Nonlocal distillation based on multisetting Bell inequality

Xiang-Jun Ye, Dong-Ling Deng, and Jing-Ling Chen

Phys. Rev. A **86**, 062103 — Published 10 December 2012
DOI: 10.1103/PhysRevA.86.062103

Nonlocal distillation based on multi-setting Bell inequality

Xiang-Jun Ye,[1,2] Dong-Ling Deng,[3] and Jing-Ling Chen[1,2,*]

[1] *Theoretical Physics Division, Chern Institute of Mathematics, Nankai University, Tianjin 300071, People's Republic of China*
[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[3] *Department of Physics and MCTP, University of Michigan, Ann Arbor, Michigan 48109, USA*

(Dated: November 26, 2012)

Inspired by the recent works of Foster *et al.* [Phys. Rev. Lett. **102**, 120401 (2009)] and Brunner *et al.* [Phys. Rev. Lett. **102**, 160403 (2009)], we present a nonlocality distillation protocol for two three-level (qutrit) systems in the framework of generalized nonsignaling theories. Our protocol is based on a three-setting Bell inequality. It works efficiently for a specific class of 3-input-3-output nonlocal boxes. In the asymptotic limit, all these nonlocal boxes can be distilled to the maximally nonlocal box defined by the inequality and nonsignaling constraints. Then we introduce a new contracting protocol that reduces these boxes to the so called "correlated nonlocal boxes". As a result, our 3-input-3-output nonlocal boxes also make communication complexity trivial and appear very unlikely to exist in nature.

PACS numbers: 03.65.Ud, 03.67.-a

I. INTRODUCTION

When different measurements are performed on two separated parts of an entangled quantum state, the corresponding outcomes can show correlations that violate a Bell inequality and therefore are unexplainable by any local hidden variable theory [1]. This kind of stronger correlations is now well known as *nonlocality*.

Quantum nonlocality is a fascinating counterintuitive phenomenon related to the foundation of quantum mechanics and has attracted much interest recently both in theoretical and experimental works [2]. It has been identified as another resource, alternative to entanglement and indispensable for device-independent quantum information processing protocols [3, 4]. For instance, in a device-independent quantum key distribution protocol, quantum nonlocality is used to generated shared secret keys between different parties in a device-independent way, i.e., in a way that the internal workings of the quantum devices are unknown or not trusted [4]. In Ref. [5], it is shown that nonlocality is also a necessary resource for nonlocal computation. Furthermore, nonlocality that to some extent is superquantum might make communication complexity trivial [6].

Although entanglement and nonlocality are closely related, they are two quite different things. There do exist quantum states with large entanglement but have no nonlocality, in the sense that these quantum states admit local hidden variable models and cannot violate any Bell inequality [7, 8]. Many protocols for quantum entanglement distillation have been proposed [9] and experimentally tested [10]. Similarly, one may ask another interesting question: can nonlocality be distilled? In other words, can we get stronger nonlocality from a number of weak nonlocal resources? Forster *et al*. [11] made a breakthrough and provided a positive answer to this question. In their paper, they presented the first nonlocality distillation protocol in the framework of nonsignaling theory [12]. Then, Brunner and Skrzypczyk presented another protocol for deterministically distilling nonlocality, which is optimal for two-copy distillation and works efficiently for a specific class of postquantum nonlocal boxes–the so called correlated nonlocal boxes [13]. In the asymptotic limit, their protocols would distill all correlated nonlocal boxes to the maximally nonlocal box of Popescu and Rohrlich [14], thus making communication complexity trivial [6].

In this work, we will focus on 3-input-3-output bipartite systems. We present a nonlocality distillation protocol for such systems in the framework of generalized nonsignaling theories. Our protocol is based on a three-setting Bell inequality for bipartite three-level (qutrit) systems [16] and works efficiently for a specific class of 3-input-3-output nonlocal boxes. In the asymptotic limit, all these nonlocal boxes are distilled to the maximally nonlocal box defined by the inequality. To show that these boxes are postquantum and unlikely to exist in nature, we introduce a new contracting protocol to reduce them to the class of correlated nonlocal boxes.

*Electronic address: chenjl@nankai.edu.cn

II. THE FRAMEWORK AND DISTILLATION PROTOCOL

To begin with, let us consider the following Bell-type scenario in terms of nonlocal boxes. Two distant parties, Alice and Bob, share a nonlocal box. Each party is allowed to input one trit into the box and gets one output trit: Alice inputs $x \in \{0,1,2\}$ and gets outcome $a \in \{0,1,2\}$; Bob inputs $y \in \{0,1,2\}$ and gets outcome $b \in \{0,1,2\}$. This device is atemporal: Alice gets her output as soon as she feeds in her input, regardless of if and when Bob feeds in his input, and vice versa. Every nonlocal box is then characterized by a set of 81 joint probabilities $P(ab|xy)$. A two-partite system, which is characterized by a conditional probability distribution $P(ab|xy)$, is said to be nonsignaling if one cannot signal from one side to the other by the choice of the input. This means that the marginal probabilities $P(a|x)$ and $P(b|y)$ are independent of y and x, respectively, i.e.,

$$\begin{cases} \sum_a P(ab|xy) = \sum_a P(ab|x'y) = P(b|y)\ \forall x, x', b, y, \\ \sum_b P(ab|xy) = \sum_b P(ab|xy') = P(a|x)\ \forall a, x, y, y'. \end{cases} \tag{1}$$

In the following, we will work on these nonsignaling boxes characterized by their probability distributions, which is stated in the matrix form.

To present our main results, another problem we should also deal with is: How to quantify non-locality in two-qutrit system? In the two-qubit case, Forster *et al.* [11] and Brunner *et al.* [13] use the CHSH inequality [15] violation as the measurement of two-qubit nonlocality. Similarly, here we use the violation of a three-setting Bell inequality introduced in Ref. [16] as the measure of nonlocality in three-qutrit system. To this end, let us briefly review the three-setting inequality. For the convenience of later utility, we rewrite the inequality in the following form:

$$\begin{aligned} I_3^{[3]} &= -2[P(00|xy) + P(12|xy) + P(21|xy)] + P(01|xy) + P(10|xy) + P(22|xy) + P(02|xy) + P(20|xy) + P(11|xy) \\ &+ P(00|xy\oplus 1) + P(12|xy\oplus 1) + P(21|xy\oplus 1) - P(02|xy\oplus 1) - P(20|xy\oplus 1) - P(11|xy\oplus 1) + P(00|x\oplus 1y) \\ &+ P(12|x\oplus 1y) + P(21|x\oplus 1y) - P(02|x\oplus 1y) - P(20|x\oplus 1y) - P(11|x\oplus 1y) + P(01|xy\oplus 2) + P(10|xy\oplus 2) \\ &+ P(22|xy\oplus 2) - P(02|xy\oplus 2) - P(20|xy\oplus 2) - P(11|xy\oplus 2) + P(01|x\oplus 2y) + P(10|x\oplus 2y) + P(22|x\oplus 2y) \\ &- P(02|x\oplus 2y) - P(20|x\oplus 2y) - P(11|x\oplus 2y) + P(01|x\oplus 1y\oplus 2) + P(10|x\oplus 1y\oplus 2) + P(22|x\oplus 1y\oplus 2) \\ &- P(02|x\oplus 1y\oplus 2) - P(20|x\oplus 1y\oplus 2) - P(11|x\oplus 1y\oplus 2) + P(01|x\oplus 2y\oplus 1) + P(10|x\oplus 2y\oplus 1) \\ &+ P(22|x\oplus 2y\oplus 1) - P(02|x\oplus 2y\oplus 1) - P(20|x\oplus 2y\oplus 1) - P(11|x\oplus 2y\oplus 1) + P(00|x\oplus 2y\oplus 2) \\ &+ P(12|x\oplus 2y\oplus 2) + P(21|x\oplus 2y\oplus 2) - P(01|x\oplus 2y\oplus 2) - P(10|x\oplus 2y\oplus 2) - P(22|x\oplus 2y\oplus 2) \le 4. \end{aligned} \tag{2}$$

Here, the pair (x, y) equals to any of the following nine pairs: (i, j) $(i, j = 0, 1, 2)$; The notation $\oplus$ means addition modulo 3. It is showed in Ref. [16] that the inequality (2) is tight and relevant to the well-known Collins-Gisin-Linden-Massar-Popescu (CGLMP) inequality [17]. This inequality has four distinguish "*roots*" [18] and its maximal quantum violation, which occurs at a nonmaximally entangled state, is 5.1803. Based on this multisetting inequality, our definition of the nonlocality of two-qutrit systems is as follows:

$$\mathcal{NL}[P] := \max_{xy}\ I_3^{[3]}. \tag{3}$$

Note that $\mathcal{NL}[P] > 4$ indicates that the correlation P violates the inequality (2) and is therefore called nonlocal.

Now, let us introduce a class of one parameter nonlocal boxes $\mathbb{P}^\epsilon$ $(0 < \epsilon < 1)$.

Definition 1. We define the classical box $\mathbb{P}^C$ as

$$\mathbb{P}^C := \begin{cases} \frac{1}{3} & \text{if } a + b \doteq 1 \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

where $\doteq$ means equality modulo 3 .

Definition 2. We define the maximal nonlocal box $\mathbb{P}^{MAX}$ as

$$\mathbb{P}^{MAX} := \begin{cases} \frac{1}{3} & \text{if } a + b \doteq (x + y + 2)^2 \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

Definition 3. The appropriate nonlocal box $\mathbb{P}^\epsilon$ which we will use for distilling is defined as follows

$$\mathbb{P}^\epsilon := \epsilon\mathbb{P}^{MAX} + (1-\epsilon)\mathbb{P}^C \qquad (0 < \epsilon < 1). \tag{6}$$

By directly calculations, it is easy to see that $\mathbb{P}^C$, $\mathbb{P}^{MAX}$, and $\mathbb{P}^\epsilon$ are non-signaling with respect to the definition (1). The matrix form of $\mathbb{P}^\epsilon$ is:

$$\mathbb{P}^\epsilon = \left(\begin{array}{c||ccccccccc} {}_{xy}{}^{ab} & 00 & 01 & 02 & 10 & 11 & 12 & 20 & 21 & 22 \\ \hline\hline 00 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} \\ 01 & \frac{\epsilon}{3} & \frac{1-\epsilon}{3} & 0 & \frac{1-\epsilon}{3} & 0 & \frac{\epsilon}{3} & 0 & \frac{\epsilon}{3} & \frac{1-\epsilon}{3} \\ 02 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} \\ 10 & \frac{\epsilon}{3} & \frac{1-\epsilon}{3} & 0 & \frac{1-\epsilon}{3} & 0 & \frac{\epsilon}{3} & 0 & \frac{\epsilon}{3} & \frac{1-\epsilon}{3} \\ 11 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} \\ 12 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} \\ 20 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} \\ 21 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} \\ 22 & \frac{\epsilon}{3} & \frac{1-\epsilon}{3} & 0 & \frac{1-\epsilon}{3} & 0 & \frac{\epsilon}{3} & 0 & \frac{\epsilon}{3} & \frac{1-\epsilon}{3} \end{array}\right).$$

According to the definition (3) , the nonlocality of $\mathbb{P}^\epsilon$ is $\mathcal{NL}[\mathbb{P}^\epsilon] = 4 + 4\epsilon$. When $\epsilon = 1$ box $\mathbb{P}^\epsilon$ turns to $\mathbb{P}^{MAX}$ with nonlocality $\mathcal{NL}[\mathbb{P}^{MAX}] = 8$, which is the maximal nonlocality value of a 3-input 3-output bi-partite box according to the Ineq. (2) [19]. In addition, when $\epsilon = 0$ box $\mathbb{P}^\epsilon$ turns to $\mathbb{P}^C$, which is classical and achievable by shared randomness.

Distillation protocol.—Now we present a distillation protocol for the nonlocal boxes $\mathbb{P}^\epsilon$. Our protocol takes four copies of any box $\mathbb{P}^\epsilon$ with $0 < \epsilon < 1$ to a new nonlocal box $\mathbb{P}^{\epsilon'}$ with $\epsilon' > \epsilon$, thus distilling nonlocality. In the asymptotic limit, any ϵ with $0 < \epsilon < 1$ is distilled arbitrarily close to 1 by iteration. The protocol is illustrated in Fig.1.

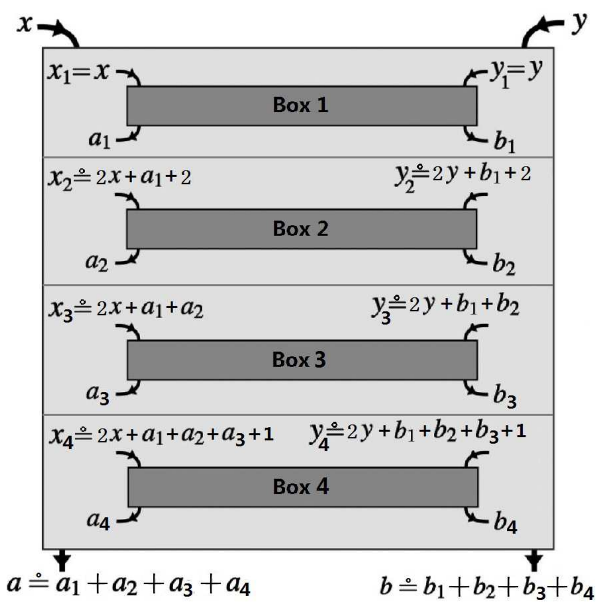


FIG. 1: Protocol for four-copy deterministic nonlocality distillation. Alice and Bob use four $\mathbb{P}^\epsilon$ boxes sequentially. They input the value x_i and y_i into the ith box and get the corresponding outputs a_i and b_i, respectively. At last, they calculate $a \doteq a_1 + a_2 + a_3 + a_4$ and $b \doteq b_1 + b_2 + b_3 + b_4$ as the final outputs of the new box.

Alice and Bob share four copies of boxes $\mathbb{P}^\epsilon$, those boxes are arranged sequentially. Let us denote x_i and y_i the value Alice and Bob input into box i, respectively. The output of the kth box is denoted by a_k and b_k. The input and output of Alice and Bob at each step are denoted as follows:

This table explicitly shows that at the side of Alice there are only symbols x and a (ignoring the subscript), so she needn't any information from Bob when she proceeds the protocol, similar is the case of Bob. This protocol is feasible, for the input of Alice (Bob) at ith step only depends on the initial input x (y) and the output at jth step with $j < i$. Notably, though the boxes are arranged sequentially and Alice and Bob have to input values step by step because the later input are depending on the former output, the two parties are independent of each other, which means Alice may have accomplished all of her operations and got the final output a while Bob did nothing—–boxes are atemporal.

By straightforward calculations, one obtain that the final box, after the above distillation protocol has been applied, is $\mathbb{P}^{\epsilon'}$ with

$$\epsilon' = \epsilon \cdot (2 - \epsilon) \cdot (\epsilon^2 - 2\epsilon + 2) \;\; (0 < \epsilon < 1) \; . \tag{7}$$

	Alice	Bob
input of each step	$x_1 = x$	$y_1 = y$
	$x_2 \doteq 2x + a_1 + 2$	$y_2 \doteq 2y + b_1 + 2$
	$x_3 \doteq 2x + a_1 + a_2$	$y_3 \doteq 2y + b_1 + b_2$
	$x_4 \doteq 2x+a_1+a_2+a_3+1$	$y_4 \doteq 2y+b_1+b_2+b_3+1$
output of each step	$a_k \quad (k = 1, 2, 3, 4)$	$b_k \quad (k = 1, 2, 3, 4)$
final output of $\mathbb{P}^{\epsilon'}$	$a \doteq a_1 + a_2 + a_3 + a_4$	$b \doteq b_1 + b_2 + b_3 + b_4$

There are two fixed points in function (7), $\epsilon = 0$ and $\epsilon = 1$. The stability can be checked by finding the eigenvalues of the Jacobian at the fixed points. We get $\lambda \mid_{\epsilon=0}= \frac{d\epsilon'}{d\epsilon} \mid_{\epsilon=0}= 4 > 1$, $\lambda \mid_{\epsilon=1}= \frac{d\epsilon'}{d\epsilon} \mid_{\epsilon=1}= 0 < 1$, so $\epsilon = 1$ is an attractive fixed point and $\epsilon = 0$ is repulsive, which means, by iteration, we could distill all nonlocal box $\mathbb{P}^{\epsilon}$ arbitrary close to $\mathbb{P}^{MAX}$ despite that the initial box may very close to classical box $\mathbb{P}^{C}$. More intuitional express of relation between ϵ and ϵ' is show in Fig.2.

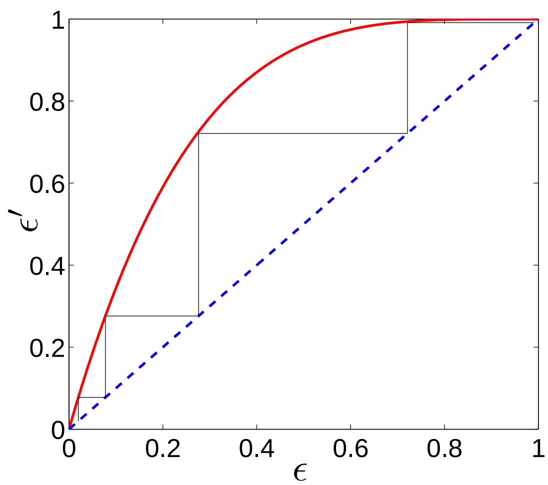


FIG. 2: (color online) The relation between ϵ and ϵ', which are the characteristic parameters of the initial and final boxes, respectively. The graph shows ϵ' as a function of ϵ, i.e., $\epsilon' = \epsilon \cdot (2 - \epsilon) \cdot (\epsilon^2 - 2\epsilon + 2)$ (the red solid line). The blue dashed straight line, $\epsilon' = \epsilon$, is given as a reference. The black thin line (steps) shows the distillation of an initial box under successive iterations of the protocol.

Proof.—Now we prove those results. First let us show how this protocol works in an intuitive way. We express the three-setting Bell inequality and the nonlocal box $\mathbb{P}^{\epsilon}$ in one graph (see Fig.3), in which color denote the parameter in front of the corresponding terms in the three-setting Bell inequality, while the numbers denote the box $\mathbb{P}^{\epsilon}$. To find a suitable nonlocal protocol is just to find a map with two properties:

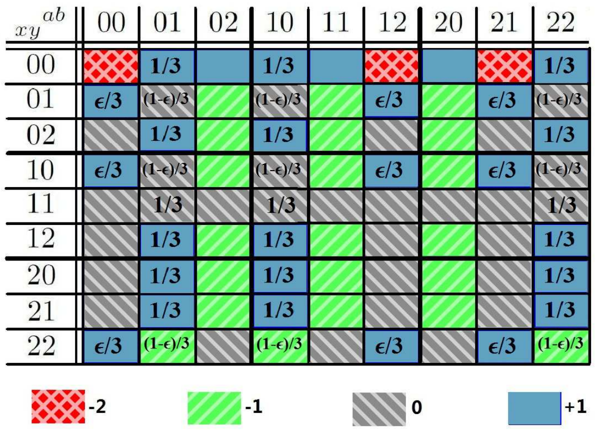
1. It is closure in $\mathbb{P}^{\epsilon}$, so we could iterate them without change the protocol.

2. The nonlocality of the final box is bigger than the nonlocality of the initially boxes.

Comparing Fig.3 we could find that two elements in $\mathbb{P}^{\epsilon}$ are the same if they have the same values of $x \oplus y$ and $a \oplus b$. For the sake of convenience, we will chose one element to express all elements with same value under operation of modulo 3. Then our purpose is to fix the rows with $x \oplus y = 0$ and $x \oplus y = 2$ unchanged and increase the values in blue blocks at rows with $x \oplus y = 1$. Now we show that the protocol achieve those requirements by straightforward calculations.

Calculate $P^{new}(ab|xy)$.—First we calculate the element $P^{new}(01|00)$ in new box $\mathbb{P}^{\epsilon'}$. According to the protocol, $P^{new}(01|00)$ equals to the summation of suitable conditional probability, which we have:

$$\begin{aligned} P^{new}(01|00) = \sum \ & P^1(a_1b_1|x_1y_1) \ \cdot P^2(a_2b_2|x_2y_2) \\ & \cdot \ P^3(a_3b_3|x_3y_3) \ \cdot P^4(a_4b_4|x_4y_4) \\ = \sum \ & P^1(a_1b_1|00) \ \cdot P^2(a_2b_2|x_2y_2) \\ & \cdot \ P^3(a_3b_3|x_3y_3) \ \cdot P^4(a_4b_4|x_4y_4) \end{aligned} \tag{8}$$



xy \ ab	00	01	02	10	11	12	20	21	22
00		1/3		1/3					1/3
01	$\epsilon/3$	$(1-\epsilon)/3$		$(1-\epsilon)/3$		$\epsilon/3$		$\epsilon/3$	$(1-\epsilon)/3$
02		1/3		1/3					1/3
10	$\epsilon/3$	$(1-\epsilon)/3$		$(1-\epsilon)/3$		$\epsilon/3$		$\epsilon/3$	$(1-\epsilon)/3$
11		1/3		1/3					1/3
12		1/3		1/3					1/3
20		1/3		1/3					1/3
21		1/3		1/3					1/3
22	$\epsilon/3$	$(1-\epsilon)/3$		$(1-\epsilon)/3$		$\epsilon/3$		$\epsilon/3$	$(1-\epsilon)/3$

FIG. 3: (color online) An intuitional denotation of three-setting Bell inequality and $\mathbb{P}^\epsilon$. Different colors denote the different parameters in front of the corresponding terms in the three-setting Bell inequality, which red (latticed shading) denote -2, green (slash shading) denote -1, gray (backslash shading) denote 0 and blue (solid shading) denote +1. The numbers in those colored blocks denote elements of $\mathbb{P}^\epsilon$, and the probability of blocks without number is zero.

The summation calculates all the cases submitted to $a_1+a_2+a_3+a_4 \doteq 0$ and $b_1+b_2+b_3+b_4 \doteq 1$. $P^i(a_ib_i|x_iy_i)$ ($i=1,2,3,4$) denote the elements in ith box. Because when $a_i+b_i \doteq 2$ (see Fig.3) $P^i(a_ib_i|x_iy_i)$ always equals to zero independent of the inputs, then those terms can not show up in the summation. Thus, there are only two kind of outputs we need to consider: $a_i+b_i \doteq 0$ and $a_i+b_i \doteq 1$. Note that $a+b=0+1=1$ then $(a_1+b_1)+(a_2+b_2)+(a_3+b_3)+(a_4+b_4) \doteq a+b \doteq 1$. There are five possible combination of a_i+b_i satisfy this, which expressed as a table:

$$\left(\begin{array}{c|c|c|c|c|c} {}_{a_i+b_i}{}^{Case} & 1 & 2 & 3 & 4 & 5 \\ \hline a_1+b_1 \doteq & 0 & 0 & 0 & 1 & 1 \\ a_2+b_2 \doteq & 0 & 0 & 1 & 0 & 1 \\ a_3+b_3 \doteq & 0 & 1 & 0 & 0 & 1 \\ a_4+b_4 \doteq & 1 & 0 & 0 & 0 & 1 \end{array}\right). \tag{9}$$

According to the protocol, $P^1(a_1b_1|x_1y_1) = P^1(a_1b_1|xy) = P^1(a_1b_1|00)$, then the cases number $1,2,3$ which with $a_1+b_1 \doteq 0$ are ill-fitting, for $P^1(00|00)=0$. In the 4th case (see Fig.3), $x_2+y_2 = 2(x+y)+(a_1+b_1)+1 \doteq 2$, thus $P^2(a_2b_2|x_2y_2) = P^2(00|02) = 0$, also ill-fitting. Only the fifth case fit the requirement. By similar analyze, in case number 5, we get $x_2+y_2 \doteq 2(x+y)+(a_1+b_1)+4 \doteq 0+1+4 \doteq 2$, $x_3+y_3 \doteq 2(x+y)+(a_1+b_1)+(a_2+b_2) \doteq 0+1+1 \doteq 2$, and $x_4+y_4 \doteq 2(x+y)+(a_1+b_1)+(a_2+b_2)+(a_3+b_3)+2 \doteq 0+1+1+1+2 \doteq 2$.

Finally we get:

$$\begin{aligned} P^{new}(01|00) &= \sum P^1(01|00)\cdot P^2(01|02) \\ &\quad \cdot P^3(01|02)\cdot P^4(01|02) \\ &= 3^3\cdot\frac{1}{3}\cdot\frac{1}{3}\cdot\frac{1}{3}\cdot\frac{1}{3} = \frac{1}{3}. \end{aligned} \tag{10}$$

Here is the 3^3 come from: let a_i ($i=1,2,3$) freely chose, then $a_4 \doteq 0-a_1-a_2-a_3$ and $b_i \doteq 1-a_i$ ($i=1,2,3,4$) are determined. Each a_i has three possible output $a_i=0,1,2$ thus totaly have 3^3 terms contribute to the summation. Note that $P^{new}(01|00)+P^{new}(10|00)+P^{new}(22|00) = 3\cdot\frac{1}{3} = 1$, so the rest probability in those rows ($x\oplus y=0$) are zero. Similarly we get:

$$\begin{aligned} P^{new}(01|02) &= \sum P^1(01|02)\cdot P^2(01|00) \\ &\quad \cdot P^3(01|00)\cdot P^4(01|00) \\ &= 3^3\cdot\frac{1}{3}\cdot\frac{1}{3}\cdot\frac{1}{3}\cdot\frac{1}{3} = \frac{1}{3}. \end{aligned} \tag{11}$$

Then comparing to the initial box we see this protocol do not change the rows with $x\oplus y=0$ and $x\oplus y=2$.

Now we calculate the element $P^{new}(00|01)$ and $P^{new}(01|01)$ to finish the proof. Because $(a_1+b_1)+(a_2+b_2)+(a_3+b_3)+(a_4+b_4) \triangleq a+b \triangleq 0$, the possible combination table of $P^{new}(00|01)$ is:

$$\left(\begin{array}{c|c|c|c|c|c} {}_{a_i+b_i}{}^{Case} & 1 & 2 & 3 & 4 & 5 \\ \hline a_1+b_1 \triangleq & 0 & 0 & 1 & 1 & 1 \\ a_2+b_2 \triangleq & 0 & 1 & 0 & 1 & 1 \\ a_3+b_3 \triangleq & 0 & 1 & 1 & 0 & 1 \\ a_4+b_4 \triangleq & 0 & 1 & 1 & 1 & 0 \end{array}\right). \tag{12}$$

The probability in each case (denote as P_i, where $i = 1,2,3,4,5$) is $P_1 = 0$, $P_2 = \frac{\epsilon}{3}$, $P_3 = \frac{\epsilon}{3}\cdot(1-\epsilon)$, $P_4 = \frac{\epsilon}{3}\cdot(1-\epsilon)^2$, $P_5 = \frac{\epsilon}{3}\cdot(1-\epsilon)^3$. So $P^{new}(00|01) = \sum_{i=1}^{5} P_i = \frac{\epsilon}{3}\cdot(2-\epsilon)\cdot(\epsilon^2-2\epsilon+2) = \frac{\epsilon'}{3}$. similarly, we get $P^{new}(01|01) = \frac{(1-\epsilon)^4}{3} = \frac{1-\epsilon'}{3}$.

Combining the calculations above we proved that this protocol works. It turns four copies of nonlocal box $\mathbb{P}^{\epsilon}$ to a new nonlocal box $\mathbb{P}^{\epsilon'}$ with $\epsilon' = \epsilon\cdot(2-\epsilon)\cdot(\epsilon^2-2\epsilon+2)$ $(0<\epsilon<1)$.

III. THE CONTRACTING PROTOCOL AND TRIVIAL COMMUNICATION COMPLEXITY

One question left behind the above distillation protocol: whether the correlations in Eq. (6) have a quantum realization? The answer is negative. Although some correlations in Eq. (6) are arbitrarily close to the set of classical correlations, all of these correlations are postquantum and make communication complexity trivial after distillation. We demonstrate these result by giving a contracting protocol which recast these nonlocal boxes to correlated nonlocal boxes, since correlated nonlocal boxes make communication complexity trivial so are these boxes.

Contracting protocol.——Now we present the contracting protocol. Our protocol takes two copies of nonlocal box $\mathbb{P}^{\epsilon}$ defined in Eq. (6) and a shared uniform randomness $r \in \{0,1\}$ to a correlated nonlocal boxes

$$\mathbb{P}_{cnb}{}^{\epsilon'} = \left(\begin{array}{c||c|c|c|c} {}_{xy}{}^{ab} & 00 & 01 & 10 & 11 \\ \hline\hline 00 & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \hline 01 & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \hline 10 & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \hline 11 & \frac{1-\epsilon'}{2} & \frac{\epsilon'}{2} & \frac{\epsilon'}{2} & \frac{1-\epsilon'}{2} \end{array}\right), \tag{13}$$

where $\epsilon' = \frac{2}{3}\epsilon$. The protocol is illustrated in Fig.4.

Alice and Bob share two copies of boxes $\mathbb{P}^{\epsilon}$, we denote them Box 1 and Box 2. The input and output at each box is as show in the table:

	Alice	Bob
initial input of $\mathbb{P}_{cnb}{}^{\epsilon'}$	x	y
input to $\mathbb{P}^{\epsilon}$ of each box	x^*	y^*
output from $\mathbb{P}^{\epsilon}$ of each box	$a_k \quad (k=1,2)$	$b_k \quad (k=1,2)$
final output of $\mathbb{P}_{cnb}{}^{\epsilon'}$	a	b

Where x^*, y^* are the functions of x and y, while $a_i{}^*$, $b_i{}^*$ are functions of a_i and b_i. Those functions denote as follow:

x	0	1
x^*	1	2

y	0	1
y^*	1	2

a_1	0	1	2
a_1^*	0	1	1

b_1	0	1	2
b_1^*	1	0	1

a_2	0	1	2
a_2^*	1	0	0

b_2	0	1	2
b_2^*	0	1	0

Notable that although we used two boxes $\mathbb{P}^{\epsilon}$ in the protocol, at each time only one of their output is used in the final output, and which one is picked is determined by the value of randomness r. Different from the boxes in distillation protocol, in this protocol two initial boxes are not necessarily sequential arranged, because the input of Box 2 are independent of the output of Box 1.

Proof.——Now we prove those results by direct calculations. First, it is easy to see that the inputs and outputs of new box are no longer trits but bits, $x,y,a,b \in \{0,1\}$, which means it could express as a 4×4 matrix. Now we prove matrix (13) is the right one.

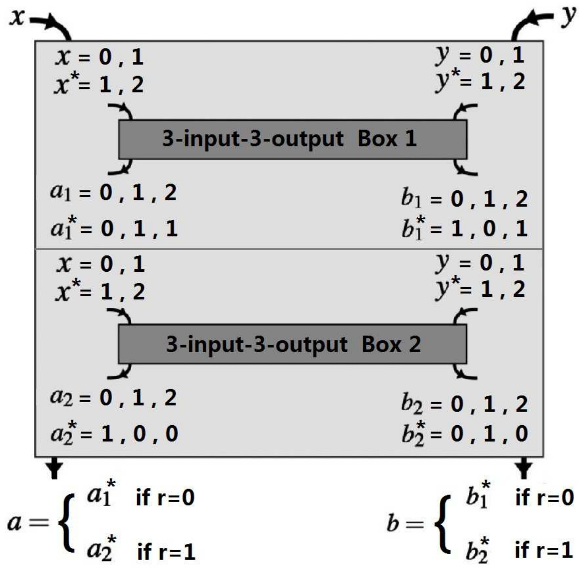


FIG. 4: Protocol to construct correlated nonlocal box. Alice and Bob use two $\mathbb{P}^{\epsilon}$ boxes and a sharing randomness r. They input x^* and y^* which is the function of x and y, respectively. a_i and b_i is the output of the ith box at each side, while ${a_i}^*$ and ${b_i}^*$ is the function of a_i and b_i, where $i = 1, 2$. They finally output a and b, which is function of ${a_i}^*$ and ${b_i}^*$.

Calculate $P^{new}(ab|xy)$.
$P^{new}(00|00) = \frac{1}{2} \cdot P(01|11) + \frac{1}{2} \cdot [P(10|11) + P(12|11) + P(20|11) + P(22|11)] = \frac{1}{2}$,
$P^{new}(11|00) = \frac{1}{2} \cdot [P(10|11) + P(12|11) + P(20|11) + P(22|11)] + \frac{1}{2} \cdot P(01|11) = \frac{1}{2}$.
Because $P^{new}(00|00) + P^{new}(11|00) = 1$, the rest elements in the row $(x, y) = (0, 0)$ are zero. Similarly, we get $P^{new}(00|01) = P^{new}(11|01) = P^{new}(00|10) = P^{new}(11|10) = \frac{1}{2}$.
While,
$P^{new}(00|11) = \frac{1}{2} \cdot P(01|22) + \frac{1}{2} \cdot [P(10|22) + P(12|22) + P(20|22) + P(22|22)] = \frac{3-2\epsilon}{6} = \frac{1-\epsilon'}{2}$, and
$P^{new}(01|11) = \frac{1}{2} \cdot [P(00|22) + P(02|22)] + \frac{1}{2} \cdot [P(11|22) + P(21|22)] = \frac{\epsilon}{3} = \frac{\epsilon'}{2}$.
Similarly, we get $P^{new}(10|11) = \frac{\epsilon'}{2}$ and $P^{new}(11|11) = \frac{1-\epsilon'}{2}$, which ends the proof. An inference from this protocol is all boxes in Eq. (6) will make communication complexity trivial. Because such boxes could construct a box in Eq. (13) with $0 < \epsilon' < \frac{2}{3}$, which have been proved to collapse the communication complexity after distillation [13].

IV. CONCLUSION

In summary, based on a three-setting Bell inequality, we have proposed a nonlocality distillation protocol that works efficiently for a class of 3-input-3-output nonlocal boxes $\mathbb{P}^{\epsilon}$. In the asymptotic limit, all boxes in this class can be distilled to the maximally nonlocal box $\mathbb{P}^{MAX}$. We also introduced a contracting protocol which can reduce $\mathbb{P}^{\epsilon}$ to correlated nonlocal box ${\mathbb{P}_{cnb}}^{\epsilon'}$. Because ${\mathbb{P}_{cnb}}^{\epsilon'}$ collapses the communication complexity after distillation, our contracting protocol has in fact proven that $\mathbb{P}^{\epsilon}$ can also trivialize communication complexity and thus unlikely to exist in nature. Our work represents a primary step to explore multi-setting Bell inequalities in the task of distilling nonlocality. It might be interesting to explore further the contracting technique in proving that certain nonlocal boxes are postquantum and unlikely to exist in nature.

J.L.C. is supported by National Basic Research Program (973 Program) of China under Grant No. 2012CB921900 and National Science Foundation of China (Grant Nos. 10975075 and 11175089). This work is also partly supported by the National Research Foundation and the Ministry of Education of Singapore.

[1] J. S. Bell, Physics (Long Island City, N. Y.) **1**, 195 (1964).
[2] G. Weihs et al, Phys. Rev. Lett. **81**, 5039 (1998); W. Tittel et al, Phys. Rev. Lett. **81**, 3563 (1998); D. N. Matsukevich et al, Phys. Rev. Lett. **100**, 150404 (2008).
[3] R. Colbeck, Ph.D. thesis, University of Cambridge, 2007; S. Pironio *et al*., Nature (London) **464**, 1021 (2010);

[4] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005); A. Acín *et al*., Phys. Rev. Lett. **98**, 230501 (2007); L. Masanes, S. Pironio, and A. Acín, Nature Commun. **2**, 238 (2011);

[5] N. Linden, S. Popescu, A. J. Short, and A. Winter, Phys. Rev. Lett. **99**, 180502 (2007).

[6] G. Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp, and F. Unger, Phys. Rev. Lett. **96**, 250401 (2006).

[7] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[8] G. Tóth and A. Acín, Phys. Rev. A **74**, 030306(R) (2006).

[9] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[10] P. G. Kwiat, S.Barraza-Lopez, A. Stefanov, and N. Gisin, Nature **409**, 1014 (2001); J. W. Pan *et al*., Nature **423**, 417 (2003); R.Reichle *et al*., Nature **443**, 838(2006).

[11] M. Forster, S. Winkler, and S. Wolf, Phys. Rev. Lett. **102**, 120401 (2009).

[12] J. Barrett, Phys. Rev. A **75**, 032304 (2007); J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).

[13] N. Brunner and P. Skrzypczyk, Phys. Rev. Lett. **102**, 160403 (2009).

[14] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).

[15] J. Clauser, M. Horne, A. Shimony, R. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[16] D. L. Deng, Z. S. Zhou, and J. L. Chen, Ann. Phys. (N.Y.) **324**, 1996 (2009).

[17] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002);

[18] J. L. Chen and D. L. Deng, Phys. Rev. A **79**, 012115 (2009).

[19] The maximal violation is 8. To see this clearly, please see FIG. 3. The color represent coefficients in Ineq. (2), we could find that the maximal coefficients in each row (except row “11”) is 1 (blue solid shading) and, each of those rows could contribute to non-signaling violation at most $1 \times 1 = 1$, the first “1” in multiplication is the maximal coefficient the second “1” is probability. Row “11” gives zero contribution and only 8 row have contribution to the non-signaling violation, that is why the maximal violation value is 8.