# Properties of dimension witnesses and their semidefinite programming relaxations

Piotr Mironowicz,[1,2,*] Hong-Wei Li,[3,4,†] and Marcin Pawłowski[5,‡]

[1]*Department of Algorithms and System Modelling, Faculty of Electronics, Telecommunications, and Informatics, Gdańsk University of Technology, Gdańsk 80-233, Poland*

[2]*National Quantum Information Centre in Gdańsk, Sopot 81-824, Poland*

[3]*Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*

[4]*Zhengzhou Information Science and Technology Institute, Zhengzhou 450004, China*

[5]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*

(Received 16 May 2014; revised manuscript received 16 July 2014; published 20 August 2014)

In this paper we develop a method for investigating semi-device-independent randomness expansion protocols that was introduced in Li *et al.* [H.-W. Li, P. Mironowicz, M. Pawłowski, Z.-Q. Yin, Y.-C. Wu, S. Wang, W. Chen, H.-G. Hu, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **87**, 020302(R) (2013)]. This method allows us to lower bound, with semi-definite programming, the randomness obtained from random number generators based on dimension witnesses. We also investigate the robustness of some randomness expanders using this method. We show the role of an assumption about the trace of the measurement operators and a way to avoid it. The method is also generalized to systems of arbitrary dimension and for a more general form of dimension witnesses than in our previous paper. Finally, we introduce a procedure of dimension witness reduction, which can be used to obtain from an existing witness a new one with a higher amount of certifiable randomness. The presented methods find an application for experiments [J. Ahrens, P. Badziag, M. Pawlowski, M. Zukowski, and M. Bourennane, Phys. Rev. Lett. **112**, 140401 (2014)].

DOI: 10.1103/PhysRevA.90.022322 PACS number(s): 03.67.Ac, 89.70.Cf

## I. INTRODUCTION

Nowadays information is one of the most important resources. However, it is very difficult to develop a reliable pseudo-random-number-generation (PRNG) method. Although there exist tests [1] that allow us to check whether a sequence of numbers conforms to a particular probability distribution, we can never be sure of its security without the knowledge of how the sequence was generated. If we know the pseudo-random-generating algorithm and the initial seed (or some sequence of generated numbers), then we can predict every sequence of numbers that will ever be obtained. All classical PRNGs have this significant [2] drawback.

On the other hand, quantum physics confuses philosophers with randomness on its deepest level. This randomness is unavoidable. We know that certain processes must be intrinsically random, or we would have to abandon some ideas that are fundamental to all physical theories. In this way the idea of the quantum randomness certification emerged [3]. If we want to be sure that a device does really produce random numbers, we perform a *Bell experiment* [4], which is a kind of self-testing. It works independently of the internal construction of the device used: if a value obtained in the experiment attains a certain threshold, we are sure that the generated results are indeed random, even if the device has been prepared by a malevolent party. The amount of the obtained secure randomness is precisely quantified by means of min-entropy [5–8]. This approach, in which we do not trust the vendor of our devices and draw conclusions only from the observed results, is called the *device-independent* (DI) approach [9].

Still, Bell experiments are very difficult to perform, since they require a high degree of precision and extremely high detection efficiencies. Now, suppose we send a state from one part of the device to another. Then we do not have any nonlocality, which is crucial for this method of certification. It was shown that, if we can bound the dimension of the communicated system, we still may use the *prepare and measure scheme* and certify the randomness [10]. Since we have to know something about the construction of the device, this approach is called the *semi-device-independent* (SDI) approach [11,12]. It offers a good compromise between security and experimental feasibility. In this framework, analogs of Bell inequalities, called *dimension witnesses* [10,13–16], are used.

Before we proceed we should stress that what we call random number generation is in fact a randomness *expansion*, the process that starts with some amount of initial randomness and uses it to obtain more of it. The presented self-testing procedure of the device also requires some amount of randomness (in order to choose the measurement settings in rounds of testing experiments). Strictly speaking, all quantum random number generators that use Bell inequalities or dimension witnesses to certify the randomness are randomness expanders.

In our previous paper [17] we have investigated the relation between random number expansion protocols based on correlations occurring in the Bell scenario and on protocols relying on the prepare and measure scheme. In this paper we develop these ideas. We clarify the methods from our previous paper and give a tighter lower bound on randomness. Using these methods we obtain better dimension witnesses, in particular, the one based on the Braunstein-Caves Bell inequality [18]. We also extend the applicability of our methods to arbitrary dimensions.

[*] piotr.mironowicz@gmail.com

[†] lihw@mail.ustc.edu.cn

[‡] dokmpa@univ.gda.pl

### A. Motivation

Suppose we are a developer of a random number generating device. Since consumers do not trust us, we are interested in finding a way of certification for our device. As mentioned above, a common method for the certification of quantum random number generators that are based on measurements of entangled particles is to estimate the value of a certain Bell inequality that is attained in this device. Still, it is too difficult to observe a loophole-free violation of Bell inequality. Thus we prefer prepare and measure protocols.

Both for prepare and measure protocols in SDI, and for correlation protocols in DI, we would like to define a value that measures how reliable is its particular realization. For this value we take the expectation value of the relevant dimension witness or Bell inequality, respectively, attained in the relevant protocol. This value is called a *security parameter*.

It is possible to consider several relations. One may ask whether, having a protocol of one type, we can relate it to some protocol of another type, in such a way that for the same value of their security parameters the min-entropy certified in one of them is upper or lower bounded by min-entropy certified by the other one.

One may start with a protocol based on a Bell inequality and construct out of it a prepare and measure protocol certifying a reasonable amount of min-entropy. This is useful since there are many randomness expansion protocols based on Bell inequalities [3,8] and it is easy to obtain new ones [19].

Another situation is when we begin with some SDI protocol and want to lower bound the certified randomness using efficient numerical methods from [20,21] that work in the device-independent approach. We present a way to obtain a new Bell inequality with the property that the DI protocol using it certifies at most as much randomness as the SDI protocol.

As mentioned above, SDI protocols are much easier to implement than the protocols based on entanglement. For this reason it is useful to have a method that allows us to develop devices of the first kind with the help of the well-established knowledge about the devices of the second type.

### B. Organization of this paper

The organization of this paper is as follows. In Sec. I A we present a scenario in which we are working. Next, in Sec. II we give basic information about Bell inequalities and dimension witnesses and recapitulate a heuristic method of obtaining a dimension witness from a Bell inequality [17]. Then, in Sec. III we precisely state the conditions when the randomness certified by the violation of a Bell inequality lower bounds the randomness certified by a certain value of dimension witness in the semi-device-independent scenario, and we investigate properties of a certain class of dimension witnesses and introduce a procedure of dimension witness reduction, which can be used to obtain from an existing witness a new one with a higher amount of certifiable randomness. In Sec. IV we give examples of application of the presented methods.

A short overview of Bell inequalities and dimension witnesses is given in Secs. II A and II B. In particular, Sec. II B states a set of useful properties of dimension witnesses in the case when we restrict our considerations to Hilbert spaces of dimension 2. The reader interested in obtaining new dimension witnesses should refer to methods from Sec. II C.

If the general problem of finding relaxation of the set of probabilities occurring in SDI is of interest, the reader should refer to Sec. III A. The following subsections are restricted to particular cases of SDI scenarios. Section III B considers Hilbert spaces of dimension 2 and a class of dimension witnesses called binary zero summing, while Sec. III C refers to the even more restricted case of so-called symmetric dimension witnesses. These additional assumptions about the problem allow us to obtain a better semidefinite programming (SDP) relaxation and, as shown in Sec. III D, to simplify the experimental setup.

Section IV contains a set of ready to use robust prepare and measure SDI randomness expansion protocols and illustrates the methods developed in preceding sections.

## II. BELL INEQUALITIES VERSUS DIMENSION WITNESSES

Let us recall some basic facts about Bell inequalities and dimension witnesses. These facts are stated in a formal way in subsections below, whereas here we give a short intuitive overview.

A Bell experiment involves at least two separated parties that share some quantum state and perform subsequent measurements with different settings without any communication between them. After a series of such measurements, the collected data are used to estimate the joint probabilities of the outcomes conditioned on the settings. A Bell operator is a linear combination of these probabilities. A Bell inequality gives a limit of the expectation value of the Bell operator allowed by the classical physics.

Dimension witnesses refer to a scenario with two parties, Alice and Bob. In each round they get some random inputs, $x$ and $y$. Afterward Alice sends a message to Bob. The message can either be a sequence of bits or a quantum state. When Bob receives this message, he performs some measurement and obtains a result $b$. After a series of such rounds the values of conditional probabilities $P(b|x,y)$ are estimated. A dimension witness states a maximal value of a certain linear combination of these probabilities that can be obtained with a given dimension of the communicated message.

### A. Bell inequalities

We define for a DI protocol the following:

*Definition 1.* Let $A$, $B$, $X$, and $Y$ be sets.

Probability distribution in the DI scheme is a conditional probability distribution $\mathbb{P}(A,B|X,Y)$ such that

$$\forall_{a\in A}\forall_{b\in B}\forall_{x\in X}\forall_{y\in Y}\, P(a,b|x,y) = \mathrm{Tr}\left(\rho M_x^a M_y^b\right),$$

where $\{\{M_x^a\}_{a\in A}\}_{x\in X}$ and $\{\{M_y^b\}_{b\in B}\}_{y\in Y}$ are sets of positive-operator valued measures (POVMs) on a Hilbert space $\mathbb{H}$, $\rho$ is a density matrix on $\mathbb{H}$, and

$$\forall_{a\in A}\forall_{b\in B}\forall_{x\in X}\forall_{y\in Y}\left[M_x^a, M_y^b\right] = 0 \text{ if } x \neq y. \quad (1)$$

We denote this probability by

$$\mathbb{P}[\rho, \{\{M_x^a\}_{a\in A}\}_{x\in X}, \{\{M_y^b\}_{b\in B}\}_{y\in Y}].$$

If $A = B = \{0,1\}$, then $\mathbb{P}(A,B|X,Y)$ is called binary.

The set of all DI probability distributions for given $A$, $B$, $X$, and $Y$ is denoted by $\mathcal{P}(A,B|X,Y)$.

This definition formalizes the intuition that all bipartite quantum probability distributions are realized by a physical scenario in that Alice and Bob share some quantum state and perform independent measurements on it.

Let us take two sets, $X$ and $Y$, that label the measurement settings of Alice and Bob in the DI scheme, and two sets, $A$ and $B$, that label their respective outcomes.

A Bell inequality is a linear function defined, in particular, for probability distributions $\mathcal{P}(A,B|X,Y)$. It is of the form

$$\begin{aligned} &I(A,B,X,Y,\{\alpha_{a,b,x,y}\},C_I)[\mathbb{P}(A,B|X,Y)] \\ &\quad \equiv = \sum_{a\in A}\sum_{b\in B}\sum_{x\in X}\sum_{y\in Y}\alpha_{a,b,x,y}P(a,b|x,y) + C_I, \end{aligned} \tag{2}$$

where $\alpha_{a,b,x,y}, C_I \in \mathbb{R}$. We omit $\mathbb{P}$ if it is obvious which probability distribution is considered.

The constant term $C_I$ in a Bell inequality does not change its properties. Still, we retain this general form, both for Bell inequalities and dimension witnesses, in the next section. In the following sections this allows us to keep the same maximal expected value when performing a transformation leading from one expression to another.

A particular form of Bell inequality is the following correlation form:

$$\begin{aligned} &\hat{I}(X,Y,\{\alpha_{x,y}\},\hat{C}_I)[\mathbb{P}(\{0,1\},\{0,1\}|X,Y)] \\ &\quad \equiv = \sum_{x\in X}\sum_{y\in Y}\hat{\alpha}_{x,y}C(x,y) + \hat{C}_I, \end{aligned} \tag{3}$$

with $\hat{\alpha}_{x,y}, \hat{C}_I \in \mathbb{R}$, and

$$\begin{aligned} C(x,y) = {} & P(0,0|x,y) - P(0,1|x,y) - P(1,0|x,y) \\ & + P(1,1|x,y). \end{aligned}$$

Obviously, the form (2) conforms to the form (3) if and only if $\alpha_{0,0,x,y} = \alpha_{1,1,x,y} = -\alpha_{0,1,x,y} = -\alpha_{1,0,x,y} = \hat{\alpha}_{x,y}$, and $\mathbb{P}(A,B|X,Y)$ is binary.

For given $A$, $B$, $X$, $Y$, $x_0 \in X$, $y_0 \in Y$, a Bell inequality $I$, and $s \in \mathbb{R}$ we define the following terms:

$$\begin{aligned} &P_{\text{guess}}(\mathbb{P}(A,B|X,Y),x_0,y_0) \\ &\quad \equiv \max_{a\in A, b\in B} P(a,b|x_0,y_0), \\ &H_\infty(\mathbb{P}(A,B|X,Y),x_0,y_0) \\ &\quad \equiv -\log_2[P_{\text{guess}}(\mathbb{P}(A,B|X,Y),x_0,y_0)], \\ &H_\infty^{\text{cert}}(I,x_0,y_0,s) \\ &\quad \equiv \min_{\mathbb{P}(A,B|X,Y)\in\mathcal{P}(A,B|X,Y)} H_\infty(\mathbb{P}(A,B|X,Y),x_0,y_0), \\ &\text{subject to } I[\mathbb{P}(A,B|X,Y)] \geqslant s. \end{aligned}$$

The expression $H_\infty(\mathbb{P}(A,B|X,Y),x_0,y_0)$ is called min-entropy, and $H_\infty^{\text{cert}}(I,x_0,y_0,s)$ is the min-entropy certified by the value $s$ of $I$.

### B. Dimension witnesses

For a SDI scheme, we have the following definition of the allowed probability distribution.

*Definition 2.* Let $\bar{B}$, $\bar{X}$, and $\bar{Y}$ be sets, and let $\mathbb{H}$ be a Hilbert space of a finite dimension $d$.

A probability distribution in the SDI scheme is a conditional probability distribution $\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y})$ such that for $b \in \bar{B}$, $x \in \bar{X}$, and $y \in \bar{Y}$ we have $P(b|x,y) = \text{Tr}(\rho_x M_y^b)$, where $\{\rho_x\}_{x\in\bar{X}}$ is a set of density matrices on $\mathbb{H}$, and $\{M_y^b\}_{b\in\bar{B}}$ are POVMs on $\mathbb{H}$ for all $y \in \bar{Y}$.

We say that $\mathbb{P}_d$ is realized by sets $\{\rho_x\}_{x\in\bar{X}}$ and $\{\{M_y^b\}_{b\in\bar{B}}\}_{y\in\bar{Y}}$, and we denote it

$$\mathbb{P}_d\big[\{\rho_x\}_{x\in\bar{X}}, \big\{\{M_y^b\}_{b\in\bar{B}}\big\}_{y\in\bar{Y}}\big].$$

If $\bar{B} = \{0,1\}$, then $\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y})$ is called a binary probability distribution.

The set of all SDI probability distributions for given $d$, $\bar{B}$, $\bar{X}$, and $\bar{Y}$ is denoted by $\mathcal{P}_d(\bar{B}|\bar{X},\bar{Y})$. The set of all SDI probability distributions with restrictions that $d = 2$, $\bar{B} = \{0,1\}$, and $\forall_{b\in\{0,1\}}\forall_{y\in\bar{Y}} \text{Tr}\, M_y^b = 1$ is denoted by $\mathcal{P}^{(P)}(\bar{X},\bar{Y})$.

Roughly speaking, a probability distribution in the SDI is realized by a setup in that Alice prepares and sends states to Bob, who, after receiving, performs on it some measurement.

Let $\bar{X}$ and $\bar{Y}$ be sets labeling the settings of Alice and Bob, in the SDI scheme, and let $\bar{B}$ be a set of the outcomes that Bob can obtain.

Dimension witnesses are linear functions of probability distributions of the form

$$\begin{aligned} &W(\bar{B},\bar{X},\bar{Y},\{\beta_{b,x,y}\},C_W)[\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y})] \\ &\quad \equiv = \sum_{b\in\bar{B}}\sum_{x\in\bar{X}}\sum_{y\in\bar{Y}}\beta_{b,x,y}P(b|x,y) + C_W, \end{aligned} \tag{4}$$

where $\beta_{b,x,y}, C_W \in \mathbb{R}$, and $d \geqslant 2$.

If $\bar{B} = \{0,1\}$, then the dimension witness is called binary. If $\forall_{b\in\bar{B}}\forall_{y\in\bar{Y}} \sum_{x\in\bar{X}}\beta_{b,x,y} = 0$, then the dimension witness is called zero summing.

For given $\bar{B}$, $\bar{X}$, $\bar{Y}$, $x_0 \in \bar{X}$, $y_0 \in \bar{Y}$, a dimension witness $W$, $s \in \mathbb{R}$, and $d \geqslant 2$ we define the following terms:

$$P_{\text{guess}}(\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y}),x_0,y_0) \equiv \max_{b\in\bar{B}} P(b|x_0,y_0), \tag{5a}$$

$$\begin{aligned} &H_\infty(\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y}),x_0,y_0) \equiv -\log_2[P_{\text{guess}}(\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y}),x_0,y_0)], \\ &P_{\text{guess}}^{\text{cert}}(W,x_0,y_0,s,d) \equiv \max_{\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y})\in\mathcal{P}_d(\bar{B}|\bar{X},\bar{Y})}\max_{b\in\bar{B}} P(b|x_0,y_0), \\ &\qquad \text{subject to } W[\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y})] \geqslant s, \end{aligned} \tag{5b}$$

$$\begin{aligned} &H_\infty^{\text{cert}}(W,x_0,y_0,s,d) \equiv -\log_2[P_{\text{guess}}^{\text{cert}}(W,x_0,y_0,s,d)], \\ &P_{\text{guess}}^{\text{cert}(P)}(W,x_0,y_0,s) \equiv \max_{\mathbb{P}_2(\bar{B}|\bar{X},\bar{Y})\in\mathcal{P}^{(P)}(\bar{X},\bar{Y})}\max_{b\in\bar{B}} P(b|x_0,y_0), \\ &\qquad \text{subject to } W[\mathbb{P}_2(\bar{B}|\bar{X},\bar{Y})] \geqslant s. \end{aligned} \tag{5c}$$

The expression $H_\infty(\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y}),x_0,y_0)$ is called min-entropy, and $H_\infty^{\text{cert}}(W,x_0,y_0,s)$ is the min-entropy certified by the value $s$ of $W$ (for the dimension $d$).

The meaning of these equations is as follows. Equation (5a) expresses the probability that the eavesdropper correctly guesses a single outcome generated on the side of Bob. The strategy used in eavesdropping is to guess the most probable result for a given distribution of outcomes $\mathbb{P}_d(\bar{B}|\bar{X},\bar{Y})$. Equation (5b) refers to the maximal guessing with all possible probability distributions of outcomes being in accordance with the observed security parameter. Equation (5c) gives this probability with a further restriction to the case with dimension 2 and projective measurements.

The following lemma summarizes some properties of dimension witnesses.

*Lemma 1.* Let $\mathbb{H}$ be a Hilbert space of dimension 2, and let $W$ be a binary dimension witness defined by certain $\bar{X}$, $\bar{Y}$, $\{\beta_{b,x,y}\}$, and $C_W$.

Let $\{\rho_x\}_{x\in\bar{X}} \equiv \mathcal{S}$ be a set of states on $\mathbb{H}$, and let $\{\{M_y^0,M_y^1\}\}_{y\in Y} \equiv \mathcal{M}$ be a set of binary POVMs on $\mathbb{H}$. Let $s \equiv W[\mathbb{P}_2(\mathcal{S},\mathcal{M})]$.

Then, the following implications hold:

(1) If $\forall_{y\in\bar{Y}} \sum_x \beta_{0,x,y} = \sum_x \beta_{1,x,y}$, then there exists a set of binary POVMs on $\mathbb{H}$, $\tilde{\mathcal{M}} \equiv \{\{\tilde{M}_y^0,\tilde{M}_y^1\}\}_y$, such that $\forall_{y,b}\operatorname{Tr}\tilde{M}_y^b = 1$, and $W[\mathbb{P}_2(\mathcal{S},\tilde{\mathcal{M}})] = s$.

(2) If $\sum_{b,x,y}\beta_{b,x,y} = 0$, and $\forall_{y,b}\operatorname{Tr}M_y^b = 1$, then for $\tilde{\mathcal{S}} = \{\mathbb{1} - \rho_x\}_{x\in\bar{X}}$, which is a set of states on $\mathbb{H}$, $W[\mathbb{P}_2(\tilde{\mathcal{S}},\mathcal{M})] = -s$.

(3) If $\forall_{y,b}\operatorname{Tr}M_y^b = 1$, then there exists a set of projective measurements, $\tilde{\mathcal{M}} \equiv \{\{\Pi_y^0,\Pi_y^1\}\}_{y\in\bar{Y}}$ with $\forall_{b\in\bar{B},y\in\bar{Y}}\operatorname{Tr}\left(\Pi_y^b\right) = 1$, such that $W[\mathbb{P}_2(\mathcal{S},\tilde{\mathcal{M}})] \geqslant s$.

*Proof.* (1) Let us take $y \in \bar{Y}$. Let $c_y = \frac{1}{2}[1 - \operatorname{Tr}(M_y^0)]$, $\tilde{M}_y^0 = M_y^0 + c_y\mathbb{1}$, and $\tilde{M}_y^1 = M_y^1 - c_y\mathbb{1}$. Obviously,

$$\tilde{M}_y^0 + \tilde{M}_y^1 = M_y^0 + M_y^1 = \mathbb{1}.$$

Now, we prove that $\forall_{y,b}\tilde{M}_y^b \succeq 0$. There exists an orthonormal basis $\{|0_y\rangle,|1_y\rangle\}$ in that

$$M_y^0 = v_0|0_y\rangle\langle 0_y| + v_1|1_y\rangle\langle 1_y|$$

and

$$M_y^1 = (1-v_0)|0_y\rangle\langle 0_y| + (1-v_1)|1_y\rangle\langle 1_y|,$$

where $v_0,v_1 \in [0,1]$. We have $c_y = \frac{1}{2}(1 - v_0 - v_1)$, and $\mathbb{1} = |0_y\rangle\langle 0_y| + |1_y\rangle\langle 1_y|$. Thus,

$$\tilde{M}_y^0 = \tfrac{1}{2}(1 + v_0 - v_1)|0\rangle\langle 0| + \tfrac{1}{2}(1 - v_0 + v_1)|1\rangle\langle 1|.$$

Since $1 + v_0 - v_1 \geqslant 0$ and $1 - v_0 + v_1 \geqslant 0$, we have $\tilde{M}_y^0 \succeq 0$, and $\operatorname{Tr}\tilde{M}_y^0 = 1$. Similarly, we check that $\tilde{M}_y^1 \succeq 0$ and $\operatorname{Tr}\tilde{M}_y^1 = 1$.

Repeating this construction for all $y \in \bar{Y}$, we obtain a set of POVMs, $\tilde{\mathcal{M}} \equiv \{\{\tilde{M}_y^0,\tilde{M}_y^1\}\}_{y\in\bar{Y}}$.

We have

$$\operatorname{Tr}\left(\rho_x\tilde{M}_y^b\right) = P(b|x,y) + (-1)^b c_y,$$

and thus

$$W[\mathbb{P}_d(\mathcal{S},\tilde{\mathcal{M}})] = \sum_{b,x,y}\beta_{b,x,y}\operatorname{Tr}\left(\rho_x\tilde{M}_y^b\right)$$

$$= s + \sum_y c_y\left(\sum_x\beta_{0,x,y} - \sum_x\beta_{1,x,y}\right) = s.$$

(2) We have

$$W[\mathbb{P}_2(\tilde{\mathcal{S}},\mathcal{M})] = \sum_{b,x,y}\beta_{b,x,y}\operatorname{Tr}\left[(\mathbb{1} - \rho_x)M_y^b\right]$$

$$= \sum_{b,x,y}\beta_{b,x,y}[1 - P(b|x,y)]$$

$$= \sum_{b,x,y}\beta_{b,x,y} - \sum_{b,x,y}\beta_{b,x,y}P(b|x,y) = -s.$$

(3) For any $y \in \bar{Y}$ we have

$$M_y^0 = \lambda_y|0_y\rangle\langle 0_y| + (1-\lambda_y)|1_y\rangle\langle 1_y|$$

and

$$M_y^1 = (1-\lambda_y)|0_y\rangle\langle 0_y| + \lambda_y|1_y\rangle\langle 1_y|,$$

for a certain basis $\{|0_y\rangle,|1_y\rangle\}$, $\lambda_y \in [0,1]$.

Let us define $s_y \equiv \sum_{b,x}\beta_{b,x,y}P(b|x,y)$. Denote

$$\sum_x\left(\beta_{0,x,y}\operatorname{Tr}(\rho_x|0_y\rangle\langle 0_y|) + \beta_{1,x,y}\operatorname{Tr}(\rho_x|1_y\rangle\langle 1_y|)\right)$$

by $s_{y,0}$ and similarly

$$\sum_x\left(\beta_{0,x,y}\operatorname{Tr}(\rho_x|1_y\rangle\langle 1_y|) + \beta_{1,x,y}\operatorname{Tr}(\rho_x|0_y\rangle\langle 0_y|)\right)$$

by $s_{y,1}$.

We have $s = \sum_y s_y$, and

$$s_y = \lambda_y s_{y,0} + (1-\lambda_y)s_{y,1}.$$

If $s_{y,0} \geqslant s_{y,1}$, then we take $\tilde{M}_y^0 \equiv |0_y\rangle\langle 0_y|$ and $\tilde{M}_y^1 \equiv |1_y\rangle\langle 1_y|$, otherwise we take $\tilde{M}_y^0 \equiv |1_y\rangle\langle 1_y|$ and $\tilde{M}_y^1 \equiv |0_y\rangle\langle 0_y|$. For $\tilde{\mathcal{M}} = \{\{\tilde{M}_y^0,\tilde{M}_y^0\}\}_{y\in\bar{Y}}$ it is easy to see that

$$W[\mathbb{P}_2(\mathcal{S},\tilde{\mathcal{M}})] = \sum_y\max(s_{y,0},s_{y,1}) \geqslant \sum_y s_y = s.$$

■

The first statement in this lemma says that in dimension 2 the condition that all measurement operators have trace 1 is not restrictive with regard to the set of values that is possible to attain. The second statement gives sufficient conditions under which an operation of negation of all states gives the same value of a dimension witness but with opposite sign. The third statement, which may be used to complement the first one, shows that under certain conditions it is not restrictive to use only projective measurements in the case when the values that can be attained are considered.

### C. A heuristic method for obtaining a dimension witness from a Bell inequality

Consider the following Bell experiment. Suppose we are given a Bell inequality of the form (2). Alice and Bob share an entangled state. Alice chooses a measurement setting $x \in X$ and obtains an outcome $a \in A$. For each setting $x$ and result $a$, we assign a conditional probability $P(a|x)$. Alice's measurement prepares some state at Bob's side. Next, Bob chooses a measurement setting $y \in Y$ and obtains an outcome $b \in B$. The probability that Bob gets $b$, knowing both the setting and the result of Alice, is $P(b|a,x,y)$.

We rewrite[1] the joint conditional probability of a given pair of results for a given pair of settings as $P(a,b|x,y) = P(b|a,x,y)P(a|x)$. Thus, defining $\bar{x} \equiv (a,x)$, the initial Bell inequality is transformed to the *form* of a dimension witness [see Eq. (4)], with $\beta_{b,\bar{x},y} \equiv \beta_{b,(a,x),y} \equiv \alpha_{a,b,x,y} P(a|x)$. We have $\bar{B} = B$, $\bar{X} = A \times X$, and $\bar{Y} = Y$.

The fact that it is possible to transform a Bell inequality into the form of a dimension witness leads us to some *heuristic* method to achieve an SDI protocol that certifies a reasonable amount of randomness, once we have a DI protocol. We get the SDI protocol if, instead of measuring on her side, Alice gets "the outcome" as a part of her input with the probability distribution $P(a|x)$. Thus, we obtain a pair $(a,x)$ that we use as an index of the state to be sent. This way, the device on the side of Alice prepares one of the $|\bar{X}| = |A| \cdot |X|$ states $\rho_{(a,x)}$. Bob still has $|\bar{Y}| = |Y|$ measurement settings.

## III. LOWER BOUNDS FOR DIMENSION WITNESSES VIA SEMIDEFINITE PROGRAMS

This section develops the method of studying the properties of SDI protocols with their semidefinite programming relaxations.

In Sec. III A we construct a sequence of devices that shows that the randomness certified by an SDI protocol can be lower bounded by the randomness certified in a certain DI protocol minus $\log_2 d$.

Then, in Sec. III B, the properties of binary zero-summing dimension witnesses are investigated. Recall that a dimension witness of the form given by Eq. (4) is called zero summing if

$$\forall_{b\in\bar{B}} \forall_{y\in\bar{Y}} \sum_{x\in\bar{X}} \beta_{b,x,y} = 0$$

and binary if $\bar{B} = \{0,1\}$. The reason to examine them is that it is possible to obtain tighter semidefinite relaxations for this class of dimension witnesses.

Finally, in Sec. III D, we show how to transform a symmetric dimension witness to a reduced one.

### A. Conversion from a dimension witness to a Bell operator

We consider a device D0 that we get from an untrusted vendor, consisting of two black boxes. Its only parameter that we can verify is the dimension of the message sent from one part of it to the another one. We assume that the device cannot communicate with the world outside the laboratory. The black box on Alice's side has buttons with labels $x \in \bar{X}$ and emits one of the quantum states of the dimension $d$ from the set of states $\{\rho_x\}_{x\in\bar{X}}$. These are unknown to us and are of arbitrary, possibly mixed, form. The black box on Bob's side has buttons with labels $y \in \bar{Y}$ and, after receiving the qubit from Alice's black box, it performs one of the measurements given by POVMs from the set $\{\{M_y^b\}_{b\in\bar{B}}\}_{y\in\bar{Y}}$. We do not know how the measurements are performed. This description is a semi-device-independent one, since we know only the dimension $d$.

Suppose we are given a dimension witness $W$ [of the form (4)] that achieves in the experiments on the device D0 the expected value $W_0$. We denote the conditional probability of obtaining the outcome $b$, when the chosen settings are $x$ and $y$, by $P_{\mathrm{D0}}(b|x,y)$.

The device D0 is not trusted, but it is possible to consider another device, D1, that consists of two parts, with buttons labeled by $x \in \bar{X}$ and $y \in \bar{Y}$ on Alice's side and on Bob's side, respectively. The parts are sharing a maximally entangled state of the dimension $d$. The part on Alice's side performs some measurement, depending on the chosen input $x$. This measurement projects Alice's part of the singlet on the state $\rho_x$ that is the same as the relevant state from the device D0. If the projection succeeded, which happens with the probability $\frac{1}{d}$, then the device returns $a = 0$ and changes the state on Alice's side into the state $\rho_x$, otherwise it returns $a = 1$. Since the shared state is a singlet, this measurement prepares the same $d$-dimensional state on Bob's side. Then he performs the same POVM $\{M_y^b\}_{b\in\bar{B}}$ as the device D0 and returns the outcome $b \in \bar{B}$.

The probability that Alice gets the outcome $a$ with the setting $x$ and simultaneously Bob gets the outcome $b$ with the setting $y$ is denoted by $P_{\mathrm{D1}}(a,b|x,y)$. It is easy to see that $P_{\mathrm{D0}}(b|x,y) = d\,P_{\mathrm{D1}}(0,b|x,y)$.

Now let us consider another device, D2. It has the same interface as D1, but the conditions on the internal working are relaxed; viz., we do not assume anything about the performed measurements, and Alice's and Bob's parts are allowed to share any, possibly entangled, state $\rho$ of an arbitrary dimension. The probability of obtaining the outcomes $a$ and $b$ with a given pair of settings $x$ and $y$ for Alice and Bob, respectively, is denoted by $P_{\mathrm{D2}}(a,b|x,y)$. We apply a constraint $\forall_{x\in X} P_{\mathrm{D2}}(0|x) = \frac{1}{d}$, where $P_{\mathrm{D2}}(a|x)$ is the probability of getting the outcome $a$ by Alice with the setting $x$ with the device D2.

Obviously, all the conditional probability distributions that can be obtained by the device D1 (and thus also by the device D0) can also be obtained by this device. Note that this description is fully device independent and that there are semidefinite programs in the Navascues-Pironio-Acin (NPA) hierarchy [20,21] that efficiently approximate the probability distributions of the device D2.

Since the device D2 is a relaxed version of the initial device D0, if both of them have the same value of the relevant security parameters, then the certified amount of min-entropy generated by the device D2 gives a lower bound of the min-entropy certified to be generated by the device D0.

We recapitulate the above results in the following theorem

*Theorem 1.* Let $B = \bar{B}$, $X = \bar{X}$, and $Y = \bar{Y}$ be sets. Let us take $s \in \mathbb{R}$, $d \geqslant 2$, a Bell inequality $I$ of the form (2), and a dimension witness $W$ of the form (4), satisfying $\beta_{b,x,y} = d\alpha_{0,b,x,y}$, $\alpha_{1,b,x,y} = 0$, and $C_I = C_W$.

Let $\mathcal{P}_{d,\mathrm{SDI}}(s)$ be a subset of $\mathcal{P}_d(\bar{B}|\bar{X},\bar{Y})$ with $d \geqslant 2$ (see definition 2) that satisfies $W = s$.

Let $\mathcal{P}_{\mathrm{DI}}(s)$ be a set of all probability distributions defined by $P(b|x,y) \equiv d\,P(0,b|x,y)$, where $\mathbb{P}(A,B|X,Y)$ is a device-independent probability distribution such that $I[\mathbb{P}(A,B|X,Y)] = s$, with $A = \{0,1\}$.

Then $\mathcal{P}_{d,\mathrm{SDI}}(s) \subseteq \mathcal{P}_{\mathrm{DI}}(s)$.

[1] We are using here the no-signaling principle.

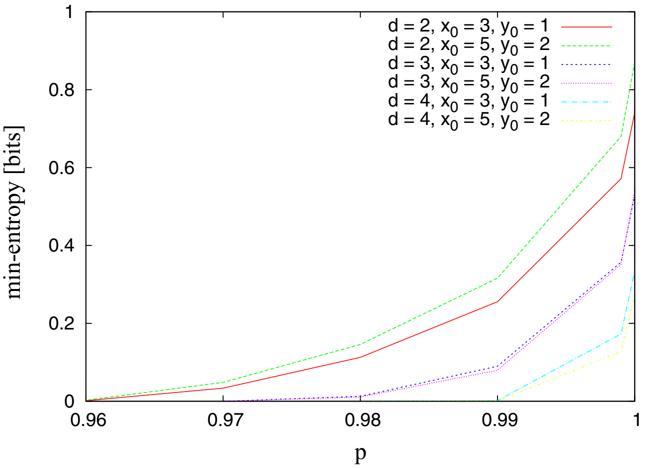


FIG. 1. (Color online) Lower bounds via SDP on the certified randomness for a dimension witness obtained from the CGLMP inequality [see Eq. (15) in Sec. IV] using the methods from Sec. III A for different values of the dimension $d$.

The theorem says that if a Bell inequality and a dimension witness are related in the given way then we can use the set of probabilities allowed with the former in the DI as a relaxation of the set of probabilities allowed with the latter in the SDI.

Figure 1 shows an example of the application of theorem 1.

In this way we obtain a way to get a relation between Bell inequalities and dimension witnesses with the property that the amount of randomness certified by a Bell inequality lower bounds the amount of randomness certified by the relevant dimension witness. One of the key features of the set $\mathcal{P}_{\mathrm{DI}}$ is that it can be efficiently approximated using semidefinite programming with the NPA hierarchy.

From the definition of $\mathcal{P}_{\mathrm{DI}}(B|X,Y)$, namely, using $P(b|x,y) = dP(0,b|x,y)$, we get that the certified min-entropy of the SDI protocol is lower bounded by the one of the DI protocol minus $\log_2 d$. A notable property of the method is that we obtain a bound for any dimension of the communicated system changing only a value of the linear bound.

### B. Binary zero-summing dimension witnesses

Let us start with a binary zero-summing dimension witness $W = W(\{0,1\},\bar{X},\bar{Y},\{\beta_{b,x,y}\},C_W)$ that is used to certify the randomness generated by measuring the state $x_0 \in \bar{X}$ with the measurement setting $y_0 \in \bar{Y}$. Let $\{\rho_x\}_{x\in\bar{X}}$ and $\{\{M_y^0,M_y^1\}\}_{y\in\bar{Y}}$ be the states and measurements that maximize the guessing probability [see Eq. (5a)] of the generated bits by the untrusted vendor.

First note that the value of such a dimension witness does not change if, for arbitrary $y \in \bar{Y}$, the measurement is changed to $\{M_y^0 + c\mathbb{1}, M_y^1 - c\mathbb{1}\}$, where $c$ is such that the spectrum of the operators remains in the range $[0,1]$. Thus, since the potential adversary is interested in increasing the probability of a particular outcome of the measurement $y_0$ as much as possible,[2] the form of these measurements that maximizes his guessing probability is the following:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1-\delta \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 0 & \delta \end{bmatrix}. \tag{6}$$

Let us note that by lemma 1(1) and 1(3) it is not restrictive for the vendor to use only projectors of trace 1 for the measurements different than $y_0$.

The strategy of using a measurement of the form (6) for the setting $y_0$ and projectors of trace 1 for all remaining measurements is equivalent to using the following mixed strategy. In $\delta$ cases, a projective measurement of trace 1 is used for the measurement $y_0$ (we call this strategy $P$), and in $1-\delta$ cases the outcome is deterministic—this is referred to hereafter as a deterministic strategy, or simply $D$. For the remaining measurements the same projective measurements of trace 1 are used in both cases.

The guessing probability for the strategy $D$ is 1 and for the strategy $P$ is $p$, and thus the average guessing probability is

$$(1-\delta) + \delta p. \tag{7}$$

In the case of a zero-summing dimension witness with the deterministic strategy, measurements with the setting $y_0$ give no contribution to the value of the witness. Thus the certification of the randomness with the dimension witness

$$W = W(\{0,1\},\bar{X},\bar{Y},\{\beta_{b,x,y}\},C_W)$$

when the vendor of the device uses the mixed strategy that is, after applying a certain affine transformation [see Eq. (7)], equivalent to the certification with a dimension witness

$$W_{(\delta,y_0)}(\{0,1\},\bar{X},\bar{Y},\{\tilde{\beta}_{b,x,y}\},C_W),$$

with $\tilde{\beta}_{b,x,y}$ defined in Eq. (8), and the strategy $P$, where the guessing probability of Eve is given by Eq. (7).

Since the vendor may choose any $\delta \in [0,1]$ that allows us to observe the required value of the dimension witness $W$ when calculating the lower bound on the certified min-entropy, the worst case should be considered for a particular situation.

In this way, we have proven the following:

*Lemma 2.* Let $W = W(\{0,1\},\bar{X},\bar{Y},\{\beta_{b,x,y}\},C_W)$ be a binary zero-summing dimension witness, $x_0 \in \bar{X}$, and $y_0 \in \bar{Y}$. Let $W_{(\delta,y_0)} = W_{(\delta,y_0)}(\{0,1\},\bar{X},\bar{Y},\{\tilde{\beta}_{b,x,y}\},C_W)$ be a dimension witness, where

$$\tilde{\beta}_{b,x,y} = \begin{cases} \beta_{b,x,y} & \text{if} \quad y \neq y_0 \\ \delta\beta_{b,x,y} & \text{if} \quad y = y_0 \end{cases}. \tag{8}$$

Then

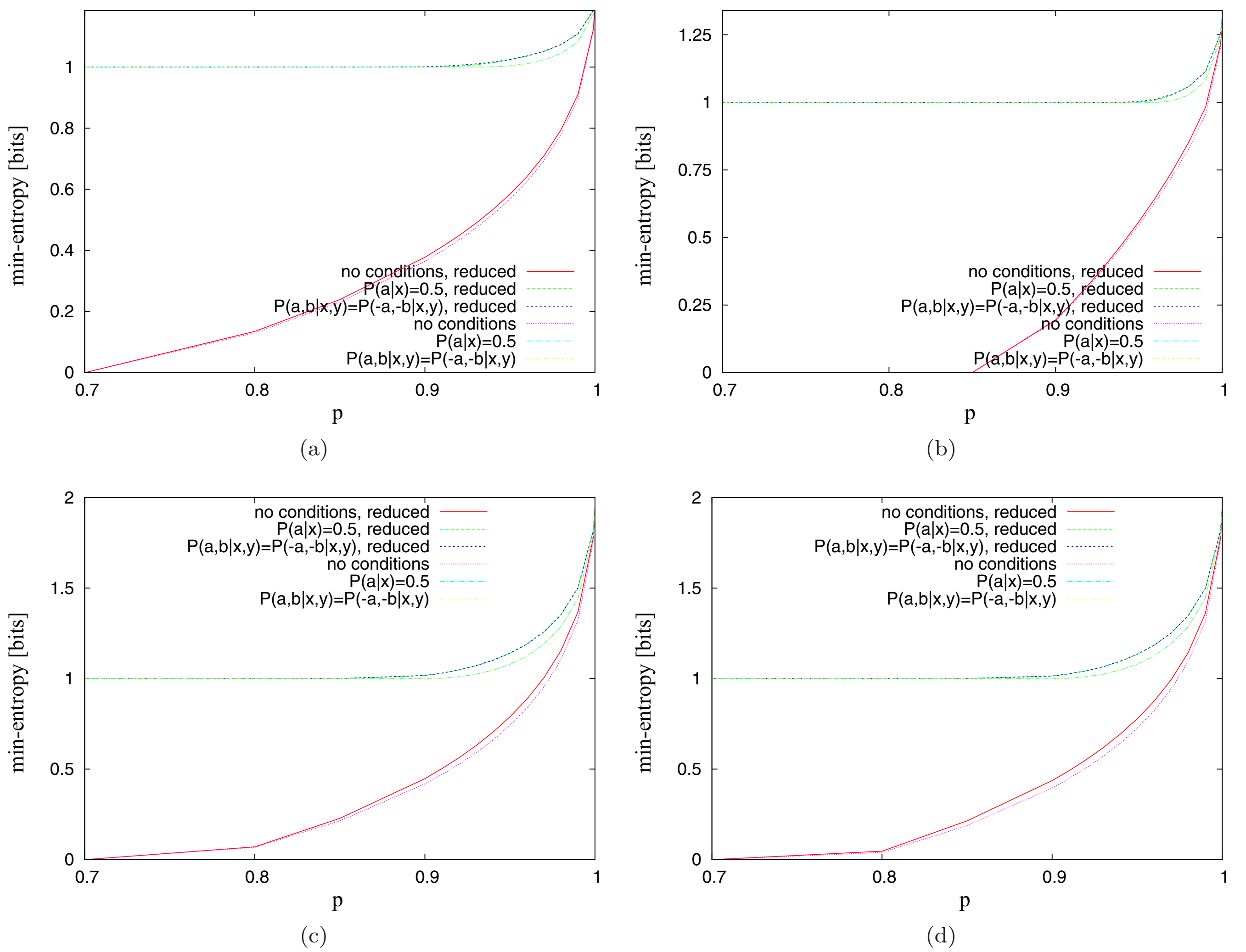
$$P_{\text{guess}}^{\text{cert}}(W,x_0,y_0,s,2) = \max_{\delta\in[0,1]} \left[(1-\delta) + \delta P_{\text{guess}}^{\text{cert}(P)}(W_{(\delta,y_0)},x_0,y_0,s)\right],$$

where $P_{\text{guess}}^{\text{cert}}(W,x_0,y_0,s,2)$ and $P_{\text{guess}}^{\text{cert}(P)}(W,x_0,y_0,s)$ are defined in Eqs. (5b) and (5c).

The consequence of restricting the vendor to dimension 2 and measurements of trace 1 is that the following holds for all $x \in \bar{X}$ and $y \in \bar{Y}$ and for any $b \in \{0,1\}$:

$$\begin{aligned} \mathrm{Tr}\left(\neg\rho_x M_y^{\neg b}\right) &= \mathrm{Tr}\left[(\mathbb{1}-\rho_x)(\mathbb{1}-M_y^b)\right] \\ &= 1 - \mathrm{Tr}\left(M_y^b\right) + \mathrm{Tr}\left(\rho_x M_y^b\right) \\ &= \mathrm{Tr}\left(\rho_x M_y^b\right) = P(b|x,y), \end{aligned} \tag{9}$$

[2] Recall that $y_0$ is the setting Bob used to generate the randomness.



(a)

(b)

(c)

(d)

FIG. 2. (Color online) Lower bounds via SDP on min-entropy certified by different Bell inequalities for different levels of noise. Several situations are considered. This illustrates the relations summarized in lemma III B. *Reduced* Bell inequalities refer to lower bounds on reduced symmetric dimension witnesses (see Sec. III C) for strategy $P$ (see Sec. III B). We observe that using reduced dimension witnesses provides an advantage in terms of certifiable randomness. Recall that by theorem III A and a remark below it, the lower bound for the randomness of a dimension witness is given by the randomness of the Bell inequality minus $\log_2 d$. This plot refers to the case with $d = 2$, and thus these methods that give values below $\log_2 2 = 1$ are not feasible for the given value of $p$. The reduced Bell operators are given by formulas (19), (22), (24), and (26), while Bell operators that may be used for lower bounding the randomness full symmetric dimension witnesses are given by formulas (18), (23), (25), and (29). These refer to $T2$ (2a), $T3$ (2b), $BC3$ (2c), and modCHSH (2d) cases, respectively.

where $\neg\rho_x \equiv \mathbb{1} - \rho_x$. This relation allows us to refine the relaxation given in Sec. III A.

Let us consider a device D1′ that models the strategy $P$ by sharing the singlet state, projecting on states $\{\rho_x\}_{x\in\bar{X}}$ on the side of Alice, and measuring on the side of Bob with measurements of trace 1, $\{\{M_y^0, M_y^1\}\}_{y\in\bar{Y}}$. In contrast to the device D1, if the projection on a state $\rho_x$ for any $x \in \bar{X}$ fails, then the prepared state is $\neg\rho_x$. It is easy to see that, by Eq. (9), the probabilities obtained in this device are constrained by the following relation:

$$P(a,b|x,y) = P(\neg a,\neg b|x,y), \tag{10}$$

for all $a,b \in \{0,1\}$, $x \in X$, and $y \in Y$. A further relaxation, analogous to the one leading from the device D1 to the device D2, allows us to obtain a device D2′, satisfying the relation (10), that can be modeled by a semidefinite program in the device-independent scheme.

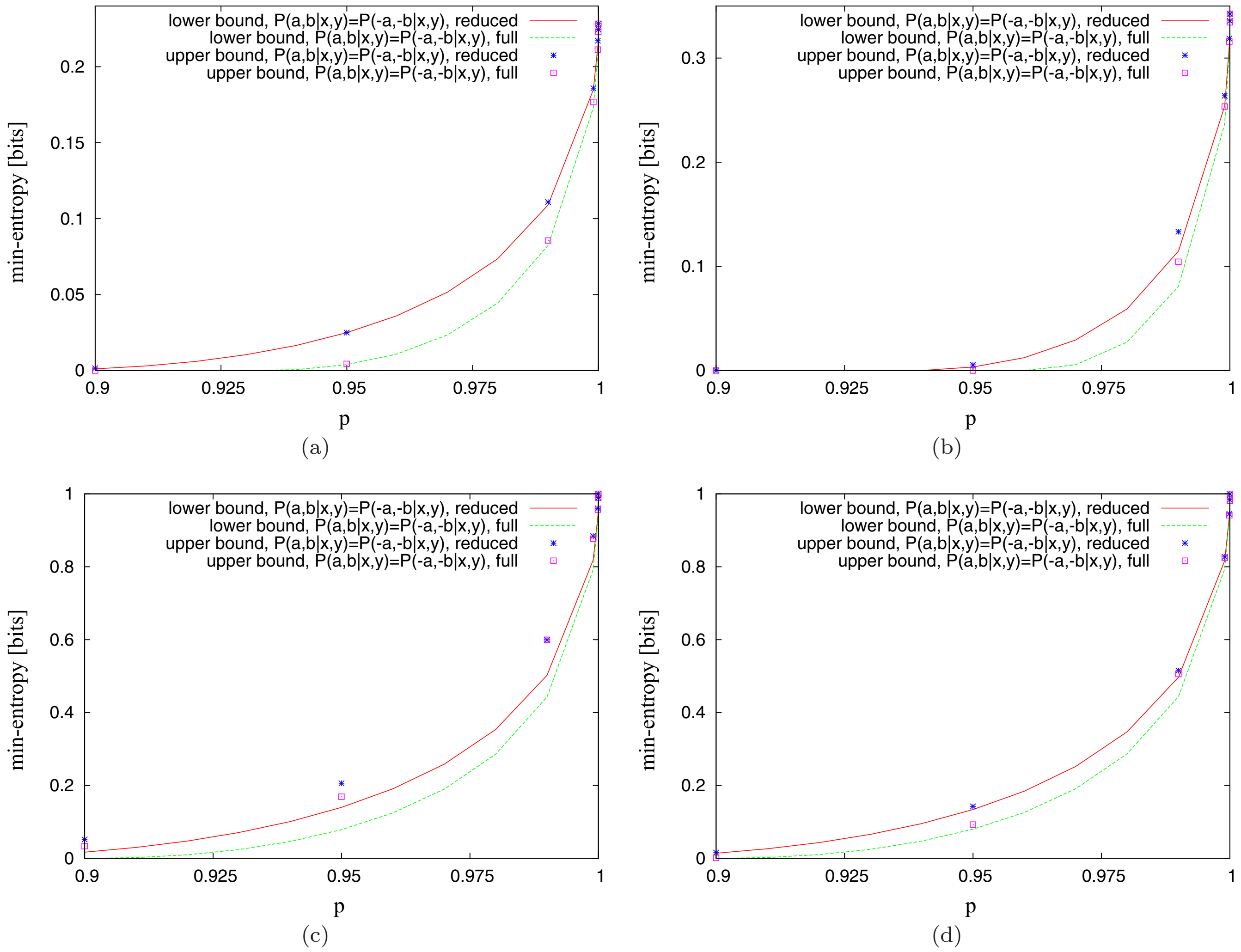
In this way we have proven the following theorem

*Theorem 2.* Let $X = \bar{X}$ and $Y = \bar{Y}$ be sets. Let us take $s \in \mathbb{R}$, a Bell inequality $I$ of the form (2), and a binary zero-summing dimension witness $W$ of the form (4), satisfying $\beta_{b,x,y} = \alpha_{0,b,x,y} = \alpha_{1,\neg b,x,y}$.

Let $\mathcal{P}^{(P)}_{\mathrm{SDI}}(s)$ be a subset of $\mathcal{P}^{(P)}(\bar{X},\bar{Y})$ (see definition 2) containing those probabilities $\mathbb{P}_2(\{0,1\}|\bar{X},\bar{Y})$ that satisfies $W[\mathbb{P}_2] = s$.

Let $\mathcal{P}_{\mathrm{DI,cond}}(s)$ be a set of probability distributions defined by $P(b|x,y) \equiv P(0,b|x,y) + P(1,\neg b|x,y)$, where $\mathbb{P}(A,B|X,Y)$ is a device-independent probability distribution that satisfies $I[\mathbb{P}(A,B|X,Y)] = s$ and the relation (10).

Then $\mathcal{P}^{(P)}_{\mathrm{SDI}}(s) \subseteq \mathcal{P}_{\mathrm{DI,cond}}(s)$.



(a)

(b)

(c)

(d)

FIG. 3. (Color online) Numerical lower bounds via SDP and upper bounds on the randomness certified for strategy $P$ (see Sec. III B), for both reduced (see Sec. III C) and full certificates and different Bell operators and dimension witnesses. Here we observe even more advantage for the reduced versions. The plots refer to the cases of $T2$ (3a), $T3$ (3b), $BC3$ (3c), and modCHSH (3d), respectively.

Similarly to theorem 1, this theorem shows how to use the set of probabilities allowed in the DI as a relaxation of the relevant set in the SDI, this time in a more restricted case.

It is straightforward to check that the following lemma holds:

*Lemma 3.* Let $a,b \in \{0,1\}$, and let us assume that

$$P(a,b|x,y) + P(a,\neg b|x,y) = P(a|x,y) = P(a|x),$$
$$P(a,b|x,y) + P(\neg a,b|x,y) = P(b|x,y) = P(b|y),$$

i.e., the no-signaling principle, and that the outcomes of Bob are binary, namely,

$$P(b|a,x,y) + P(\neg b|a,x,y) = 1. \tag{11}$$

Then we have the following implications:

(1) If $P(a,b|x,y) = P(\neg a,\neg b|x,y)$ holds, then we have $P(a|x) = \frac{1}{2}$ and $P(b|a,x,y) + P(b|\neg a,x,y) = 1$.

(2) If $P(b|a,x,y) + P(b|\neg a,x,y) = 1$ holds, then we have $P(b|a,x,y) = P(\neg b|\neg a,x,y)$.

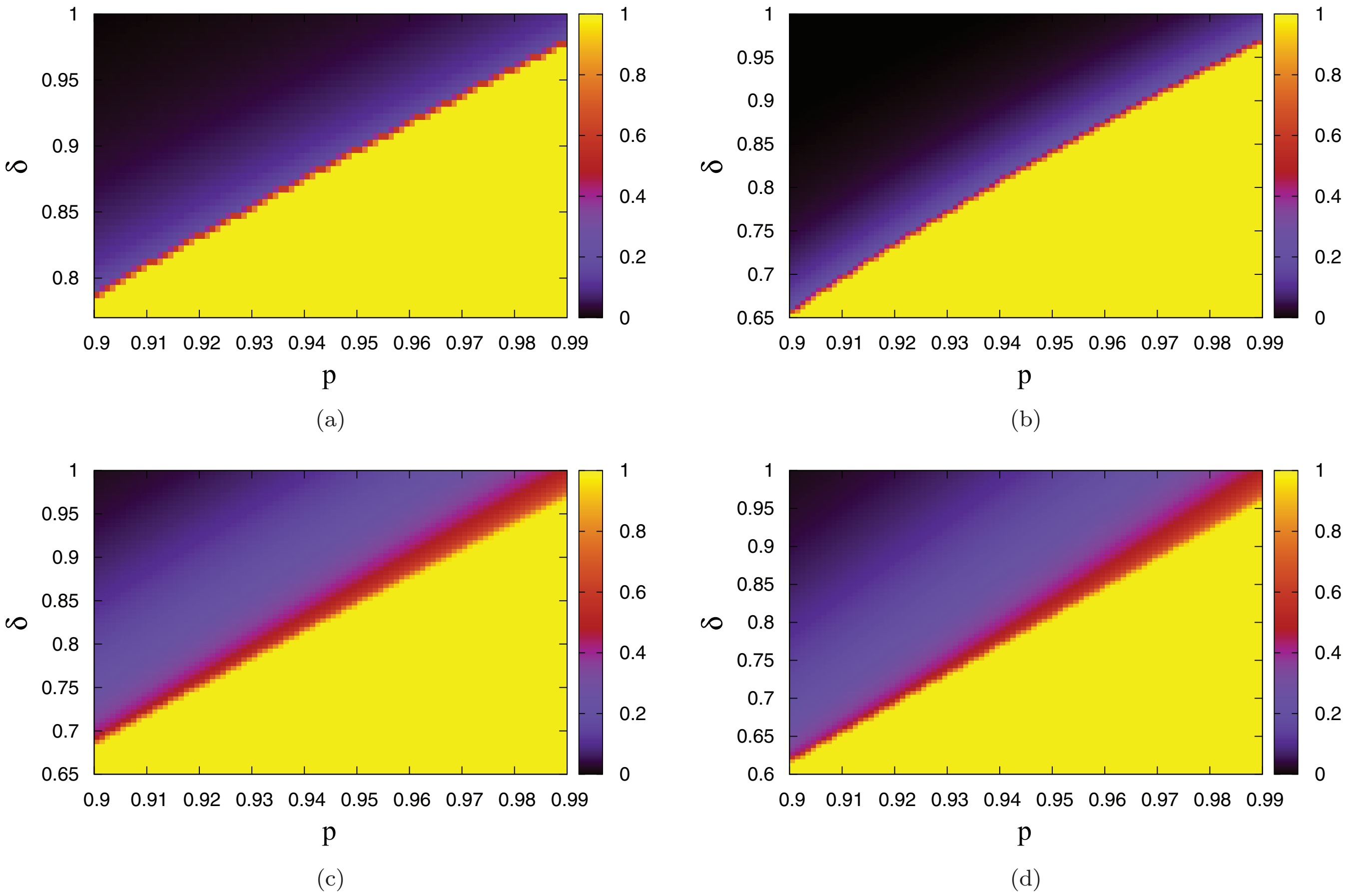
(3) If $P(a|x) = \frac{1}{2}$ and $P(b|a,x,y) = P(\neg b|\neg a,x,y)$ hold, then we have $P(a,b|x,y) = P(\neg a,\neg b|x,y)$.

From this lemma we get that the condition $P(a,b|x,y) = P(\neg a,\neg b|x,y)$ is more restrictive than $P(a|x) = \frac{1}{2}$. From this, we conjecture that for any $s$

$$\mathbb{P}^{(P)}_{\mathrm{SDI}}(s) \subseteq \mathbb{P}_{\mathrm{DI,cond}}(s) \subseteq \mathbb{P}_{\mathrm{DI}}(s),$$

where the sets are defined in theorems 1 and 2. Thus theorem 2 refines the results of theorem 1 for the case of binary zero-summing dimension witnesses.

Figures 2 and 3 show examples of lower and upper bounds for min-entropy certified when the untrusted vendor uses the strategy $P$. Figures 4 and 5 show lower bounds for the certified min-entropy in the case when the untrusted vendor uses the mixed strategy. All lower bounds are calculated via semidefinite programs with the NPA hierarchy, using the interior point method with the SeDuMi solver [22,23]. The upper bounds have been obtained by finding explicit representations of states and measurements. This optimization has been carried over pure states and projective measurements and is not guarantied to reach global minima, in contrast to the semidefinite programming method.



(a)

(b)

(c)

(d)

FIG. 4. (Color online) Lower bounds via SDP on the certified randomness in the semi-device-independent scenario for the reduced dimension witnesses (see Sec. III C) when the untrusted vendor uses the mixed strategy with different values of the parameter $\delta$ (see Sec. III B). If a certain value of a dimension witness is impossible to achieve with a given $\delta$, then, since the eavesdropper cannot mislead us this way, we use the value 1. The cases of $T2$ (4a), $T3$ (4b), $BC3$ (4c), and modCHSH (4d) are shown on these plots.

Interestingly, in all protocols considered in Fig. 5, it is optimal for the adversary to use $\delta = 1$; i.e., using the mixed strategy gives no gain compared to the strategy $P$.

### C. Symmetric dimension witnesses

Let us introduce the following definition:

*Definition 3.* A dimension witness $W$ of the form (4) with the set of Alice's settings $\bar{X}$ of even size, and $\bar{B} = \{0,1\}$, is *symmetric*, if there exists a surjective automorphism $\phi : \bar{X} \to \bar{X}$ with $\phi(x) \neq x$ and $\beta_{b,x,y} = -\beta_{b,\phi(x),y} = -\beta_{\neg b,x,y}$.

For a set $\bar{\chi} \subset \bar{X}$ we define

$$W_{\bar{\chi}} \equiv \sum_{b\in\{0,1\}} \sum_{x\in\bar{\chi}} \sum_{y\in\bar{Y}} \beta_{b,x,y} P(b|x,y).$$

A set $\bar{\chi} \subset \bar{X}$ satisfying $\bar{\chi} \cap \phi(\bar{\chi}) = \emptyset$ and $\bar{\chi} \cup \phi(\bar{\chi}) = \bar{X}$ is called a half of $\bar{X}$.

If a set $\bar{\chi}$ is a half, then $W_{\bar{\chi}}$ is called a dimension witness reduced with respect to $\chi$. $\phi$ and $\chi$ may be omitted if it is obvious which automorphism or set is considered.

It is easy to see that every symmetric dimension witness is also a binary zero-summing dimension witness.

If a dimension witness is symmetric, then there is a way to reduce the size of $\bar{X}$, while the obtained dimension witness can certify at least the same amount of randomness as the initial one.

The following theorem is an immediate result of theorem 2 and lemma 1(2):

*Theorem 3.* For a SDI protocol using the strategy $P$ with a symmetric dimension witness that attains the value of the security parameter $s$ on a Hilbert space of dimension 2 and certifies the randomness $r$, the same value can still be attained and certifies at least the same randomness, if we impose an additional condition that $\rho_x = \mathbb{1} - \rho_{\phi(x)}$, which implies $P(b|x,y) = P(\neg b|\phi(x),y)$.

Simply speaking this theorem says that symmetric dimension witnesses possess some kind of degree of freedom that does not increase the range of values that can be attained but allows an adversary to "distribute" the value of the witness among the states in such a way that misleads about the reliability of the device. The proposed method shows a way to remove this freedom.

### D. Obtaining and reducing a symmetric dimension witness

It is possible to use a known Bell inequality to obtain a new dimension witness. Examples of such protocols, $T2$, $T3$, $BC3$, and modCHSH, are described below in Sec. IV.

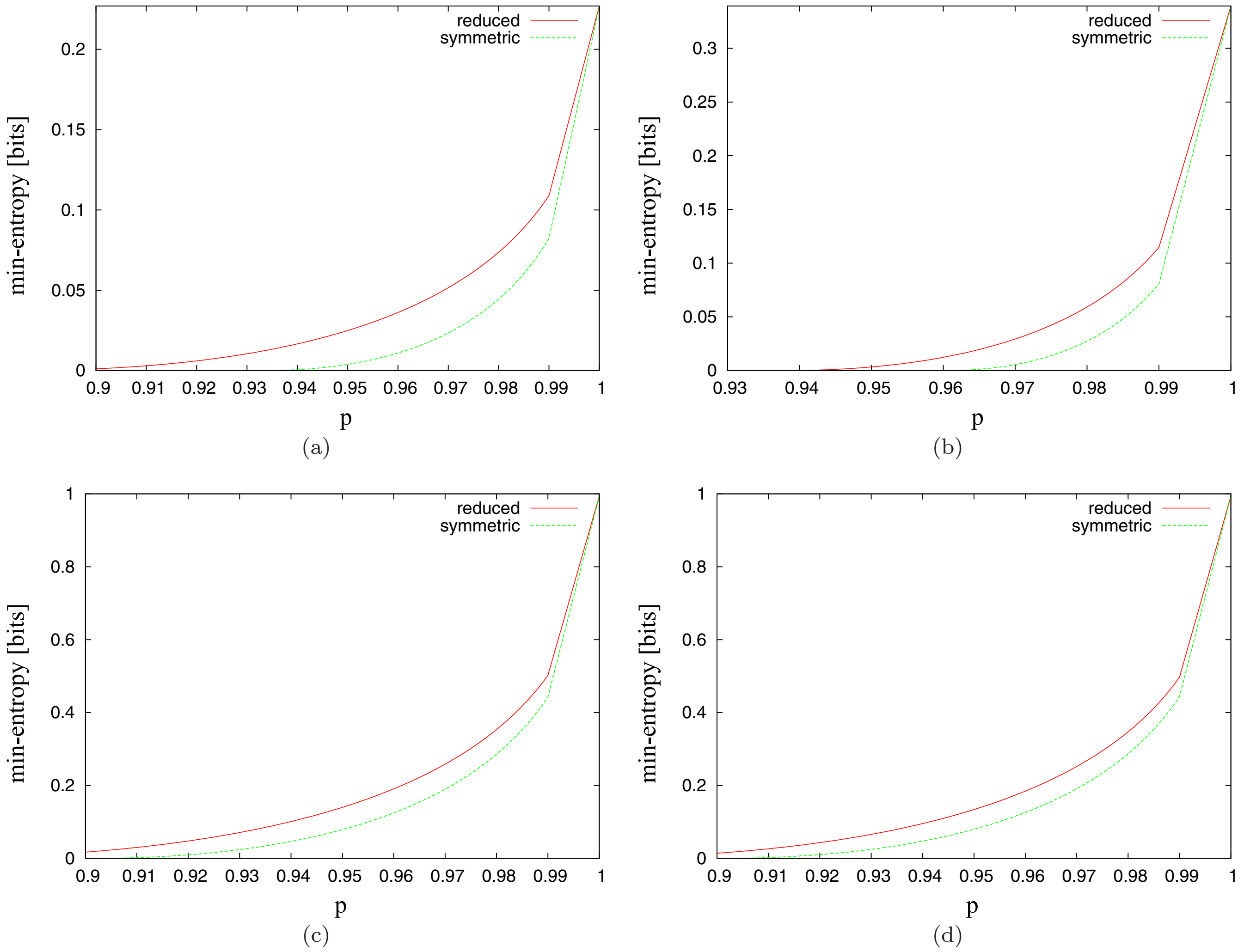


FIG. 5. (Color online) Lower bounds via SDP on the certified randomness for both reduced and symmetric dimension witnesses (see Sec. III C) when the untrusted vendor uses the mixed strategy with the worst case value of the parameter $\delta$ (see Sec. III B), which is 1 in all cases. The plots shows the cases referring to $T2$ (5a), $T3$ (5b), $BC3$ (5c), and modCHSH (5d).

From a Bell inequality of the form

$$\sum_{x,y}\dot{\alpha}_{x,y}\left\{\frac{1}{2p_{0,x}}[P(0,0|x,y)-P(0,1|x,y)] + \frac{1}{2p_{1,x}}[P(1,1|x,y)-P(1,0|x,y)]\right\} \qquad (12)$$

(where $p_{0,x}+p_{1,x}=1$), using the method from Sec. II C, we obtain a symmetric dimension witness of the form (4), with $\beta_{0,x,y}=\dot{\alpha}_{x,y}$ and $\beta_{1,x,y}=-\dot{\alpha}_{x,y}$. For the new SDI protocol, we assume that $a$ is chosen randomly by Alice, with the distribution $P(a|x)\equiv p_{a,x}$.

Note that Bell inequalities in the correlation form [see Eq. (3)] are a special case of the inequalities of the form (12) with $p_{a,x}=\frac{1}{2}$ and $\dot{\alpha}_{x,y}=\bar{\alpha}_{x,y}$, which means that it is always possible to obtain a symmetric dimension witness from a correlation-based Bell inequality. Then $C(x,y)$ turns into

$$\begin{aligned} W'(x,y) &\equiv \tfrac{1}{2}[P(0|(0,x),y)+P(1|(1,x),y) \\ &\quad - P(1|(0,x),y) - P(0|(1,x),y)] \\ &= P(0|(0,x),y) - P(0|(1,x),y). \end{aligned} \qquad (13)$$

It is easy to see that a dimension witness which is a linear combination of expressions (13) is symmetric.

We define $\phi((a,x))\equiv(\neg a,x)$ and $\chi\equiv\{(0,x):x\in X\}\subseteq\{0,1\}\times X$. The condition $P(b|(a,x),y)=P(\neg b|(\neg a,x),y)$ allows us to take

$$W(x,y)\equiv 2P(0|(0,x),y)-1\equiv 2P(0|x,y)-1, \qquad (14)$$

instead of $W'(x,y)$ from Eq. (13), which is an example of the reduction.

Note that using the method of reduction of a symmetric dimension witness the number of states used by Alice is reduced twice without loss of ability to certify both the randomness and the dimension.

On the other hand every symmetric dimension witness is a linear combination of expressions $D(x,y)\equiv P(0|x,y)-P(1|x,y)$ that refers in the DI scenario to the expression $2P(0,0|x,y)-2P(0,1|x,y)$. Assuming that the dimension of the Hilbert space is 2, and the eavesdropper uses the strategy $P$, we get from Eq. (10) that $2P(0,0|x,y)-2P(0,1|x,y)=C(x,y)$. Thus, there is a one-to-one relation between symmetric dimension witnesses and correlation Bell inequalities.

## IV. EXAMPLES OF APPLICATION

In this section we give five examples of applications of the methods presented above. Four of them—B, C, D, and E—concern Bell inequalities in the correlation form and symmetric dimension witnesses.

All figures are plotted with respect to a relative parameter $p$. The value $p = 1$ refers to the case when the maximal value of the relevant Bell inequality or dimension witness is achieved. Values $p < 1$ relate to the situation with noise, when the attained value is equal to the maximum multiplied by $p$.

### A. CGLMP

In the first example we start with the CGLMP inequality introduced in [24], in which Both Alice and Bob have two measurement settings with three outcomes and use the following Bell operator:

$$\begin{aligned}&P(0,0|1,1) - P(0,2|1,1) + P(0,0|1,2) - P(0,2|1,2) - P(1,0|1,1) + P(1,1|1,1) - P(1,0|1,2) + P(1,1|1,2)\\&- P(2,1|1,1) + P(2,2|1,1) - P(2,1|1,2) + P(2,2|1,2) - P(0,0|2,1) + P(0,1|2,1) + P(0,0|2,2) - P(0,2|2,2)\\&- P(1,1|2,1) + P(1,2|2,1) - P(1,0|2,2) + P(1,1|2,2) + P(2,0|2,1) - P(2,2|2,1) - P(2,1|2,2) + P(2,2|2,2).\end{aligned}$$

Using the heuristic method from Sec. II C we obtain the following dimension witness:

$$\begin{aligned}&P(0|1,1) - P(2|1,1) + P(0|1,2) - P(2|1,2) - P(0|2,1) + P(1|2,1) - P(0|2,2) + P(1|2,2)\\&- P(1|3,1) + P(2|3,1) - P(1|3,2) + P(2|3,2) - P(0|4,1) + P(1|4,1) + P(0|4,2) - P(2|4,2)\\&- P(1|5,1) + P(2|5,1) - P(0|5,2) + P(1|5,2) + P(0|6,1) - P(2|6,1) - P(1|6,2) + P(2|6,2). \qquad (15)\end{aligned}$$

Applying the method from Sec. III A, we get the following expression, which may be used in a semidefinite program:

$$\begin{aligned}&P(0,0|1,1) - P(0,2|1,1) + P(0,0|1,2) - P(0,2|1,2) - P(0,0|2,1) + P(0,1|2,1) - P(0,0|2,2) + P(0,1|2,2)\\&- P(0,1|3,1) + P(0,2|3,1) - P(0,1|3,2) + P(0,2|3,2) - P(0,0|4,1) + P(0,1|4,1) + P(0,0|4,2) - P(0,2|4,2)\\&- P(0,1|5,1) + P(0,2|5,1) - P(0,0|5,2) + P(0,1|5,2) + P(0,0|6,1) - P(0,2|6,1) - P(0,1|6,2) + P(0,2|6,2).\end{aligned}$$

The certified randomness for CGLMP is shown in Fig. 1.

### B. $T2$

A simple Bell inequality is obtained from the symmetric dimension witness of the two-to-one quantum random access code (QRAC) used in [13,15]. It has the following form:

$$W'(1,1) + W'(1,2) + W'(2,1) - W'(2,2), \qquad (16)$$

where $W'$ is defined in Eq. (13) and $\delta = 1$. The reduced form of this dimension witness is

$$W(1,1) + W(1,2) + W(2,1) - W(2,2), \qquad (17)$$

where $W$ is defined by Eq. (14) and $\delta = 1$. Robustness of the reduced version has been already investigated in [17], in Fig. 4. The randomness certified by these two dimension witnesses is lower bounded by the values obtained with the following two Bell inequalities. For the dimension witness defined in Eq. (16), we use a Bell inequality:

$$\begin{aligned}&\tfrac{1}{2}[C(1,1) + C(1,2) + C(2,1) - C(2,2)\\&\quad + C(3,1) + C(3,2) + C(4,1) - C(4,2)], \qquad (18)\end{aligned}$$

and for the dimension witness from Eq. (17)

$$T2 \equiv C(1,1) + C(1,2) + C(2,1) - C(2,2). \qquad (19)$$

The operator defined in Eq. (19) is exactly the CHSH Bell operator [25]. Lower bounds for this case are shown in Figs. 2(a), 3(a), 4(a), and 5(a).

The reduced witness (17) has recently been experimentally realized [26]. The values obtained in this experiment refer to $p = 0.974$ (5.51 in the scaling used there) and $p = 0.984$ (5.56), concluded therein to certify 0.0595 and 0.082 bits of randomness, respectively. If the reduction had not been performed, then only 0.0567 and 0.0305 would have been certified.

### C. $T3$

The third example starts with a dimension witness based on the three-to-one quantum random access code (QRAC) [13,27] and relates it, and its reduced version, to two Bell inequalities, where the second one is $T3$ introduced in [28].

In the three-to-one QRAC Alice encodes three bits by sending one of the $2^3$ states to Bob, who tries to guess one of them, performing one of three measurements. The average success probability of correctly guessing an arbitrarily chosen bit is directly related to the value of the following dimension witness:

$$\sum_{x\in\bar{X},\, y\in\bar{Y}} (-1)^{x_y} P(0|x,y), \qquad (20)$$

where $\bar{X} = \{000,\ldots,111\}$, $\bar{Y} = \{0,1,2\}$. Its maximal value attainable with qubits is $4\sqrt{3}$.

Taking $\phi(x) = \neg x$ (negation is meant here as bitwise), $\bar{X} = \{00,01,10,11\}$, and $\bar{Y} = \bar{Y}$, we get the following reduced dimension witness:

$$\begin{aligned}&P(0|00,0) + P(0|01,0) + P(0|10,0) + P(0|11,0)\\&\quad + P(0|00,1) + P(0|00,2) + P(0|01,1) - P(0|01,2)\\&\quad - P(0|10,1) + P(0|10,2) - P(0|11,1) - P(0|11,2). \quad (21)\end{aligned}$$

From this dimension witness, using the method from Sec. III C, we get the following Bell operator:

$$\begin{aligned}&C(1,1)+C(2,1)+C(3,1)+C(4,1)\\&\quad+C(1,2)+C(1,3)+C(2,2)-C(2,3)\\&\quad-C(3,2)+C(3,3)-C(4,2)-C(4,3).\end{aligned}\tag{22}$$

If we do not reduce the dimension witness and use the formula (20) directly, we get the following Bell operator:

$$\begin{aligned}T3'\equiv{}&\tfrac{1}{2}[C(1,1)-C(5,1)+C(2,1)-C(6,1)\\&+C(3,1)-C(7,1)+C(4,1)-C(8,1)\\&+C(1,2)-C(5,2)+C(1,3)-C(5,3)\\&+C(2,2)-C(6,2)-C(2,3)+C(6,3)\\&-C(3,2)+C(7,2)+C(3,3)-C(7,3)\\&-C(4,2)+C(8,2)-C(4,3)+C(8,3)].\end{aligned}\tag{23}$$

The Bell operator defined in Eq. (22) is the one used in [17,19,28].

It is possible to calculate a lower bound on the certified min-entropy, $H_\infty^{\text{cert}}(T3,x_0,y_0,s,d)$, with $x_0=1$, $y_0=1$ using theorem 2, i.e., via a semidefinite relaxation with a minimization on a higher level over $\delta\in[0,1]$.

Figure 2(b) shows the min entropies certified with the Bell inequality $T3$ for different additional conditions. In Fig. 3(b) lower bounds on the certified min-entropy obtained by theorem 1 from the NPA hierarchy with additional condition $P(a,b|x,y)=P(\neg a,\neg b|x,y)$ are plotted. These values assume that the untrusted vendor uses the strategy $P$ (see Sec. III B). Figures 4(b) and 5(b) contain the relevant data for the mixed strategy.

### D. $BC3$

In this example we start with a well known Braunstein-Caves inequality [denoted $BC3$, it is a Bell inequality in the form (3)] with three settings for each of the two parties and convert it to a symmetric dimension witness with six prepared states. After reduction, we will obtain a dimension witness with three states and show that the lower-bounding Bell inequality is identical to the original $BC3$.

$BC3$ inequality is of the form

$$\begin{aligned}BC_3\equiv{}&C(1,1)+C(1,2)+C(2,2)\\&+C(2,3)+C(3,3)-C(3,1),\end{aligned}\tag{24}$$

with $\delta=1$. For $BC_3$ we have $x,y\in\{1,2,3\}$. Thus we obtain a symmetric dimension witness with six states prepared by Alice and three measurements performed by Bob.

The explicit form of this symmetric dimension witness is

$$\begin{aligned}&P(0|(0,1),1)-P(0|(1,1),1)+P(0|(0,1),2)\\&\quad-P(0|(1,1),2)+P(0|(0,2),2)-P(0|(1,2),2)\\&\quad+P(0|(0,2),3)-P(0|(1,2),3)+P(0|(0,3),3)\\&\quad-P(0|(1,3),3)-P(0|(0,3),1)+P(0|(1,3),1).\end{aligned}$$

Using the method for symmetric dimension witnesses from Sec. III C, this may be transformed into a dimension witness with three states. We define $\phi[(a,x)]\equiv(\neg a,x)$ and $\chi\equiv\{(0,x):x\in X\}\subseteq\{0,1\}\times X$.

The explicit form of this reduced dimension witness is

$$\begin{aligned}&2\,[P(0|1,1)+P(0|1,2)+P(0|2,2)\\&\quad+P(0|2,3)+P(0|3,3)-P(0|3,1)]-4.\end{aligned}$$

Now, using theorem 2, we go from this reduced dimension witness back to the Bell inequality that gives a lower-bounding relation. Assuming $P(a,b|x,y)=P(\neg a,\neg b|x,y)$, we get that the lower-bounding Bell inequality is exactly the initial Braunstein-Caves inequality. If we use a full dimension witness, then the Bell inequality used in lower bounding with theorem 2 is

$$\begin{aligned}&\tfrac{1}{2}[C(1,1)+C(1,2)+C(2,2)+C(2,3)\\&\quad+C(3,3)-C(3,1)+C(4,1)+C(4,2)\\&\quad+C(5,2)+C(5,3)+C(6,3)-C(6,1)],\end{aligned}\tag{25}$$

where $(0,1)\equiv1$, $(0,2)\equiv2$, $(0,3)\equiv3$, $(1,1)\equiv4$, $(1,2)\equiv5$, and $(1,3)\equiv6$.

In Fig. 2(c), the min entropies certified with the Bell inequality $BC3$ with different additional conditions are plotted. Figure 3(c) shows lower bounds on the min-entropy certified in this SDI protocol, obtained by theorem 1 from the NPA hierarchy with additional condition $P(a,b|x,y)=P(\neg a,\neg b|x,y)$. These values assume that the untrusted vendor uses the strategy $P$ (see Sec. III B). Plots relevant to the mixed strategy are shown in Figs. 4(c) and 5(c).

### E. modCHSH

In [19] the following Bell operator is investigated:

$$\text{modCHSH}\equiv C(1,2)+C(1,3)+C(2,1)+C(2,2)-C(2,3).\tag{26}$$

This Bell operator is similar in form to the dimension witness introduced in [14]. Since the relevant Bell inequality is very robust in certifying the randomness, the dimension witness with randomness lower bounded by it may also be expected to be robust. Assuming $P(a|x)=\frac{1}{2}$, we turn it into the following dimension witness:

$$W'(1,2)+W'(1,3)+W'(2,1)+W'(2,2)-W'(2,3).\tag{27}$$

Since this dimension witness is symmetric, we follow the steps which lead from the expression (13) to the expression (14), to obtain the following reduced dimension witness:

$$W(1,2)+W(1,3)+W(2,1)+W(2,2)-W(2,3).\tag{28}$$

If we start with the dimension witness defined in Eq. (27), and do not use the symmetry, we get the following lower-bounding Bell inequality:

$$\begin{aligned}&\tfrac{1}{2}[C(1,2)+C(1,3)+C(2,1)+C(2,2)-C(2,3)\\&\quad+C(3,2)+C(3,3)+C(4,1)+C(4,2)-C(4,3)].\end{aligned}\tag{29}$$

The dimension witness from Eq. (27) lower bounds the dimension witness from Eq. (28), and thus both are lower bounded (in the sense of theorem 1 and the conjecture below it) by the Bell inequality from Eq. (29), but only the second dimension witness is proved to be lower bounded by modCHSH [see Eq. (26)]. Lower bounds for this set of DI and SDI protocols are shown in Figs. 2(d), 3(d), 4(d), and 5(d).

## V. CONCLUSIONS

In this paper we explained in more detail the ideas from our previous paper [17]. In particular all steps of the proof of theorem 1 were provided. A tighter bound, using condition $P(a,b|x,y) = P(\neg a,\neg b|x,y)$ in the DI scheme, has been introduced. We have presented a new method of dimension witness reduction, and a clear distinction between reduced and full dimension witnesses has been made. Reduced dimension witnesses have been shown to be able to certify more randomness. Min entropies of several protocols, that had not been considered previously in [17], were evaluated.

Recently a new method that allows us to lower bound the randomness obtained in a SDI scheme directly, using semidefinite programming, has been introduced in [29]. However, the complexity of their algorithm increases significantly with the dimension of Hilbert space, while in our case the same computation provides a bound for all dimensions.

It remains an open question, what are the conditions on a dimension witness under which the adversary has no gain in using the mixed strategy rather than $P$.

## ACKNOWLEDGMENTS

SDP was implemented in OCTAVE using SeDuMi [22] toolbox. This work is supported by a grant of Ministry of Science and Higher Education of the Republic of Poland IDEAS PLUS (IdP2011 000361), National Science Centre (NCN) Grant No. 2013/08/M/ST2/00626, Foundation for Polish Science FNP TEAM, and the National Natural Science Foundation of China (Grant No. 11304397). The major part of this work has been written in the forests of Sopot.

[1] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *Special Publication 800-22 Revision 1a*, National Institute of Standards and Technology, U.S. Department of Commerce, available at http://csrc.nist.gov/publications/PubsSPs.html.

[2] K. Mitnick, *The Art of Intrusion* (Wiley, New York, 2005).

[3] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).

[4] J. S. Bell, Physics **1**, 195 (1964).

[5] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Th. **55**, 4337 (2009).

[6] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbu, *NIST Special Publication 800-63-2*, National Institute of Standards and Technology, U.S. Department of Commerce, available at http://csrc.nist.gov/publications/PubsSPs.html.

[7] R. Colbeck, arXiv:0911.3814.

[8] R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011).

[9] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS '98)* (IEEE Computer Society, Washington, DC, USA 1998), p. 503.

[10] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).

[11] Y.-C. Liang, T. Vertesi, and N. Brunner, Phys. Rev. A **83**, 022108 (2011).

[12] Y.-K. Wang, S.-J. Qin, T.-T. Song, F.-Z. Guo, W. Huang, and H.-J. Zuo, Phys. Rev. A **89**, 032312 (2014).

[13] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Methot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).

[14] R. Gallego, N. Brunner, C. Hadley, and A. Acin, Phys. Rev. Lett. **105**, 230501 (2010).

[15] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).

[16] M. Dall'Arno, E. Passaro, R. Gallego, and A. Acin, Phys. Rev. A **86**, 042312 (2012).

[17] H.-W. Li, P. Mironowicz, M. Pawłowski, Z.-Q. Yin, Y.-C. Wu, S. Wang, W. Chen, H.-G. Hu, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **87**, 020302(R) (2013).

[18] S. L. Braunstein and C. M. Caves, Phys. Rev. Lett. **61**, 662 (1988).

[19] P. Mironowicz and M. Pawłowski, Phys. Rev. A **88**, 032319 (2013).

[20] M. Navascues, S. Pironio, and A. Acin, Phys. Rev. Lett. **98**, 010401 (2007).

[21] M. Navascues, S. Pironio, and A. Acin, New J. Phys. **10**, 073013 (2008).

[22] J. F. Sturm, Optimization Methods and Software **11**, 625 (1999).

[23] J. F. Sturm, Optimization Methods and Software **17**, 6 (2002).

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

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

[26] J. Ahrens, P. Badziag, M. Pawlowski, M. Zukowski, and M. Bourennane, Phys. Rev. Lett. **112**, 140401 (2014).

[27] A. Ambainis, A. Nayak, A. Ta-shma, and U. Vazirani, in *Proceedings of the thirty-first annual ACM symposium on Theory of computing (STOC '99)* (ACM, New York, 1999), pp. 376–383.

[28] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).

[29] M. Navascués, G. de la Torre, and T. Vértesi, Phys. Rev. X **4**, 011011 (2014).