , and the body will be convex combination of other 23 extremal points of the set of non-signalling boxes. We recall that $\beta_{rst}(B_{rst}) = 4$. Equality $\beta_{rst}(X) = 2$ defines a hyperplane $H^{(rst)}$. By the set of X satisfying $\beta_{rst}(X) \geq 2$ we mean $H_+^{(rst)}$. In what follows we fix r, s and t and omit it, as the proof goes the same way for all indices.

The main thesis of this section is the following

Theorem 3 $H_+ \cap B = \text{conv}(\{x_0, \tilde{x}_1, \dots, \tilde{x}_n\})$ where \tilde{x}_i is a point from H (the half plain defined by $\beta(x) = 2$) which belongs to ray starting at x_0 and passing through x_i .

In what follows we use numerous the following lemma:

Lemma 5 If $x = az + (1-a)x_0$ $a \in R$ and linear function $\beta(x) = \lambda\beta(z) + (1-\lambda)\beta(x_0)$, then either $\lambda = a$ or $\beta(z) = \beta(x_0)$.

Proof

By linearity of β we have $\beta(x) = a\beta(z) + (1-a)\beta(x_0)$ but such a combination is unique in real numbers, hence either $a = \lambda$ or $\beta(z) = \beta(x_0)$, which ends the proof. ■

In what follows, we will have $\beta(x_0) \neq \beta(z)$, but we do not state it each time. Armed with this lemma, we can observe the following property:

Lemma 6 $H_+ \cap B = H_+ \cap C$ where H_+ is a half space defined by $\beta(x) \geq 2$, B is body spanned by $\{x_0, x_1, \dots, x_n\}$ distinct points, and C is a cone obtained by operation $\text{cone}(x_0, \text{conv}\{x_1, \dots, x_n\})$.

Proof

If $x \in \text{RHS}$, then $\beta(x) \geq 2$ and there exists $y \in \text{conv}\{x_1, \dots, x_n\}$ such that $x = \alpha x_0 + (1 - \alpha)y$ for $\alpha \in R_{>0}$. By lemma 5, this means that $x \in [x_0, y]$ because $\beta(x_0) = 4$, $\beta(y) < 2$ and $\beta(x) \geq 2$ and we have $\beta(x) \leq 4$. Since $\beta(x) \geq 2$, we have $x \in H_+$ which proves $x \in \text{LHS}$. Take now the converse: $x \in \text{LHS}$. This means that $x = \sum_{i=0}^n p_i x_i$, hence $x = p_0 x_0 + (1 - p_0) \sum_{i=1}^n p_i / (1 - p_0) x_i$ which means $x \in \text{cone}(x_0, \text{conv}\{x_1, \dots, x_n\})$, and hence $x \in C$, which taking into account $x \in H_+$, gives $x \in \text{RHS}$ which proves the thesis. ■

We can now prove the following lemma, which enables us to state the main question of this section:

Lemma 7 H has one point of intersection with each of the segments $[x_0, x_i]$, denoted as \tilde{x}_i .

proof We have $L_i = \{x : (1 - \alpha)x_0 + \alpha x_i = x\}$, $H = \{z : \beta(z) = 2\}$. We want to prove that $H \cap L = \{\tilde{x}_i\}$. To this end we observe that $x \in H \cap L$ implies $\beta(x) = 2$. Taking this into account and $\beta(x_0) = 4$ as well as $\beta(x_i) \leq 2$ we have by lemma 5 that there exists unique $\alpha \in [0, 1]$ such that $x = (1 - \alpha)x_0 + \alpha x_i$, call it \tilde{x}_i i.e. $\tilde{x}_i \in [x_0, x_i]$ as we claimed.

To prove theorem 3, we first show the following inclusion:

Lemma 8 $H_+ \cap B \supseteq \text{conv}(\{x_0, \tilde{x}_1, \dots, \tilde{x}_n\})$.

Proof

Take x from RHS. First we prove that $x \in H_+$. This is easy since $x = \gamma_0 x_0 + \sum_{i=1}^n \gamma_i \tilde{x}_i$, by linearity of function β we have $\beta(x) = \gamma_0 \beta(x_0) + \sum_{i=1}^n \gamma_i 2$ since for each \tilde{x}_i we have $\beta(\tilde{x}_i) = 2$. Thus, following $\beta(x_0) > 2$ we have also $\beta(x) > 2$ i.e. $x \in H_+$.

We prove now that $x \in B$. To this end note that by definition $\tilde{x}_i = \alpha_i x_0 + (1 - \alpha_i) x_i$, hence $x = (\gamma_0 + \sum_{i=1}^n \gamma_i \alpha_i) x_0 + \sum_{i=1}^n \gamma_i (1 - \alpha_i) x_i \in \text{conv}\{x_0, x_1, \dots, x_n\}$. ■

To prove the converse inclusion: $H_+ \cap B \subseteq \text{conv}(\{x_0, \tilde{x}_1, \dots, \tilde{x}_n\})$ we need the following lemma:

Lemma 9 Equivalent definition of a cone C is the set of all points satisfying $x = x_0 + \sum_i \alpha_i r_i$ with $r_i = x_i - x_0$ and α_i are non-negative coefficients.

Proof

We have the following chain of equivalences. $x = x_0 + \sum_i \alpha_i r_i$. This is if and only if $x = x_0 + \sum_i \alpha_i (x_i - x_0)$,

which is iff $\sum_i \alpha_i x_i + (1 - \sum_i \alpha_i) x_0$ and this is equivalent to $\alpha \sum_i \alpha_i / \alpha x_i + (1 - \alpha) x_0$ which we aimed to prove. ■

This lemma gives the following

Corrolary 3 Equivalent definition of C is the set of all points satisfying $x = x_0 + \sum_i \gamma_i \tilde{r}_i$ where $\tilde{r}_i = \tilde{x}_i - x_0$ and γ_i are non-negative coefficients.

Proof

We know that $\tilde{x}_i = \lambda_i x_i + (1 - \lambda_i) x_0$ where $\lambda_i \in R_+$ hence $\tilde{r}_i = \lambda_i (x_i - x_0) = \lambda_i r_i$, which ends the proof, since \tilde{r}_i are just scaled r_i and the proof goes with similar lines to that of lemma 9. ■

To complete the proof of theorem 3 we now proceed with the proof of the converse inclusion: $H_+ \cap B \subseteq \text{conv}(\{x_0, \tilde{x}_1, \dots, \tilde{x}_n\})$. Thanks to lemma 6, we may assume that $x \in H_+ \cap C$. Now, thanks to lemma 5, if we take the ray with beginning x_0 crossing H in point \tilde{x}_0 , that passes through x then if $x \in H_+$, there is $x \in [x_0, \tilde{x}_0]$. This is because $\beta(x_0) > 2$ and $\beta(x_0) \geq \beta(x) > 2$ while $\beta(\tilde{x}_0) = 2$.

Hence to prove that $x \in \text{conv}(x_0, \tilde{x}_1, \dots, \tilde{x}_n)$, it is sufficient to show that \tilde{x}_0 is spanned by $\{\tilde{x}_1, \dots, \tilde{x}_n\}$. We will show it in what follows. Namely, by corollary (3), there is $\tilde{x}_0 = \sum_i \gamma_i \tilde{x}_i$ where $\gamma_i \in R_+$. By linearity of β there is $\beta(\tilde{x}_0) = \sum_i \gamma_i \beta(\tilde{x}_i) = \sum_i \gamma_i 2$. Since $\tilde{x}_0 \in H$, there is also $\beta(\tilde{x}_0) = 2$. Hence there is $\sum_i \gamma_i = 1$, which taking into account non-negativity of γ_i shows that γ_i forms a convex combination of \tilde{x}_i which we aimed to prove. This ends the proof that $H_+ \cap B = \text{conv}\{\tilde{x}_1, \dots, \tilde{x}_n\}$, and following lemma 8, ends the proof of theorem 3.

Acknowledgments

We thank T. Szarek and D. Reeb for interesting discussions. This work was supported by the Polish Ministry of Science under Grant No. NN202231937 and later by Polish Ministry of Science and Higher Education Grant no. IdP2011 000361. It was also partially supported by EC grant QESSENCE and Foundation of Polish Science from International PhD Project: "Physics of future quantum-based information technologies". K.H. acknowledges grant BMN nr 538-5300-0637-1.

- [1] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
- [2] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
- [3] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).
- [4] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, PRA **71**, 022101 (2005), arXiv:quant-ph/0404097.
- [5] L. Masanes, A. Acin, and N. Gisin, Phys. Rev. A **73**, 012112 (2006), arXiv:quant-ph/0508016.
- [6] M. Pawłowski and C. Brukner, Phys. Rev. Lett. **102**, 030403 (2009), arXiv:0810.1175.
- [7] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [8] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**,

010503 (2005).

- [9] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett (2006), arXiv:quant-ph/0606049.
- [10] E. Hänggi, Ph.D. thesis, ETH, Zurich (2010).
- [11] N. Brunner and P. Skrzypczyk, Phys. Rev. Lett. **102**, 160403 (2009), arXiv:0901.4070.
- [12] J. Allcock, N. Brunner, N. Linden, S. Popescu, P. Skrzypczyk, and T. Vertesi, Phys. Rev. A **80**, 062107 (2009), arXiv:0908.1496.
- [13] M. Forster, Phys. Rev. A **83**, 062114 (2011), arXiv:1105.1357.
- [14] N. Brunner, D. Cavalcanti, A. Salles, and P. Skrzypczyk,



- Phys. Rev. Lett. **106**, 020402 (2011), arXiv:1009.4207.
- [15] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
- [16] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **53**, 2818 (1996).
- [17] H. Barnum, J. Barrett, M. Leifer, and A. Wilce (2006), arXiv:quant-ph/0611295.
- [18] M. Piani, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **100**, 090502 (2008), arXiv:0707.0848.
- [19] M. Horodecki, A. S. De, and U. Sen, PRA **70**, 052326 (2004), arXiv:quant-ph/0403169.
- [20] M. Piani, M. Christandl, C. E. Mora, and P. Horodecki, Phys. Rev. Lett. **102**, 250503 (2009), arXiv:0901.1280.
- [21] S. Luo, Lett. Math. Phys. **92**, 143 (2010).
- [22] S. Luo and W. Sun, PRA **82**, 012338 (2010).
- [23] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999), quant-ph/9806094.
- [24] M. Horodecki, A. Sen(De), and U. Sen, Phys. Rev. A **70**, 052326 (2004), quant-ph/0403169.
- [25] D. Yang, M. Horodecki, R. Horodecki, and B. Synak-Radtke, Phys. Rev. Lett. **95**, 190501 (2005), quant-ph/0506138.
- [26] M. Piani, Phys. Rev. Lett. **103**, 160504 (2009), arXiv:0904.2705.
- [27] F. G. Brandao and M. B. Plenio (2007), arXiv:0710.5827.
- [28] J. Barrett (2005), arXiv:quant-ph/0508211.
- [29] L. Masanes, A. Acin, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).
- [30] A. J. Short, Phys. Rev. Lett. **102**, 180502 (2009), arXiv:0809.2622v1.
- [31] M. Fitzi, E. Hanggi, V. Scarani, and S. Wolf, J. Phys. A **43**, 465305 (2010).
- [32] K. Horodecki, *On distinguishing nonsignaling boxes via completely locality preserving operations*, In preparation.
- [33] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States. An Introduction to Quantum Entanglement* (Cambridge University Press, 2006).