

Multi-User Non-Locality Amplification

Helen Ebbe and Stefan Wolf

Abstract—*Non-local correlations* are among the most fascinating features of quantum theory from the point of view of information: Such correlations, although not allowing for signaling, are unexplainable by pre-shared information. The correlations have applications in cryptography, communication complexity, and sit at the very heart of many attempts of understanding quantum theory — and its limits — in terms of classical information. In these contexts, the question is crucial whether such correlations can be *amplified* or *distilled*, *i.e.*, whether and how weak correlations can be used for generating (a smaller amount of) stronger. Whereas the question has been studied quite extensively for *bipartite* correlations (yielding both pessimistic and optimistic results), only little is known in the *multi-partite* case.

We introduce a general framework of reductions between multi-party input-output systems. Within this formalism, we show that a natural n -party generalization of the well-known *Popescu-Rohrlich box* can be distilled, by an adaptive protocol, to the algebraic maximum. We use this result further to show that a much broader class of correlations, including *all* purely three-partite correlations, can be distilled from arbitrarily weak to almost maximal strength with *partial communication*, *i.e.*, using only a subset of the channels required for the creation of the same correlation from scratch. Alternatively, this means that arbitrarily weak non-local correlations can have a “communication value” in the context of the generation of maximal non-locality.

Index Terms—Correlation distillation, information-theoretic systems, multiparty non-locality, quantum entanglement, quantum theory

I. INTRODUCTION

ONE of the most mysterious, challenging, but also useful consequences of quantum theory are non-local correlations: The joint behavior under (different possible) measurements of a quantum system can be unexplainable by pre-shared (classical) information determining all the outcomes *locally*. This result by Bell [3] can be seen as a late reply to the claim, in 1935, of Einstein, Podolsky, and Rosen [13] that quantum theory was incomplete and must be augmented by *hidden variables*, *i.e.*, classical information predicting all measurements’ outcomes.¹

It has been a prominent open problem why nature does display non-local behavior, yet no maximal one. More specifically, why can Bell’s inequality be violated, but a perfect

Popescu-Rohrlich box [26] cannot be realized [7]? A number of attempts have been made to single out quantum correlations among general non-signaling systems: Are quantum correlations the ones that do not collapse *communication complexity* [4], that are of no help for *non-local computation* [22], that respect *information causality*, a principle generalizing the non-signaling principle to the case of limited communication [24], or that are *locally orthogonal* [16], *i.e.*, respect Specker’s principle that if *any pair* of questions about a system can be answered, then *all questions together* can be answered simultaneously [6]?

It has turned out that non-local correlations have important applications for information processing, *e.g.*, device-independent cryptography or communication complexity. In all these contexts, a question of paramount importance is the one of *distillation of non-locality*: Given weak correlations, is it possible to generate stronger ones by local wirings? For instance, distillation can potentially lead to higher confidentiality levels or to a collapse of communication complexity by (apparently) weak correlations.

In the two-party scenario, the possibility of distillation has already been extensively studied and, notably, led to complementary results adding up to a pretty complete picture: Whereas *isotropic CHSH-type* [8] correlations seem undistillable [11], the same fails to hold in general [14], [5], [20]. In fact, certain arbitrarily weak CHSH correlations can even be distilled up to virtually perfect PR boxes by adaptive protocols.

In the case of three or more parties, much less is known. It was shown that the straight-forward generalization of the (non-adaptive) XOR protocol [14] to more parties fails to distill extremal boxes of the non-signalling polytope to almost-perfect [21].

The contribution of the present work is as follows: We introduce a general framework for reductions of systems. In this model, we show that the natural generalization of PR boxes to n parties has the property that non-isotropic faulty versions thereof can be distilled to close-to-perfect by a multi-party variant of Brunner and Skrzypczyk’s [5] protocol (Section IV). This result is used to show distillability for a much larger class of correlations, where the distillation is supported by partial communication, *i.e.*, a subset of the parties is allowed to communicate, whereas this communication *alone* is insufficient for generating the target correlation (Section V). We call this partial communication supported distillation *non-locality amplification*. The result can alternatively be interpreted as arbitrarily weak non-local correlations having a “communication value” in the context of the generation of almost-perfect systems. In Section VI, the general results and procedures are illustrated with two examples.

Manuscript submitted July 30, 2013. This work was supported by the Swiss National Science Foundation (SNF), the NCCR “Quantum Science and Technology” (QSIT), and the COST action on “Fundamental Problems in Quantum Physics.” The results were presented in part at ISIT 2013 [12]. This article has been submitted to IEEE Transactions on Information Theory and the copyright for the article has been transferred to IEEE.

H. Ebbe and S. Wolf are with the Faculty of Informatics, University of Lugano, 6900 Lugano, Switzerland (e-mail: ebbeh@usi.ch; wolfs@usi.ch).

¹Bell’s paradox only persists under the assumption that measurement bases are chosen freely; at the same time, however, none of the *deterministic* interpretations of quantum physics satisfies with an *explanation* neither of the correlations’ origin nor of their limitations.

II. SYSTEMS, BOXES, AND NON-LOCALITY

A. Systems

Definition 1 (n -Partite System) An n -partite system is a conditional distribution

$$P_{A_1 A_2 \dots A_n | X_1 X_2 \dots X_n}, \quad (1)$$

where X_i is the input and A_i is the output variable of the i th party.

B. Boxes are Non-Signalling Systems

Definition 2 (Non-Signaling) An n -partite system with conditional probability distribution $P(a_1 a_2 \dots a_n | x_1 x_2 \dots x_n)$ is said *non-signaling* if the marginal distribution for each subset of parties $\{a_{k_1}, a_{k_2}, \dots, a_{k_m}\}$ only depends on its corresponding inputs

$$P(a_{k_1} \dots a_{k_m} | x_1 \dots x_n) = P(a_{k_1} \dots a_{k_m} | x_{k_1} \dots x_{k_m}). \quad (2)$$

An equivalent condition to Definition 2 can be found in [23], [1]:

$$\sum_{a_k} P(a_1 \dots a_k \dots a_n | x_1 \dots x_k \dots x_n) = \sum_{a_k} P(a_1 \dots a_k \dots a_n | x_1 \dots x'_k \dots x_n) \quad (3)$$

for all $k \in \{1, 2, \dots, n\}$, all inputs a_1, a_2, \dots, a_n , and outputs $x_1, x_2, \dots, x_{k-1}, x_k, x'_k, x_{k+1}, \dots, x_n$.

Definition 3 (n -Partite Box) An n -partite box is a n -partite system that is non-signaling.

The ranges of A_i and X_i , respectively, are arbitrary sets \mathcal{A}_i and \mathcal{X}_i .

C. Multipartite Locality

Of central interest for us are n -partite boxes with the property that the parties cannot simulate the behavior of the box without communication but shared randomness only. This property is called *non-locality*.

Definition 4 (Local Box) An n -partite box with input variables X_1, X_2, \dots, X_n and output variables A_1, A_2, \dots, A_n is local if

$$P_{A_1 A_2 \dots A_n | X_1 X_2 \dots X_n} = \sum_{r \in \mathcal{R}} P_R(r) \cdot P_{A_1 | X_1}^r \dots P_{A_n | X_n}^r \quad (4)$$

for some random variable R .

Equivalently, there exists a distribution P under which all joint outputs coexist.

Lemma 1 (Locality means Realism) A box P is local if and only if there exists a distribution

$$P'_{A_{1,0} A_{1,1} \dots A_{1,|\mathcal{X}_1|-1} A_{2,0} \dots A_{2,|\mathcal{X}_2|-1} \dots A_{n,0} \dots A_{n,|\mathcal{X}_n|-1}} \quad (5)$$

with the property that its marginals satisfy

$$P'_{A_{1,i_1} \dots A_{n,i_n}} = P_{A_1 \dots A_n | X_1 = i_1, \dots, X_n = i_n} \quad (6)$$

for any $i_j \in \mathcal{X}_j$ for $j \in \{1, 2, \dots, n\}$.

Proof: We assume that P' exists and define the random variable

$$R := A_{1,0} A_{1,1} \dots A_{1,|\mathcal{X}_1|-1} A_{2,0} \dots A_{n,0} \dots A_{n,|\mathcal{X}_n|-1}. \quad (7)$$

Obviously, this random variable R satisfies (4).

Assume that P is local. In order to see that P' exists, we define

$$P'_{A_{1,0} A_{1,1} \dots A_{n,0} A_{n,1}}(a_{1,0} a_{1,1} \dots a_{n,0} a_{n,1}) := \sum_{r \in \mathcal{R}} P_R(r) \cdot \prod_{i=1}^n P_{A_i | X_i}^r(a_{i,0}, 0) \cdot P_{A_i | X_i}^r(a_{i,1}, 1) \quad (8)$$

and compute the marginals. ■

Throughout, the remainder of this article, all the ranges \mathcal{A}_i and \mathcal{X}_i are assumed to be $\{0, 1\}$.

D. Specific Non-Local Boxes

We define certain classes and specific types of n -partite boxes which we will use for our reductions. They are generalizations of the bipartite boxes studied in [14], [5], [2].

We focus our attention to *full-correlation boxes*. Intuitively speaking, such a box displays correlation only with respect to the *full* set of players.

In the following definitions, the n -tuple of inputs is denoted by $\mathbf{x} = (x_1, x_2, \dots, x_n)$, where $x_i \in \{0, 1\}$. The n -tuple of outputs is $\mathbf{a} = (a_1, a_2, \dots, a_n)$, where $a_i \in \{0, 1\}$ for all i .

Definition 5 (Full-Correlation Box) An n -partite *full-correlation box* is characterized by the following conditional distribution:

$$P(\mathbf{a} | \mathbf{x}) = \begin{cases} \frac{1}{2^{n-1}} & \sum_i a_i \equiv f(\mathbf{x}) \pmod{2} \\ 0 & \text{otherwise,} \end{cases} \quad (9)$$

where $f(\mathbf{x})$ is a Boolean function of the inputs.

Two special cases of the full-correlation boxes are the *n -partite Popescu-Rohrlich box* and the *even-parity box for n parties*.

Definition 6 (n -Partite Popescu-Rohrlich Box) An n -partite *Popescu-Rohrlich box* (or *n -PR box*) is characterized by the following conditional distribution

$$P_n^{\text{PR}}(\mathbf{a} | \mathbf{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_i a_i = \prod_i x_i \\ 0 & \text{otherwise.} \end{cases} \quad (10)$$

Definition 7 (n -Partite Even-Parity Box) An *even-parity box for n parties* is characterized by the following conditional distribution

$$P_n^c(\mathbf{a} | \mathbf{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_i a_i = 0 \\ 0 & \text{otherwise.} \end{cases} \quad (11)$$

Note that the box of Definition 7 is *local*. A convex combination of the boxes of Definitions 6 and 7 is called a *correlated non-local box for n parties*.

Definition 8 (Correlated Non-Local Boxes) The family of correlated non-local boxes for n parties is defined by

$$P_{n,\varepsilon}^{\text{PR}} = \varepsilon P_n^{\text{PR}} + (1 - \varepsilon) P_n^c, \quad (12)$$

where $0 \leq \varepsilon \leq 1$.

E. Communication as Systems

In the protocols below, we will not only use n -partite boxes as resources, but also communication between some of the parties, *i.e.*, signaling systems. This partial communication can be seen as a directed graph G with n vertices and directed edges which correspond to the one-way communication channel between the n parties. We denote the one-way communication channels with $C(G)$, these channels can be used once in arbitrary order.

III. A REDUCTION CALCULUS FOR SYSTEMS

A. Protocols

A *protocol* is a distributed algorithm that takes the inputs of the parties and produces outputs for every one. If the protocol also takes shared systems to produce outputs, it is called a *reduction protocol*. Its goal can be to simulate some target system T , either perfectly or arbitrarily precisely [15]. Assume there are n parties that share m n -partite systems S_1, S_2, \dots, S_m and a random variable R . The parties get the input $\mathbf{x} = (x_1, x_2, \dots, x_n)$, and finally, they output $\mathbf{a} = (a_1, a_2, \dots, a_n)$. During the protocol, the parties are allowed to apply any classical circuitry to their local parts of the shared system. Such a circuitry is called *wiring* and consists of choices for the inputs of the boxes and the generation of the outputs [1], [27].

Definition 9 (Adaptive Protocol) In an *adaptive protocol*, every Party i gets the input x_i and acts as follows: Party i inputs $f_j(x_i, R, b_{i_1}, b_{i_2}, \dots, b_{i_{j-1}})$ to the shared system S_{i_j} for all $j \in \{1, 2, \dots, m\}$, where the index i_j depends on x_i, R , and the former output bits $b_{i_1}, b_{i_2}, \dots, b_{i_{j-1}}$. The system S_{i_j} outputs b_{i_j} to party i . The final output of Party i is given by the function $f^{x_i}(R, b_1, b_2, \dots, b_m)$.

Definition 10 (Non-Adaptive Protocol) In a *non-adaptive protocol*, every Party i gets the input x_i and acts as follows: Party i inputs $f_j(x_i, R)$ to the shared system S_j for all $j \in \{1, 2, \dots, m\}$. The system S_j outputs b_j to party i . The final output of Party i is given by the function $f^{x_i}(R, b_1, b_2, \dots, b_m)$.

In contrast to adaptive protocols, no input of a system depends on the output of another one in a non-adaptive protocol.

B. Resources Inequalities

In the following, we use *resources inequalities* as introduced in [9], [10], [19]. They are used to express whether some resource can be simulated by other resources plus shared randomness. Assume we have two systems R and R' . We write

$$R \succeq R' \quad (13)$$

if there exists a protocol that simulates R' using R and shared randomness.

Clearly, if (13) holds, then there also exists a protocol that simulates R' using arbitrarily many copies of R (k copies of R is written as $R^{\otimes k}$), an arbitrary other resource R'' , and shared randomness

$$\{R^{\otimes k}, R''\} \succeq R', \quad (14)$$

where $k \in \mathbb{N} \cup \{\infty\}$.

We write

$$R \succeq^* R' \quad (15)$$

if there exists a protocol that simulates R' using arbitrary many copies of R and shared randomness. If R' can be simulated arbitrarily precisely with a small number of copies of R then we write

$$R \rightarrow^* R'. \quad (16)$$

C. Examples of Reductions

With this notation, we are able to rephrase some well-known results. Obviously,

$$\emptyset \succeq P \quad (17)$$

if and only if P is local.

From the definition of correlated non-local boxes for n parties, we know that such a box is a convex combination of the even-parity box P_n^c and the n -PR box P_n^{PR} . Since the even parity box is local, $\emptyset \succeq P_n^c$ and, therefore,

$$P_{n,\varepsilon'}^{\text{PR}} \succeq P_{n,\varepsilon}^{\text{PR}} \quad \text{for all } 0 \leq \varepsilon \leq \varepsilon' \leq 1. \quad (18)$$

In a Section IV, we see that for every $0 < \varepsilon < 1$ exists $\varepsilon' > \varepsilon$ such that

$$P_{n,\varepsilon}^{\text{PR} \otimes 2} \succeq P_{n,\varepsilon'}^{\text{PR}}, \quad (19)$$

and for all $0 < \varepsilon < 1$

$$P_{n,\varepsilon}^{\text{PR}} \rightarrow^* P_n^{\text{PR}}. \quad (20)$$

IV. MULTI-PARTY NON-LOCALITY DISTILLATION

Non-locality distillation protocols are executed by n parties without communication. The protocol simulates a binary input/output system by classical (local) operations on non-local boxes [14]. The goal is to use weak non-local boxes for simulating stronger ones. Since these protocols only use a given set of boxes and local operations that can be simulated by shared randomness, we can describe the result of the non-locality distillation as a resources inequality: Assume that the distillation protocol uses as resources the boxes P_1, P_2, \dots, P_n , where $n \in \mathbb{N} \cup \{\infty\}$, to simulate the box P . Therefore, we get the resources inequality

$$\{P_1, P_2, \dots, P_n\} \succeq P. \quad (21)$$

Brunner and Skrzypczyk [5] proposed an adaptive protocol for two parties that distills non-locality in the asymptotic limit: All correlated non-local boxes are distilled arbitrarily closely to the (maximally non-local) PR box. In the notation of resources inequalities, we could describe this kind of distillation as

$$P_{2,\varepsilon}^{\text{PR} \otimes 2} \succeq P_{2,\varepsilon'}^{\text{PR}} \quad (22)$$

and

$$P_{2,\varepsilon}^{\text{PR}} \rightarrow^* P_2^{\text{PR}}, \quad (23)$$

where $0 < \varepsilon < 1$ and $\varepsilon' = \varepsilon/2 \cdot (3 - \varepsilon) > \varepsilon$. We extend this to all n -partite PR boxes in Protocol 1 and Theorem 1.

Protocol 1 (Generalized BS Protocol for n -PR Boxes) *All n parties share two boxes, where we denote by x_i the value that the i th party inputs to the first box and by y_i the value that the i th party inputs to the second box. The output bit of the first box for the i th party is a_i , and the output bit of the second box is b_i . The n parties proceed as follows: $y_i = x_i \bar{a}_i$ and they output, finally, $c_i = a_i \oplus b_i$ (see also Fig. 1).*

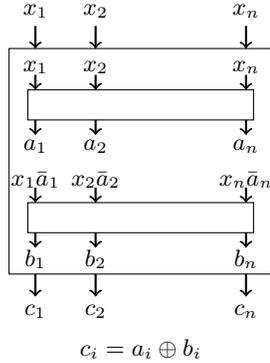


Figure 1. Generalized BS Protocol for n -PR boxes

Theorem 1 *Protocol 1 distills two copies of an arbitrary box $P_{n,\varepsilon}^{\text{PR}}$ with $0 < \varepsilon < 1$ to an n -partite correlated non-local box $P_{n,\varepsilon'}^{\text{PR}}$ with $\varepsilon' > \varepsilon$.*

$$P_{n,\varepsilon}^{\text{PR} \otimes 2} \succeq P_{n,\varepsilon'}^{\text{PR}}. \quad (24)$$

In the asymptotic limit of many copies, Protocol 1 distills any $P_{n,\varepsilon}^{\text{PR}}$ with $\varepsilon > 0$ to a box arbitrarily closely to the n -PR box

$$P_{n,\varepsilon}^{\text{PR}} \rightarrow^* P_n^{\text{PR}}. \quad (25)$$

In the language of distillation, we say that in the asymptotic case of many copies, any $P_{n,\varepsilon}^{\text{PR}}$ with $\varepsilon > 0$ can be distilled arbitrarily closely to the n -PR box. This shows that also in the multipartite case, non-locality can be distilled.

Proof: We introduce the notation $A \triangleright B$, which means that the first box in Protocol 1 acts like A and the second one like B . The initial two-box state of Protocol 1 is given by

$$\begin{aligned} P_{n,\varepsilon}^{\text{PR}} \triangleright P_{n,\varepsilon}^{\text{PR}} &= \varepsilon^2 P_n^{\text{PR}} \triangleright P_n^{\text{PR}} \\ &+ \varepsilon(1 - \varepsilon) (P_n^{\text{PR}} \triangleright P_n^c + P_n^c \triangleright P_n^{\text{PR}}) \\ &+ (1 - \varepsilon)^2 P_n^c \triangleright P_n^c. \end{aligned} \quad (26)$$

We apply Protocol 1 and get the following relations: $P_n^{\text{PR}} \triangleright P_n^{\text{PR}} \equiv P_n^{\text{PR}}$ (i.e., P_n^{PR} is a fixpoint), $P_n^{\text{PR}} \triangleright P_n^c \equiv P_n^{\text{PR}}$, $P_n^c \triangleright P_n^{\text{PR}} \equiv 2^{1-n} P_n^{\text{PR}} + (1 - 2^{1-n}) P_n^c$, and $P_n^c \triangleright P_n^c \equiv P_n^c$.

After the application of Protocol 1, we get the final box, which is

$$\begin{aligned} P_{n,\varepsilon'}^{\text{PR}} &= \frac{\varepsilon}{2^{n-1}} (2^{n-1} + 1 - \varepsilon) P_n^{\text{PR}} \\ &+ \left(1 - \frac{\varepsilon}{2^{n-1}} (2^{n-1} + 1 - \varepsilon)\right) P_n^c. \end{aligned} \quad (27)$$

Hence, $\varepsilon' = \varepsilon/2^{n-1} \cdot (2^{n-1} + 1 - \varepsilon)$. We show that $\varepsilon' > \varepsilon$ for all $0 < \varepsilon < 1$, therefore, the protocol takes any correlated non-local box $P_{n,\varepsilon}^{\text{PR}}$ to a stronger box $P_{n,\varepsilon'}^{\text{PR}}$.

We show that in the asymptotic regime of many copies, any $P_{n,\varepsilon}^{\text{PR}}$ with $0 < \varepsilon < 1$ can be distilled arbitrarily closely to the n -PR box. We are starting with 2^m copies of the box $P_{n,\varepsilon}^{\text{PR}}$ and get, finally, the box $P_{n,\varepsilon_m}^{\text{PR}}$, where

$$T_n(\varepsilon) = \frac{\varepsilon}{2^{n-1}} (2^{n-1} + 1 - \varepsilon), \quad (28)$$

$$\varepsilon_m = T_n(\varepsilon_{m-1}), \quad \text{and} \quad \varepsilon_0 := \varepsilon. \quad (29)$$

The fixed points of this map are $\varepsilon = 0$ and $\varepsilon = 1$. To analyze the stability of these two fixed points we calculate the eigenvalues of the Jacobian (since the map is one-dimensional, the Jacobian is a real value and not a matrix). For the box P_n^c ($\varepsilon = 0$), we find $dT_n/d\varepsilon|_{\varepsilon=0} = 1 + 1/2^{n-1} > 1$, so this box is repulsive. For the other box P_n^{PR} we find $dT_n/d\varepsilon|_{\varepsilon=1} = 1 + 1/2^{n-1} - 1/2^{n-2} < 1$; the box is attractive. ■

V. MULTI-PARTY NON-LOCALITY AMPLIFICATION

The generalized BS protocol can be used to obtain non-locality amplification protocols for full-correlation boxes, where the use of communication is allowed to some of the parties. We allow a subset of the parties to use one-way communication channels (as often as required). We show that we are able to amplify a general class of full-correlation boxes arbitrarily closely to the maximum with such protocols.

A. Construction of Full-Correlation Boxes

Lemma 2 *If f is a Boolean function of the input elements x_1, x_2, \dots, x_n , then it can be written as*

$$f(x_1, \dots, x_n) = \bigoplus_{I \in \mathcal{I}} \left(a_I \cdot \bigwedge_{i \in I} x_i \right), \quad (30)$$

where $\mathcal{I} = \mathcal{P}(\{1, 2, \dots, n\})$ and $a_I \in \{0, 1\}$ for all $I \in \mathcal{I}$.

Hence, it is obvious that the full-correlation box associated to the Boolean function f can be constructed by $\sum_{I \in \mathcal{I}} a_I$ n -PR boxes. Indeed, for every $a_I = 1$, an n -PR box is needed, where the i th party inputs x_i if $i \in I$, and otherwise he inputs 1. Then, the box will output b_i^I . In the end, every party outputs $c_i = \bigoplus_{I \in \mathcal{I}, a_I=1} b_i^I$. For an example, see Fig. 2. Note that the n -PR boxes belonging to a_I where $|I| \leq 1$ are local and can be simulated by local operations and shared randomness.

We already know that all n -partite full-correlation boxes can be simulated by n -partite PR boxes. We define the set of all n -PR boxes that are needed to simulate the full-correlation box: Let

$$\mathcal{J} := \{I \in \mathcal{I} \mid a_I = 1 \text{ and } |I| \geq 2\}. \quad (31)$$

This set can be partitioned into pairwise disjoint subsets $\{J_1, J_2, \dots, J_{n_{\mathcal{J}}}\}$ such that all $A \in J_i$ and $B \in J_j$ fulfill $A \cap B = \emptyset$ for all $i \neq j$. We define the maximal number of such subsets as $n_{\mathcal{J}}$ and denote this partition as the

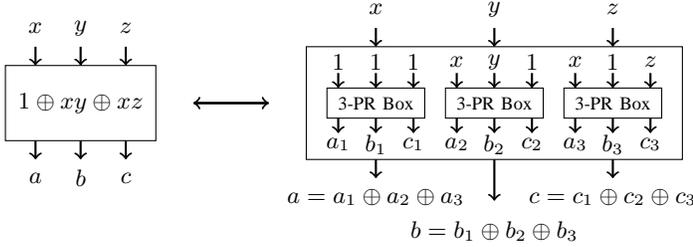


Figure 2. Construction of the $1 \oplus xy \oplus xz$ -Box

empty-overlap partition of \mathcal{J} . We define, for all $I \in \mathcal{J}$, $m_I := |I \setminus \bigcup_{J \in \mathcal{J} \setminus I} J|$, i.e., the number of variables that only appear in the non-local box corresponding to $I \in \mathcal{J}$.

We take two full-correlation boxes. The first is given by

$$P_1(a_1 \cdots a_{k_2} | x_1 \cdots x_{k_2}) = \begin{cases} \frac{1}{2^{k_2-1}} & \bigoplus_{i=1}^{k_2} a_i = g_1(x_1, \dots, x_{k_2}) \\ 0 & \text{otherwise,} \end{cases} \quad (32)$$

where g_1 is a Boolean function which depends on all of its input variables, and $k_2 < n$. The second box is defined as

$$P_2(b_{k_1} \cdots b_n | x_{k_1} \cdots x_n) = \begin{cases} \frac{1}{2^{n-k_1}} & \bigoplus_{i=k_1}^n b_i = \prod_{i=k_1}^{k_3} x_i \\ 0 & \text{otherwise,} \end{cases} \quad (33)$$

where $0 < k_1 < k_2 < k_3 \leq n$. We construct an n -partite full-correlation box with these two boxes by taking the XOR of the two outputs a_i and b_i if Party i participates at both boxes, otherwise the party outputs a_i or b_i :

$$c_i = \begin{cases} a_i & i \in \{1, 2, \dots, k_1 - 1\} \\ a_i \oplus b_i & i \in \{k_1, k_1 + 1, \dots, k_2\} \\ b_i & i \in \{k_2 + 1, k_2 + 2, \dots, n\}. \end{cases} \quad (34)$$

Lemma 3 *Box (34) is equal (i.e., the joint probabilities are equal) to the full-correlation box defined by*

$$P(c|x) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_{i=1}^n c_i = g_1(x_1, \dots, x_{k_2}) \oplus \prod_{i=k_1}^{k_3} x_i \\ 0 & \text{otherwise.} \end{cases} \quad (35)$$

Proof: The statement follows directly from the property of the full-correlation box that the set of outputs of any subset of $n - 1$ parties (or smaller) is completely random [2], and the property that the XOR conserves randomness in case of independence. ■

Theorem 2 (Construction of a Full-Correlation Box) *Let P^f be the full-correlation box associated to the Boolean function f , and let f be written as in Lemma 2. If f fulfills $n_{\mathcal{J}} = 1$, then there exist subsets of parties such that the full-correlation box can be simulated with generalized PR boxes shared between the parties of a subset with the condition that the number of PR boxes in that some parties inputs all the time a constants is at most one.*

Proof: We replace full-correlation boxes with $a_I = 1$ for $|I| \leq 1$ by the full-correlation box with $a_I = 0$ for $|I| \leq 1$,

and all other a_I for all $I \in \mathcal{I} \setminus \{\emptyset\}$ keep their values (i.e., we ignore the *trivial part of the box*). We can do this by taking the XOR of the original box and the local box with $a_I = 1$ for $|I| \leq 1$. To get our original box back in the end, we take again the XOR of the modified box and the local box.

We replace the boxes step by step. In the first step, we are beginning with a n -PR box with the associated set I . To that end, we are looking for another n -PR box with associated set J such that $I \cap J \neq \emptyset$ (this is possible because of the assumption made). Because of Lemma 3, we are able to replace these two boxes by two smaller boxes: We substitute the first box by an $|I \setminus J|$ -PR box with inputs I . The second box is substituted by an $(n - |I|)$ -box, where we input J and for the parties $\{1, 2, \dots, n\} \setminus (I \cup J)$, we input 1.

Assume that we have, in this way, replaced some n -PR boxes by new boxes. Let there be a further n -PR box which is not yet replaced, and whose input elements intersect with the input elements of the new box. We are making the same steps as before to replace these two boxes. In the end, we have replaced all n -PR boxes by a new box with the claimed properties. ■

B. Imperfect Full-Correlation Boxes

Assume we have a non-local full-correlation box P^f associated to the Boolean function f and a local full-correlation box P^{f_l} associated to the Boolean function

$$f_l = \bigoplus_{I \in \mathcal{I} \setminus \mathcal{J}} \bigwedge_{i \in I} x_i, \quad (36)$$

where \mathcal{J} and the a_i 's are with respect to the function f . This box corresponds to the trivial part of the full-correlation box P^f .

The imperfect box P_ε^f is defined as the convex combination of these two boxes,

$$P_\varepsilon^f = \varepsilon P^f + (1 - \varepsilon) P^{f_l}, \quad (37)$$

where $0 < \varepsilon < 1$.

We define the XOR of boxes:

Definition 11 (XOR of boxes) Let P and P' be two n -partite boxes that output (a_1, a_2, \dots, a_n) , resp. (b_1, b_2, \dots, b_n) , for the input (x_1, x_2, \dots, x_n) . The XOR of the two boxes P and P' , i.e., $P \oplus P'$, is an n -partite box P^* with output $(a_1 \oplus b_1, a_2 \oplus b_2, \dots, a_n \oplus b_n)$ for the input (x_1, x_2, \dots, x_n) .

Definition 12 (XOR* of boxes) Let P_1 and P_2 be two n -partite full correlation boxes, and $P_{i,\varepsilon} = \varepsilon P_1 + (1 - \varepsilon) P^c$ for $i \in \{1, 2\}$. The XOR* of $P_{1,\varepsilon}$ and $P_{2,\varepsilon}$, i.e., $P_{1,\varepsilon} \oplus^* P_{2,\varepsilon}$, is defined by

$$\begin{aligned} P_{i,\varepsilon} \oplus^* P_{j,\varepsilon} &:= \varepsilon P_i \oplus P_j + (1 - \varepsilon) P^c \oplus P^c \\ &= \varepsilon P_i \oplus P_j + (1 - \varepsilon) P^c. \end{aligned} \quad (38)$$

We can assume without loss of generality that P^{f_l} is the even-parity box ($f_l = 0$, if this is not the case redefine $P_{\text{new}}^f = P^f \oplus P^{f_l}$, $P_{\text{new}}^{f_l} = P^{f_l} \oplus P^{f_l}$, and $P_{\varepsilon,\text{new}}^f = P_\varepsilon^f \oplus P^{f_l}$). Note that the box P^f can be written as the XOR of generalized n -PR boxes P_1, P_2, \dots, P_m as seen in Section V-A

$$P^f = P_1 \oplus P_2 \oplus \dots \oplus P_m. \quad (39)$$

For that reason, P_ε^f can be rewritten as

$$P_\varepsilon^f = P_{1,\varepsilon} \oplus^* P_{2,\varepsilon} \oplus^* \cdots \oplus^* P_{m,\varepsilon}, \quad (40)$$

where $P_{i,\varepsilon} = \varepsilon P_i + (1 - \varepsilon) P^c$ for all $i \in \{1, 2, \dots, m\}$. That means we can simulate the box P_ε^f with imperfect full-correlation boxes that all work correctly at the same time or all work incorrectly at the same time.

Theorem 3 (Construction of an Imperfect F-C. Box) *Let $0 < \varepsilon < 1$, let P^f be a full-correlation box associated to the Boolean function f , let f be written as in Lemma 2, and let P_ε^f be defined as above. If f fulfills $n_{\mathcal{J}} = 1$, then there exists subsets of parties such that the box P_ε^f can be simulated with imperfect generalized PR-boxes shared between the parties of a subset with the condition that the number of imperfect PR boxes in that some parties inputs all the time a constants is at most one. If all these imperfect generalized PR boxes work at the same time correctly and at the same time incorrectly then the simulation is equivalent to the box P_ε^f .*

Proof: The proof is similar to the proof of Theorem 2. ■

C. Protocols Based on Partial Communication

Assume we have an n -partite full-correlation box P^f that is to be simulated by one-way communication channels and shared randomness. The question is: How many one-way communication channels do we need for simulating an n -partite full-correlation box? Theorem 4 answers this question.

Theorem 4 (Number of Communication Channels) *Let f be the Boolean function associated to an n -partite full-correlation box P^f , and let f be defined as in Lemma 2. The number $N_{comm}^{scratch}$ of one-way communication channels to simulate the full-correlation box from scratch is*

$$N_{comm}^{scratch} = \left| \bigcup_{I \in \mathcal{J}} I \right| - n_{\mathcal{J}}. \quad (41)$$

Proof: We first prove the statement for $n_{\mathcal{J}} = 1$ by induction. We ignore the local part of the Boolean function f (i.e., the terms of single variables) and start with the case when the function f depends on two variables. The case $|\mathcal{J}| = 2$ is equivalent to a PR box. From [25], we know that it can be simulated by one one-way communication channel. Now, we assume that the claim is true for $|\mathcal{J}| \leq n$. Assume further that we have a function with $|\mathcal{J}| = n + 1$ that still fulfills the assumption. We substitute 1 for x_i , where x_i is the input which is an element of a minimal number of elements of \mathcal{J} . This new function also fulfills the assumption of the theorem. We also know that $|\mathcal{J}| = n$ and, therefore, we need $n - 1$ communication channels to simulate the associated box. We combine all these n function values into one variable. The original function can be written with two variables. Therefore, we are back at the case $|\mathcal{J}| = 2$. Together, we need n one-way communication channels for simulating a function with $|\mathcal{J}| = n + 1$.

Assume now $n_{\mathcal{J}} > 1$. We write the original full-correlation box as a combination of $n_{\mathcal{J}}$ other non-local full-correlation

boxes and at most one local full-correlation box (that can be simulated by shared randomness). Each of these boxes belongs to one of the sets of the empty-overlap partition $\{J_1, J_2, \dots, J_{n_{\mathcal{J}}}\}$ of \mathcal{J} . The full-correlation box that belongs to J_i is defined by the function

$$f_i(x_1, x_2, \dots, x_n) = \bigoplus_{J \in J_i} \bigwedge_{j \in J} x_j. \quad (42)$$

From the first part of the proof, we know that we need $|\bigcup_{J \in J_i} J| - 1$ communication channels to simulate this box from scratch. Thus, we need to simulate all the $n_{\mathcal{J}}$ n -partite non-local full-correlation boxes, for which we need

$$N_{comm}^{scratch} = \left| \bigcup_{I \in \mathcal{J}} I \right| - n_{\mathcal{J}} \quad (43)$$

communication channels. ■

From Theorem 4, we know that all parties that belong to one of the sets of the empty-overlap partition of \mathcal{J} , say J_i , have to communicate directly or indirectly to one of these parties. Corollary 1 follows from this property.

Corollary 1 *Let f be the Boolean function associated to an n -partite full-correlation box P^f , and let f be defined as in Lemma 2. Then*

$$C(G) \succeq P^f, \quad (44)$$

where G is a directed graph with n vertices and the property that for every set J_i , i.e., a set of the empty-overlap partition of \mathcal{J} , there exists a vertex $v \in (\bigcup_{J \in J_i} J)$ such that from every other vertex $w \in (\bigcup_{J \in J_i} J)$, there exists a path to v for all $i \in \{1, 2, \dots, n_{\mathcal{J}}\}$.

D. Protocol Based on Brunner/Skrypczyk-Protocol that Allows Partial Communication

We have seen protocols that only use copies of some given boxes or partial communication. Now we study a combination of them.

Theorems 5 and 6 state that a general class of full-correlation boxes can be simulated by (distillation) protocols and classical one-way communication channels. The number of these one-way channels is then smaller than the number of one-way communication channels we need if we do not apply a distillation protocol, i.e., operate from scratch. More specifically, there exists a minimal set of one-way communication channels that simulates such a full-correlation box, but only a subset of these channels is used to simulate the box using a (distillation) protocol.

Assume we have the non-local full-correlation box P^f associated to the Boolean function f . Let the boxes P_i^f and P_ε^f be defined as in Section V-B. We show that the box P_ε^f can be distilled arbitrarily closely to the full-correlation box P^f using partial communication if it fulfills certain conditions.

Theorem 5 (Distillation with Communication I) *Let $0 < \varepsilon < 1$, let P^f be a full-correlation box associated to the Boolean function f , let f be written as in Lemma 2, and let the box P_ε^f be defined as in Section V-B. If f fulfills $n_{\mathcal{J}} = 1$, then the number $N_{comm}^{distill}$ of one-way communication channels*

required for distilling the box P_ε^f up to the full-correlation box P^f with using the generalized BS protocol is

$$N_{comm}^{distill} \leq \begin{cases} n-1 - \max_{I \in \mathcal{J}}(m_I) & \max_{I \in \mathcal{J}}(m_I) \neq n \\ 0 & \max_{I \in \mathcal{J}}(m_I) = n. \end{cases} \quad (45)$$

Proof: Here, we replace full-correlation boxes with $a_I = 1$ for $|I| \leq 1$ by the full-correlation box with $a_I = 0$ for $|I| \leq 1$, and the other a_I , for all $I \in \mathcal{I} \setminus \{\emptyset\}$, keep their values. We do the same with the imperfect full-correlation box P_ε^f . We can do this by taking the XOR of the original box and the local box with $a_I = 1$ for $|I| \leq 1$. To get our original box back in the end, we take again the XOR of the modified box and the local box.

We assume that the replacement is made according to Theorem 3. We have replaced the original correlated n -partite boxes in such a way that the correlated box with constant input does not correspond to the original correlated n -partite box belonging to the largest m_I . This is possible since we can replace this box first. We are now able to isolate the box belonging to the largest m_I . Therefore, we allow all parties that appear at least twice as well as the parties that input all the time a constant to communicate their inputs and outputs to a party that also has an input for the isolated box. We have isolated the correlated multipartite box belonging to the largest m_I , and we are able to apply the generalized BS protocol to this box. All the other correlated boxes that appear in the abstraction of Theorem 3 can be simulated by the communication of the parties and shared randomness. So we will need $\max_{I \in \mathcal{J}}(m_I)$ one-way-communication channels less than if we started from scratch. ■

The following is a corollary of Theorem 5:

Corollary 2 *Let $0 < \varepsilon < 1$, let P^f be a full-correlation box associated to the Boolean function f , let f be written as in Lemma 2, and let I be the set of the inputs of the box that belongs to the largest m_I . If f fulfills $n_{\mathcal{J}} = 1$, then*

$$\{P_\varepsilon^f, C(G)\} \rightarrow^* P^f, \quad (46)$$

where the box P_ε^f is defined as in Section V-B and G is a directed graph with n vertices with the property that there exists a vertex $v \in (\bigcup_{J \in \mathcal{J}} J) \cap I$ such that from every vertex $w \in (\{1, 2, \dots, n\} \setminus I) \cup (\bigcup_{J \in \mathcal{J}} J)$, there exists a path to v .

Corollary 3 *Let $0 < \varepsilon < 1$, let P^f be a full-correlation box associated to the Boolean function f , and let f be written as in Lemma 2. If $n_{\mathcal{J}} = 1$ and $\max_{I \in \mathcal{J}}(m_I) > n - |\bigcup_{I \in \mathcal{J}} I|$, then*

$$N_{comm}^{distill} < N_{comm}^{scratch}, \quad (47)$$

where $N_{comm}^{distill}$ is the number of one-way communication channels needed for distilling the box P_ε^f that is defined as in Section V-B.

Proof: The statement follows from Theorems 4 and 5. ■

Theorem 6 (Distillation with Communication II) *Let $0 < \varepsilon < 1$, let P^f be a full-correlation box associated to the Boolean function f , let f be written as in Lemma 2, and let*

the box P_ε^f be defined as in Section V-B. If

$$\max_{I \in \mathcal{J}}(m_I) > n - \left| \bigcup_{I \in \mathcal{J}} I \right|, \quad (48)$$

and $n_{\mathcal{J}} = 1$, then there exists a graph G with $N_{comm}^{scratch}$ directed edges and a proper subgraph $G' \subset G$ with $N_{comm}^{distill}$ directed edges such that $C(G) \succeq P^f$ and $\{P_\varepsilon^f, C(G')\} \rightarrow^* P^f$.

Proof: The statement follows from Theorems 4 and 5, and Corollary 1. ■

All extremal three-partite full-correlation boxes of the non-signalling polytope fulfill the conditions of Corollary 6. For more parties, it is unknown how many extremal boxes also fulfill the condition.

VI. EXAMPLES

A. Example of an Amplifiable System

In this example, we simulate the following full-correlation box:

$$P^1(\mathbf{a}|\mathbf{x}) = \begin{cases} \frac{1}{2^3} \bigoplus_{i=1}^4 a_i = x_1 x_2 x_3 \oplus x_3 x_4 \oplus x_1 & \\ 0 & \text{otherwise.} \end{cases} \quad (49)$$

Therefore, we determine first the above-defined sets and constants. Let $\mathcal{I} = \mathcal{P}(\{1, 2, 3, 4\})$. From Lemma 2, we know that all $a_I = 1$ for $I \in \{\{1, 2, 3\}, \{3, 4\}, \{1\}\}$, and otherwise $a_I = 0$. This means that the given full-correlation box can be simulated by three 4-PR boxes with some constant inputs, where one of these boxes is local (see Fig. 3 a)). We are also able to determine the set \mathcal{J} of non-local n -PR boxes that are required to simulate the full-correlation box:

$$\mathcal{J} = \{\{1, 2, 3\}, \{3, 4\}\} \quad (50)$$

Both of these non-local 4-PR boxes can be obtained from the original box by taking the XOR of the original box and the local 4-PR box when every party inputs his bits except for the parties that input the constant 1 to the 4-PR box, they input 0 in both boxes. If we apply Theorem 5 (i), then we know that the non-local part of the original full-correlation box can be simulated by two connected n -PR boxes with no constant input (see Fig. 3 b)).

Since there is only one set in the empty-overlap partition of \mathcal{J} , $n_{\mathcal{J}} = 1$. Therefore, the number of required one-way communication channels for simulating the full-correlation box can be calculated according to Theorem 4:

$$N_{comm}^{scratch} = \left| \bigcup_{I \in \mathcal{J}} I \right| - 1 = 3. \quad (51)$$

One of the graphs that characterizes the one-way communication channels is $G = (V, E)$ with $V = \{1, 2, 3, 4, 5\}$ and $E = \{(4, 3), (3, 2), (2, 1)\}$. That leads to

$$C(G) \succeq P^1. \quad (52)$$

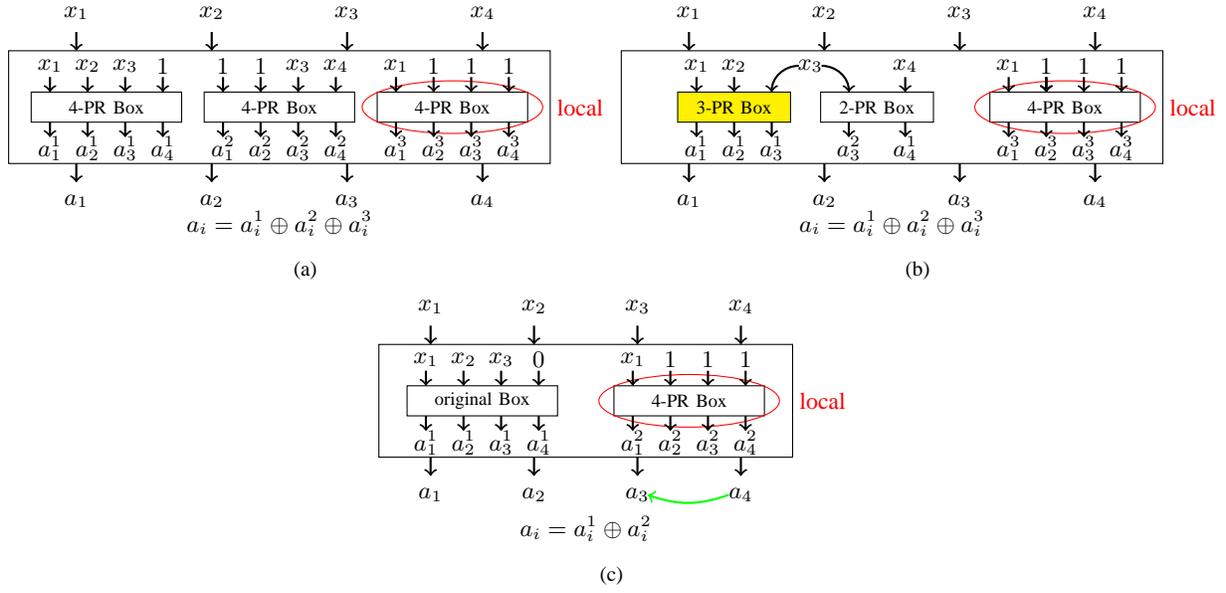


Figure 3. (a) Simulating the full-correlation box with three 4-PR boxes. (b) Simulation of the full-correlation box with generalized PR boxes without a constant input and a local box. (c) How to simulate the 3-PR box with the original full-correlation box and a local box.

Obviously, this box is not local. We define the trivial part of this full-correlation box

$$P^L(\mathbf{a}|\mathbf{x}) = \begin{cases} \frac{1}{2^3} \bigoplus_{i=1}^4 a_i = x_1 \\ 0 & \text{otherwise.} \end{cases} \quad (53)$$

We start with the second part of the example, where we show in detail how we take a box from the family $P_\varepsilon = \varepsilon P + (1-\varepsilon)P^L$, where $0 < \varepsilon < 1$, to the box $P(\mathbf{a}|\mathbf{x})$. For that, we determine first which of the parties have to communicate. Therefore, we calculate the number of parties that only belong to one of the non-local 4-PR boxes: $m_{\{1,2,3\}} = 2$ and $m_{\{3,4\}} = 1$. This means that we isolate the box that belongs to the 4-PR box with three arbitrary inputs. This can be done in the same way as before: We input $(x_1, x_2, x_3, 0)$ to P_ε and the local box and take the XOR of its outputs. Then, we use a one-way communication channel from Party 4 to 3. This corresponds to a graph $G' = (V', E')$ with $V' = V$ and $E' = \{(4, 3)\}$, which means we need one one-way communication channel. Remember that the communication channel can be used as often as required. Hence, we are able to simulate perfectly the other 2-PR boxes, and the imperfect 3-PR box can be isolated by communicating the inputs and outputs of the 2-PR box to Party 3 (see Fig. 3 c)). We have isolated the box $P_{3,\varepsilon}^{PR}$ that is known to be asymptotically distillable up to P_3^{PR} by the generalized BS protocol. In this way, we are able to take the box P_ε to the full-correlation box in the beginning. This results in the resources inequality

$$P^L \otimes^\infty \otimes C(G') \succeq P^1. \quad (54)$$

We get that G' is a proper subgraph of G and the number of one-way communication channels that is needed for this kind of protocol is $N_{comm}^{distill} = 1$, i.e., less than $N_{comm}^{scratch} = 3$.

B. Example of a Non-Amplifiable System

In this example we simulate the following full-correlation box:

$$P^2(\mathbf{a}|\mathbf{x}) = \begin{cases} \frac{1}{2^5} \bigoplus_{i=1}^6 a_i = f(x_1, x_2, \dots, x_6) \\ 0 & \text{otherwise,} \end{cases} \quad (55)$$

where $f(x_1, x_2, \dots, x_6) = x_1x_2 \oplus x_2x_3 \oplus x_4x_5x_6 \oplus x_5$.

Let $\mathcal{I} = \mathcal{P}(\{1, 2, 3, 4, 5, 6\})$. From Lemma 2 we know that all $a_I = 1$ for $I \in \{\{1, 2\}, \{2, 3\}, \{4, 5, 6\}, \{5\}\}$, and otherwise $a_I = 0$. This means that the given full-correlation box can be simulated by four 6-PR boxes with some constant inputs, where one of these boxes is local. We are also able to assign the set \mathcal{J} of non-local n -PR boxes that are needed to simulate the full-correlation box:

$$\mathcal{J} = \{\{1, 2\}, \{2, 3\}, \{4, 5, 6\}\}. \quad (56)$$

Each of these three non-local 6-PR boxes can be obtained from the original box by taking the XOR of the original box and the local 5-PR box when every party inputs its bits except for the parties that input the constant 1 to the 5-PR box, they input 0 in both boxes.

Since we know \mathcal{J} , we can determine the empty-overlap partition $\{J_1, J_2\}$, where $J_1 = \{\{1, 2\}, \{2, 3\}\}$ and $J_2 = \{\{4, 5, 6\}\}$. Therefore, $n_{\mathcal{J}} = 2$ and the number of required one-way communication channels for simulating the full-correlation box can be calculated according to Theorem 4:

$$N_{comm}^{scratch} = \left| \bigcup_{I \in \mathcal{J}} I \right| - n_{\mathcal{J}} = 4. \quad (57)$$

One of the graphs that characterizes the one-way communication channels is $G = (V, E)$ with $V = \{1, 2, 3, 4, 5, 6\}$ and $E = \{(1, 2), (2, 3), (4, 5), (5, 6)\}$. That leads us to

$$C(G) \succeq P^2. \quad (58)$$

Since $n_{\mathcal{J}} \neq 1$, Theorem 5 does not apply.

VII. CONCLUSION

We have studied the problem of non-locality distillation in the multi-partite setting. We have found, first, that arbitrarily weakly non-local non-isotropic approximations to the natural generalization of a PR box to n parties are distillable by an adaptation of a protocol for two parties. Second, this can be applied to showing that a much more general class of extremal correlations, including *all* purely three-partite correlations, can be amplified to using *partial* communication requiring only a subset of directed pairwise channels than as compared to the case when weak systems can be used. In this context, weak non-locality, hence, manages to replace communication between a subset of parties. It remains a challenging open problem to understand, classify, and apply multi-party non-locality systematically. It seems that for certain tasks (such as randomness amplification [17], [18]), multi-party non-locality outperforms bipartite correlations.

ACKNOWLEDGMENT

The authors thank Ä. Baumeler, D. Frauchiger, A. Montina, M. Pfaffhauser, J. Rashid, and B. Salwey for helpful discussions.

REFERENCES

- [1] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, “Nonlocal correlations as an information-theoretic resource,” *Phys. Rev. A*, Vol. 71, 2005.
- [2] J. Barrett and S. Pironio, “Popescu-Rohrlich correlations as a unit of nonlocality,” *Phys. Rev. Lett.*, Vol. 95, 2005.
- [3] J. S. Bell, “On the Einstein-Podolsky-Rosen paradox,” *Physics*, Vol. 1, pp. 195–200, 1964.
- [4] G. Brassard, H. Buhrman, N. Linden, A. Méthot, A. Tapp, and F. Unger, “Limit on nonlocality in any world in which communication complexity is not trivial,” *Phys. Rev. Lett.*, Vol. 96, 2006.
- [5] N. Brunner and P. Skrzypczyk, “Nonlocality distillation and postquantum theories with trivial communication complexity,” *Phys. Rev. Lett.*, Vol. 102, 2009.
- [6] A. Cabello, “Specker’s fundamental principle of quantum mechanics,” quant-ph/1212.1756, 2012.
- [7] B. S. Cirel’son, “Quantum generalizations of Bell’s inequality,” *Lett. Math. Phys.*, Vol. 4, No. 93, 1980.
- [8] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” *Phys. Rev. Lett.*, Vol. 23, No. 15, pp. 880–884, 1969.
- [9] I. Devetak, A.W. Harrow, and A. Winter, “A family of quantum protocols,” quant-ph/0308044, 2003.
- [10] I. Devetak, A.W. Harrow, and A. Winter, “A resource framework for quantum Shannon theory,” quant-ph/0512015, 2005.
- [11] D. Dukaric and S. Wolf, “A limit on non-locality distillation,” quant-ph/0808.3317, 2008.
- [12] H. Ebbe and S. Wolf, “Distillation of multi-party non-locality with and without partial communication,” *Proc. IEEE Int. Symp. Inf. Theory*, Istanbul, 2013.
- [13] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?,” *Phys. Rev.*, Vol. 41, 1935.
- [14] M. Forster, S. Winkler, and S. Wolf, “Distilling nonlocality,” *Phys. Rev. Lett.*, Vol. 102, 2009.
- [15] M. Forster, “Distillation and units of nonlocality,” Diss. ETH No. 20152, 2012.
- [16] T. Fritz, A.B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acin, “Local orthogonality: a multipartite principle for correlations,” quant-ph/1210.3018, 2012.
- [17] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acin, “Full randomness from arbitrarily deterministic events,” quant-ph/1210.6514, 2012.
- [18] V. Galliard, “Randomness from non-local correlations,” Diss. ETH No. 20654, 2012.
- [19] N. Gisin, S. Popescu, V. Scarani, S. Wolf, and J. Wullschleger, “Oblivious transfer and quantum channels as communication resources,” *Nat. Comp.*, Vol. , No. 12, 2013.
- [20] P. Høyer and J. Rashid, “Optimal protocols for nonlocality distillation,” *Phys. Rev. A*, Vol. 82, No. 4, 2010.
- [21] Li-Yi Hsu and Keng-Shuo Wu, “Multipartite nonlocality distillation,” *Phys. Rev. A*, Vol. 82, 2010.
- [22] N. Linden, S. Popescu, A. J. Short, and A. Winter, “No quantum advantage for nonlocal computation,” quant-ph/0610097, 2006.
- [23] L. Masanes, A. Acin, and N. Gisin, “General properties of nonsignaling theories,” *Phys. Rev. A*, Vol. 73, 2006.
- [24] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, “Information causality as a physical principle,” *Nature* 461, 1101, 2009.
- [25] S. Pironio, J.-D. Bancal, and V. Scarani, “Extremal correlations of the tripartite no-signaling polytope,” *J. Phys. A: Math Theor.*, Vol. 44, 2011.
- [26] S. Popescu and D. Rohrlich, “Nonlocality as an axiom,” *Foundations of Physics*, Vol. 24, pp. 379, 1994.
- [27] A. J. Short, S. Popescu, and N. Gisin, “Entanglement swapping for generalized nonlocal correlations,” *Phys. Rev. A*, Vol. 59, 2006.