ISIT'2013 1569717473

Distillation of Multi-Party Non-Locality With and Without Partial Communication

Helen Ebbe
Department of Mathematics
ETH Zentrum
8092 Zurich, Switzerland
Email: heebbe@ethz.ch

Stefan Wolf
Faculty of Informatics
University of Lugano (USI)
6900 Lugano, Switzerland
Email: wolfs@usi.ch

***Abstract*—Non-local correlations are one of the most fascinating consequences of quantum physics 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 — better in terms of classical information. In these contexts, the question is crucial whether such correlations can be *distilled*, i.e., whether 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 show that a natural generalization of the well-known Popsecu-Rohrlich box can be distilled, by an adaptive protocol, to the algebraic maximum. We use this result further to show that a much bigger class of correlations, including *all* purely three-partite correlations, can be distilled from arbitrarily weak to maximal strength with partial communication, i.e., using only a subset of the channels required for the creation of the same correlation from scratch. In other words, we show that arbitrarily weak non-local correlations can have a "communication value" in the context of the generation of maximal non-locality.

I. Introduction

One of the most mysterious, challenging, but also useful consequences of quantum theory is the possibility of non-local correlations: The joint behavior under (different possible) measurements of a quantum system is such that it cannot be explained by pre-shared (classical) information determining all the outcomes locally. This result by Bell [1] can be seen as a late reply to the claim, in 1935, of Einstein, Podoslky, and Rosen [2] 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, i.e., the behavior of a perfect PR box [8] cannot be realized [9]. A number of attempts have been made to single out quantum correlations as compared to general non-signaling systems: Are quantum correlations the ones that do not collapse *communication complexity* [10], that are of no help for *non-local computation* [12], or that respect *information causality*, a principle generalizing the non-signaling principle to the case of limited communication [11]? Furthermore, it has turned out that non-local correlations have important applications for information processing, e.g., device-independent cryptography or communication complexity. In all the mentioned contexts, a question of paramount importance is the one of *distillation of non-locality*: Given weak correlations, is it possible to generate stronger by some 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 complex picture: Whereas *isotropic CHSH-type* [13] correlations seem undistillable [14], the same fails to be true in general [4], [5], [15]. In fact, certain arbitrarily weak CHSH correlations can even be distilled up to arbitrarily close to 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 [4] to more parties fails to distill extremal boxes of the non-signalling polytope to almost-perfect [3].

The contribution of the present work is two-fold: First, we show that the natural generalization of PR boxes to n parties has the property that non-isotropic faulty versions of it can be distilled to close-to-perfect by a multi-party variant of the BS protocol (Section III). Second, 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, where this communication *alone* is insufficient for generating the target correlation (Section IV). This 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 V, the general results and procedures are illustrated with a representative example.

II. Definitions

Here we define certain classes and specific types of n-partite boxes which we will use in our distillation protocols. They are

[1] Bell's result only persists under the assumption that measurement bases are chosen freely; but at the same time, none of the deterministic interpretations of quantum physics satisfies with an explanation of the correlations' origin.

generalizations of important bipartite boxes in [4], [5], [6].

The most general type that we define is a *full-correlation box*. Intuitively speaking it has a correlation only w.r.t. the *full* set of players. A *full-correlation box* is an n-partite box which takes n inputs and produces n outputs. We denote the n-tuple of inputs as $\vec{x} = (x_1, x_2, ..., x_n)$, where $x_i \in \{0, 1\}$. The n-tuple of outputs is $\vec{a} = (a_1, a_2, ..., a_n)$, where $a_i \in \{0, 1\}$ for all i. The *full-correlation box* is characterized by the following conditional distribution:

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

where $f(\vec{x})$ is a Boolean function of the inputs. Two special cases of this type of box are the *n-partite Popescu-Rohrlich box* and the *even parity box for n parties*. An *n-partite Popescu-Rohrlich box* (or short *n-PR box*) takes n inputs $\vec{x} = (x_1, x_2, ..., x_n)$ and produces n outputs $\vec{a} = (a_1, a_2, ..., a_n)$ according to the conditional distribution

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

An *even-parity box for n parties* takes n inputs $\vec{x} = (x_1, x_2, ..., x_n)$ and produces n outputs $\vec{a} = (a_1, a_2, ..., a_n)$ according to the conditional distribution

$$P_n^{c}(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_i a_i = 0 \\ 0 & \text{otherwise.} \end{cases} \quad (3)$$

Note that this latter box is *local*. A convex combination of the last two boxes is called a *correlated non-local box for n parties*. The *family of correlated non-local boxes for n parties* is defined as follows:

$$P_{n,\varepsilon}^{PR} = \varepsilon P_n^{PR} + (1 - \varepsilon) P_n^{c} \quad (4)$$

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

III. Generalization of the Brunner-Skrzypczyk Protocol

Brunner and Skrzypczyk presented in [5] a protocol for two parties that distills non-locality and in the asymtotic limit: All correlated non-local boxes are distilled to the maximally non-local PR box. This result can be generalized to all n-partite PR boxes Protocol 1.

Protocol 1 (Generalized BS Protocol for n-PR Boxes) *The protocol works as follows (see also Fig. 1). All n parties share two boxes, where we denote by x_i the value that the ith party inputs to the first box and by y_i the value that the ith party inputs to the second box. The output bit of the first box for the ith party is then 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, $c_i = a_i \oplus b_i$.*

With this protocol we are also able to distill a large class of boxes arbitrarily closely to the n-PR box.

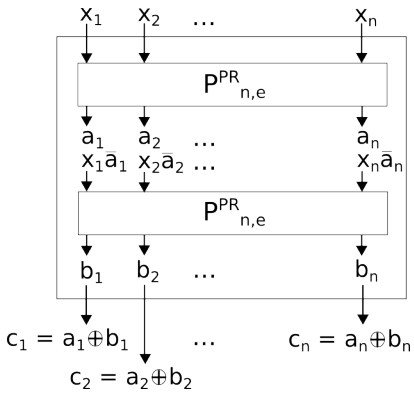

Figure 1. Generalized BS protocol for n-PR boxes

Theorem 1 *The generalized BS protocol takes two copies of an arbitrary box $P_{n,\varepsilon}^{PR}$ with $0 < \varepsilon < 1$ to an n-partite correlated non-local box $P_{n,\varepsilon'}^{PR}$ with $\varepsilon' > \varepsilon$, i.e., is distilling non-locality. In the asymptotic case of many copies, any $P_{n,\varepsilon}^{PR}$ with $0 < \varepsilon$ is distilled arbitrarily closely to the n-PR box.*

Since the Protocol 1 and Theorem 1 are generalizations of [5], the proof works almost in the same manner.

Proof: We start with the initial two-box state of the protocol which is given by

$$\begin{aligned} P_{n,\varepsilon}^{PR} P_{n,\varepsilon}^{PR} &= \varepsilon^2 P_n^{PR} P_n^{PR} + \varepsilon(1-\varepsilon)\left(P_n^{PR} P_n^{c} + P_n^{c} P_n^{PR}\right) \\ &\quad + (1-\varepsilon)^2 P_n^{c} P_n^{c} \,. \end{aligned} \quad (5)$$

We apply the above distillation protocol and get the final box. As in [5], we use the notation $P_i P_i' \longrightarrow P_f$, which means that the protocol takes two initial boxes, P_i and P_i', to one copy of the final box P_f.

So we get the following relations: $P_n^{PR} P_n^{PR} \longrightarrow P_n^{PR}$, $P_n^{PR} P_n^{c} \longrightarrow P_n^{PR}$, $P_n^{c} P_n^{PR} \longrightarrow 2^{1-n} P_n^{PR} + \left(1 - 2^{1-n}\right) P_n^{c}$, and $P_n^{c} P_n^{c} \longrightarrow P_n^{c}$.

After the application of the distillation protocol we get the final box, which is given by

$$\begin{aligned} P_{n,\varepsilon'}^{PR} &= \frac{\varepsilon}{2^{n-1}}\left(2^{n-1} + 1 - \varepsilon\right) P_n^{PR} \\ &\quad + \left(1 - \frac{\varepsilon}{2^{n-1}}\left(2^{n-1} + 1 - \varepsilon\right)\right) P_n^{c} \,. \end{aligned} \quad (6)$$

Hence, $\varepsilon' = \frac{\varepsilon}{2^{n-1}}\left(2^{n-1} + 1 - \varepsilon\right)$. We are now able to determine what kind of boxes can be distilled by this protocol. If the protocol distills the box $P_{n,\varepsilon}^{PR}$ to $P_{n,\varepsilon'}^{PR}$ then ε has to fulfill $\varepsilon' > \varepsilon$. We observe that all $0 < \varepsilon < 1$ fulfill this condition and, therefore, the protocol distills any box of the family of correlated non-local boxes.

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

$$T_n(\varepsilon) = \frac{\varepsilon}{2^{n-1}}\left(2^{n-1} + 1 - \varepsilon\right). \quad (7)$$

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 $\frac{dT}{d\varepsilon}|_{\varepsilon=0} = 1 + \frac{1}{2^{n-1}} > 1$, so this box is repulsive. For the other box P_n^{PR} we find $\frac{dT}{d\varepsilon}|_{\varepsilon=1} = 1 + \frac{1}{2^{n-1}} - \frac{1}{2^{n-2}} < 1$, so this box is attractive. ■

IV. Application: Distillation with Partial Communication

The generalized BS protocol can be used for distillation protocols for full-correlation boxes, where the use of communication is allowed to some of the parties. That means we are looking for distillation protocols based on the generalized BS protocol, but that are also allowing one-way communication channels between some of the parties, that can be used as often as required. We show that we are able to distill a general class of full-correlation boxes arbitrarily closely to the maximum with such a protocol.

Lemma 1 *If f is a Boolean function of the input elements $x_1, x_2, ..., x_n$, then it can be written as*

$$f(x_1, ..., x_n) = \bigoplus_{I \in \mathcal{I}} \left(a_I \cdot \bigwedge_{i \in I} x_i \right), \tag{8}$$

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

Proof: The constant, the AND, and the XOR allow for implementing the universal Boolean functions AND and NOT. ■

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 ith 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.

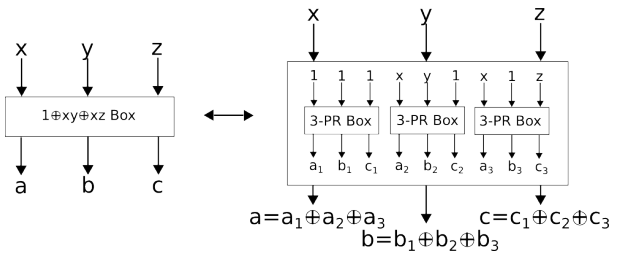

Figure 2. Construction of $1 \oplus xy \oplus xz$ box

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

$$\mathcal{J} := \{I \in \mathcal{I} \,|\, a_I = 1 \text{ and } |I| \geq 2\}. \tag{9}$$

This set can be partitioned into disjoint subsets $\{J_1, J_2, ..., J_{n_\mathcal{J}}\}$ 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 $n_\mathcal{J}$. Later, we will see that it is important to know how many of the variables in a non-local box appear only in this non-local box, for that we define $m_I = |I \setminus \bigcup_{J \in \mathcal{J} \setminus I} J|$ for all $I \in \mathcal{J}$.

Theorem 2 shows how many one-way communication channels are needed to simulate an n-partite full-correlation box.

Theorem 2 (Number of one-way communication channels) *Let f be the Boolean function associated to an n-partite full-correlation box, and let f be defined as in Lemma 1. If $n_\mathcal{J} = 1$, then the number $N_{comm}^{scratch}$ of one-way communication channels to simulate the full-correlation box from scratch is*

$$N_{comm}^{scratch} = \left| \bigcup_{I \in \mathcal{J}} I \right| - 1. \tag{10}$$

Proof: We prove the statement 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 [7], 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 we have a function with $|\mathcal{J}| = n+1$ that still fulfills the assumption of the theorem. 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 still 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 in the case $|\mathcal{J}| = 2$. Together, we need n one-way communication channels to simulate a function with $|\mathcal{J}| = n + 1$. ■

We construct an n-partite box where the outputs depend on the outputs of two full-correlation boxes for less than n parties. These two boxes are defined by

$$P_1(a_1...a_{k_2}|x_1...x_{k_2}) = \begin{cases} \frac{1}{2^{k_2-1}} & \bigoplus_{i=1}^{k_2} a_i = g_1(x_1, ..., x_{k_2}) \\ 0 & \text{otherwise,} \end{cases} \tag{11}$$

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

$$P_2(b_{k_1}...b_n|x_{k_1}...x_n) = \begin{cases} \frac{1}{2^{n-k_1}} & \bigoplus_{i=k_1}^{n} b_i = \prod_{i=k_1}^{k_3} x_i \\ 0 & \text{otherwise,} \end{cases} \tag{12}$$

where $0 < k_1 < k_2 < k_3 \leq n$. These two boxes can be calculated in parallel. Finally the constructed box outputs to party i

$$c_i = \begin{cases} a_i & i \in \{1, 2, ..., k_1 - 1\} \\ a_i \oplus b_i & i \in \{k_1, k_1 + 1, ..., k_2\} \\ b_i & i \in \{k_2 + 1, k_2 + 2, ..., n\}. \end{cases} \tag{13}$$

Lemma 2 *The constructed box is equivalent (i.e. the joint probabilities are equal) to the full-correlation box defined by*

$$P(\vec{c}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_{i=1}^{n} c_i = g_1(x_1, ..., x_{k_2}) \oplus \prod_{i=k_1}^{k_3} x_i \\ 0 & \textit{otherwise.} \end{cases} \quad (14)$$

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 [6], and the property that the XOR conserves randomness in case of independence. ∎

Theorem 3 and Corollary 1 state that a general class of full-correlation boxes can be simulated by distillation 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.

Theorem 3 (Distillation with Communication) *Let f be a Boolean function associated to an n-partite full correlation box, and let f be written as in Lemma 1. If f fulfills $n_{\mathcal{J}} = 1$, then:*

(i) *The full-correlation box can be constructed from generalized PR-boxes shared between a different number of parties such that in at most one generalized PR box some parties input all the time a constant.*

(ii) *The number $N_{comm}^{distill}$ of necessary one-way communication channels for simulating the full-correlation box with using the generalized BS protocol is*

$$N_{comm}^{distill} \leq \begin{cases} n - 1 - \max_{I \in \mathcal{J}}(m_I) & \max_{I \in \mathcal{J}}(m_I) \neq n \\ 0 & \max_{I \in \mathcal{J}}(m_I) = n. \end{cases} \quad (15)$$

Proof: In this 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. 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 changed box and the local box.

We start to prove part (i) of the theorem. The idea is to 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 of the theorem). Because of Lemma 2, 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 $\{1, 2, ..., n\} \setminus (I \cup J)$, we input 1.

Assume that we have, in this way, replaced some n-PR boxes by new boxes. Again, we are looking for an 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 to a new box with the claimed properties.

We prove part (ii) of the theorem. For this part, we assume that the replacement is made according to part (i). We have replaced the original n-PR boxes such that the general PR box with constant element does not correspond to the original n-PR box belonging to the biggest m_I. This is possible, since we can replace this box first. We are now able to isolate the box belonging to the biggest 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 which acts also in the isolated box. We have isolated the general PR box, and we are able to apply the generalized BS protocol to this box. All the other generalized PR boxes that appear in the abstraction of part (i) in the theorem 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 when we start from scratch. ∎

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

$$N_{comm}^{distill} < N_{comm}^{scratch} \ . \quad (16)$$

Proof: The statement follows directly from Theorems 2 and 3. ∎

All extremal three-partite full-correlation boxes of the non-signalling polytope fulfill the preconditions of Corollary 1. For more parties, it is unknown how many extremal boxes also fulfill this precondition.

V. EXAMPLE

In this example we want to distill some boxes up to the following full-correlation box:

$$P(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_{i=1}^{5} a_i = x_1x_2x_3 \oplus x_1x_4 \oplus x_4x_5 \oplus x_3 \\ 0 & \text{otherwise.} \end{cases} \quad (17)$$

Therefore, we determine first the above-defined sets and constants. Let $\mathcal{I} = \mathcal{P}(\{1, 2, 3\})$. From Lemma 1, we know that all $a_I = 1$ for $I \in \{\{1, 2, 3\}, \{1, 4\}, \{4, 5\}, \{3\}\}$, and otherwise $a_I = 0$. This means that the given full-correlation box can be simulated by four 5-PR boxes with some constant inputs, where one of these boxes is local (see Fig. 3 a)). 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:

$$\mathcal{J} = \{\{1, 2, 3\}, \{1, 4\}, \{4, 5\}\} \quad (18)$$

Each of these three non-local 5-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

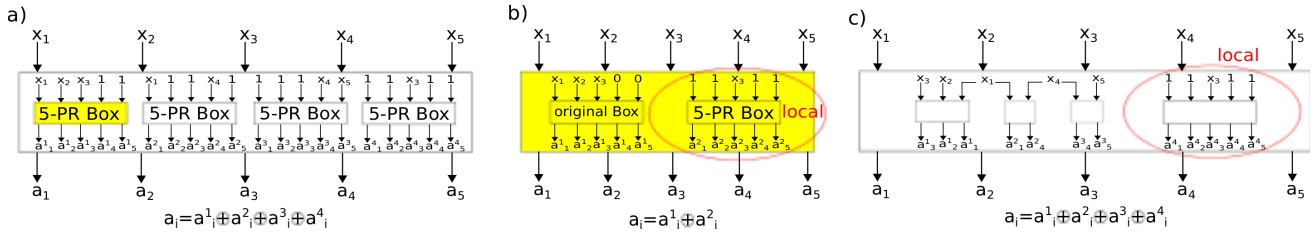

Figure 3. a) Simulating the full-correlation box with four 5-PR boxes. b) How to simulate the first 5-PR box with the original full-correlation box and a local box. c) Simulation of the full-correlation box with n-PR boxes without a constant input and a local box.

in both boxes (see Fig. 3 b)). If we apply Theorem 3 (i), then we know that the non-local part of the original full-correlation box can be simulated by three connected n-PR boxes with no constant input.

Since we know $\mathcal{J}$, the number of required one-way communication channels for simulating the full-correlation box can be calculated with Theorem 2:

$$N_{comm}^{distill} = \left| \bigcup_{I \in \mathcal{J}} I \right| - 1 = 4. \tag{19}$$

Obviously, this box is not local. To determine the distance (measured in the L^1-norm), we can use a linear program and get that the distance is 20, and the closest local box (not unique) is given by

$$P^L(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_{i=1}^{5} a_i = x_3 \\ 0 & \text{otherwise.} \end{cases} \tag{20}$$

We start with the second part of the example, where we show in detail how we distill a box from the family $P_\varepsilon = \varepsilon P + (1-\varepsilon)P^L$, where $0 < \varepsilon < 1$, up to $P(\vec{a}|\vec{x})$.

We want to distill this box arbitrarily closely to the full-correlation box above. 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 5-PR boxes: $m_{\{1,2,3\}} = 2$, $m_{\{1,4\}} = 1$, and $m_{\{4,5\}} = 1$. This means that we isolate the box that belongs to the 5-PR box with three arbitrary inputs. This can be done in the same way as before: We input $(x_1, x_2, x_3, 0, 0)$ in P_ε and the local box and take then the XOR of its outputs. Then, we use one-way communication channels from Party 5 to 4 and one from 4 to 1. Remember that the communication channels can be used as often as the parties want. Hence, we are able to simulate perfectly the two 2-PR box, and the non-perfect 3-PR box can be isolated by communicating the inputs and outputs of the two 2-PR box to Party 1 (see Fig. 3 c)). We have isolated the box $P_{3,\varepsilon}^{PR}$ that is known to be distillable up to P_3^{PR} by the generalized BS protocol. In this way, we are able to distill the box P_ε up to the full-correlation box in the beginning.

We get that the number of one-way communication channels that is needed for this kind of distillation is $N_{comm}^{distill} = 2$, i.e., less than $N_{comm}^{scratch} = 4$.

VI. Conclusion

We have considered 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 distilled to using *partial* communication (less than if no 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 better. It seems that for certain tasks (such as randomness amplification), multi-party non-locality outperforms bipartite correlations.

References

[1] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics*, Vol. 1, pp. 195–200, 1964.

[2] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Phys. Rev.*, Vol. 41, 1935.

[3] Li-Yi Hsu and Keng-Shuo Wu, "Multipartite nonlocality distillation," *Phys. Rev. A*, Vol. 82, 2010.

[4] M. Forster, S. Winkler, and S. Wolf, "Distilling nonlocality," *Phys. Rev. Lett.*, Vol. 102, 2009.

[5] N. Brunner and P. Skrzypczyk, "Nonlocality distillation and postquantum theories with trivial communication complexity," *Phys. Rev. Lett.*, Vol. 102, 2009.

[6] J. Barrett and S. Pironio, "Popescu-Rohrlich correlations as a unit of nonlocality," *Phys. Rev. Lett.*, Vol. 95, 2005.

[7] S. Pironio, J.-D. Bancal, and V. Scarani, "Extremal correlations of the tripartite no-signaling polytope," *J. Phys. A: Math Theor.*, Vol. 44, 2011.

[8] S. Popescu and D. Rohrlich, "Nonlocality as an axiom," *Foundations of Physics*, Vol. 24, pp. 379, 1994.

[9] B. S. Cirel'son, "Quantum generalizations of Bell's inequality," *Lett. Math. Phys.*, Vol 4, No. 93, 1980.

[10] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, "A limit on non-local correlations in any world where communication complexity is not trivial," *Phys. Rev. Lett.*, Vol. 96, 2006.

[11] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, "Information causality as a physical principle," *Nature* 461, 1101, 2009.

[12] N. Linden, S. Popescu, A. Short, and A. Winter, "No quantum advantage for nonlocal computation," quant-ph/0610097, 2006.

[13] 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.

[14] D. Dukaric and S. Wolf, "A limit on non-locality distillation," quant-ph/0808.3317, 2008.

[15] P. Hoyer and J. Rashid, "Optimal protocols for nonlocality distillation," *Phys. Rev. A*, Vol. 82, No. 4, 2010.