Certifying the Dimension of Classical and Quantum Systems in a Prepare-and-Measure Scenario with Independent Devices

Joseph Bowles,[1] Marco Túlio Quintino,[1] and Nicolas Brunner[1,2]
[1]*Département de Physique Théorique, Université de Genève, 1211 Genève, Switzerland*
[2]*H.H. Wills Physics Laboratory, University of Bristol, Bristol BS8 1TL, United Kingdom*

(Received 11 November 2013; published 11 April 2014)

We consider the problem of testing the dimension of uncharacterized classical and quantum systems in a prepare-and-measure setup. Here we assume the preparation and measurement devices to be independent, thereby making the problem nonconvex. We present a simple method for generating nonlinear dimension witnesses for systems of arbitrary dimension. The simplest of our witnesses is highly robust to technical imperfections, and can certify the use of qubits in the presence of arbitrary noise and arbitrarily low detection efficiency. Finally, we show that this witness can be used to certify the presence of randomness, suggesting applications in quantum information processing.

DOI: 10.1103/PhysRevLett.112.140407 PACS numbers: 03.65.Ta, 03.67.-a

The problem of estimating the dimension of uncharacterized physical systems has recently attracted attention. From a fundamental point of view, this problem is well motivated, as it shows that dimension—the number of (relevant) degrees of freedom—of an unknown system can be determined in a device-independent way. That is, dimension can be tested from measurement data alone, in a scenario in which all devices used in the experiment, including the measurement device, are uncharacterized; i.e., no assumption about the internal working of the devices is needed. Beyond the fundamental interest, this problem is also relevant in the context of quantum information, where the dimension of quantum systems—i.e., the Hilbert space dimension—represents a resource for performing information-theoretic tasks. Specifically, higher dimensional quantum systems can increase the performance of certain protocols, and/or simplify their implementation.

First approaches to this problem considered Bell inequality tests [1–6], random access codes [7], and monitoring of an observable of a dynamic system [8]. More recently, a general formalism was developed to estimate the dimension of classical and quantum systems in a prepare-and-measure setup [9], the simplest but also the most general scenario. Consider two uncharacterized devices, hence described as black boxes (see Fig. 1). The first device prepares upon request a physical system in an unknown state ρ_x. A second device then performs a measurement on the system. The observer tests the devices, by choosing a preparation x and a measurement y, then receiving measurement outcome b. Repeating the experiment many times, the observer obtains the probability distribution $p(b|x,y)$, called here the data. The goal for the observer is then to give a lower bound on the dimension of the unknown set of states $\{\rho_x\}$ from the data alone. This can be achieved using "dimension witnesses" [9–11] (see also Refs. [12,13] for different approaches). These ideas were shown to be relevant experimentally [14,15], and for quantum information processing [16,17].

Here we discuss this problem assuming the preparation and measurement devices to be independent. This assumption is rather natural in a device-independent estimation scenario, where devices are uncharacterized but do not conspire maliciously against the observer. The main difficulty of this problem is that it is nonconvex, a feature that makes generic problems with independent variables hard to tackle. Note that previous works on dimension witnesses allowed the devices to be correlated via shared randomness (hence relaxing the independence assumption), making the problem convex. Although these techniques can in principle be applied in our case, they are far from optimal, as we shall see below.

It is therefore desirable to develop novel methods, which is the goal of this work. Specifically, we present a simple technique for deriving nonlinear dimension witnesses, tailored for device-independent tests of dimension assuming independent devices. We derive witnesses for systems of arbitrary dimension, obtaining a quadratic gap between classical and quantum dimensions. The simplest witness is discussed in detail. We show that it is extremely robust to technical imperfections, and can be used to certify the presence of randomness.

Scenario.—We consider the setup of Fig. 1. The experiment is characterized by the set of conditional probabilities

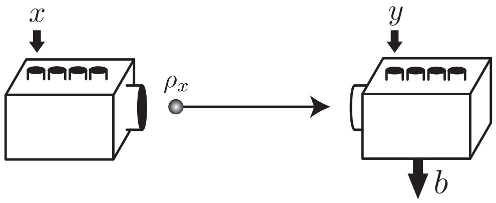

FIG. 1. Prepare-and-measure setup.

$p(b|x,y)$ (i.e., the data) which gives the probability of obtaining outcome b when performing measurement y on preparation x.

Consider first the case of quantum systems. We say that the experiment admits a d-dimensional quantum representation when there exist states ρ_x and measurement operators $M_{b|y}$ both acting on $\mathbb{C}^d$, such that

$$p(b|x,y) = \mathrm{Tr}(\rho_x M_{b|y}). \tag{1}$$

Next consider the situation of classical systems of dimension d. Given the choice of preparation x, the first device sends a classical message $m = 0, \ldots, d-1$. Note that the device may have an internal source of randomness (represented by a random variable λ_1). Hence, which message m is sent depends on both x and λ_1. The measurement device, upon receiving message m, and input y from the observer, delivers an outcome b. As it also features a source of randomness (random variable λ_2), the output b depends on m, y, and λ_2. The behavior observed in the experiment is then given by

$$p(b|x,y) = \int d\lambda_1 d\lambda_2 \rho(\lambda_1,\lambda_2) \sum_{m=0}^{d-1} p(m|x,\lambda_1) p(b|m,y,\lambda_2).$$

The main point now is to consider the joint distribution of random variables $\lambda_{1,2}$. If $\rho(\lambda_1,\lambda_2) \neq \rho_1(\lambda_1)\rho_2(\lambda_2)$, the variables are correlated; hence, the devices may follow a (preestablished) correlated strategy. Previous works focused on this situation. As the set of behaviors of the above form is convex, it can be fully characterized with linear dimension witnesses [9].

Here we consider the situation in which the devices are independent, i.e., $\rho(\lambda_1,\lambda_2) = \rho_1(\lambda_1)\rho_2(\lambda_2)$. That is, although each device features an internal source of randomness, the devices have no shared randomness. In this case, the observed statistics can be written as

$$p(b|x,y) = \sum_{m=0}^{d-1} s(m|x) t(b|m,y) \tag{2}$$

where $s(m|x) = \int d\lambda_1 \rho_1(\lambda_1) p(m|x,\lambda_1)$ is the distribution of possible messages m for each preparation x, and $t(b|m,y) = \int d\lambda_2 \rho_2(\lambda_2) p(b|m,y,\lambda_2)$ is the distribution of outcomes b for measurement y when receiving message m. Below we will see how to characterize the set of behaviors of the form Eq. (2). This will require nonlinear dimension witnesses as the set is nonconvex.

Determinant witness.—In this work we focus on experiments with binary outcomes, denoted $b = 0$, 1. We will construct nonlinear witnesses based on the determinant of a matrix. We first discuss the simplest case, with four preparations $x = 0, \ldots, 3$ and two measurements $y = 0$, 1. Consider the following matrix

$$\mathbf{W}_2 = \begin{pmatrix} p(0,0) - p(1,0) & p(2,0) - p(3,0) \\ p(0,1) - p(1,1) & p(2,1) - p(3,1) \end{pmatrix} \tag{3}$$

where we write $p(x,y) = p(b=0|x,y)$ for simplicity. For any strategy involving a classical bit [i.e., its statistics admits a decomposition of the form Eq. (2) with $d = 2$], one has that

$$W_2 = \det(\mathbf{W}_2) = 0. \tag{4}$$

The proof is straightforward. Note that for any statistics of the form Eq. (2) with $d = 2$, we have that $p(x,y) = s(0|x)[t(0|0,y) - t(0|1,y)] + t(0|1,y)$. Hence we write

$$\begin{aligned} p(x,y) - p(x',y) &= [s(0|x) - s(0|x')][t(0|0,y) - t(0|1,y)] \\ &= S_{xx'} T_y \end{aligned} \tag{5}$$

from which it follows that

$$W_2 = \begin{vmatrix} S_{01}T_0 & S_{23}T_0 \\ S_{01}T_1 & S_{23}T_1 \end{vmatrix} = 0. \tag{6}$$

An interesting feature of the above witness is that it is given by an equality, whereas linear witnesses are given by inequalities [9]. Moreover, our witness turns out to characterize fully the set of experiments involving a classical bit. Specifically, for any experiment achieving $W_2 = 0$ (for all relabelings of the preparation x), there exists a decomposition of the form Eq. (2) with $d = 2$ (see Supplemental Material [18]). Note that if the preparation and measurement devices are correlated, then classical bit strategies can reach $W_2 = 1$. Consider for instance the equal mixture of the two following deterministic strategies: (i) $s(0|x) = 1$ iff $x = 0, 3$ and $t(0|m,y) = m + y \bmod 2$, (ii) $s(0|x) = 1$ iff $x = 0$, 2 and $t(0|m,y) = m$. Hence we get $\mathbf{W}_2 = \mathbb{1}_2$ and $W_2 = 1$. This shows that our witness is tailored for the case in which the devices are independent.

Next we investigate the performance of qubit strategies, i.e., statistics of the form Eq. (1) with $d = 2$. States are given by density matrices $\rho_x = (\mathbb{1}_2 + \vec{s}_x \cdot \vec{\sigma})/2$ and measurement operators by $M_{0|y} = c_y \mathbb{1}_2 + \vec{T}_y \cdot \vec{\sigma}/2$, where $\vec{s}_x$ and $\vec{T}_y$ are Bloch vectors and $|c_y| \leq 1$ [19]. Similarly to above, we write

$$p(x,y) - p(x',y) = \mathrm{Tr}[(\rho_x - \rho_{x'})M_{0|y}] = \vec{S}_{xx'} \cdot \vec{T}_y \tag{7}$$

where $\vec{S}_{xx'} = (\vec{s}_x - \vec{s}_{x'})/2$. Finally, we get

$$W_2 = \begin{vmatrix} \vec{S}_{01} \cdot \vec{T}_0 & \vec{S}_{23} \cdot \vec{T}_0 \\ \vec{S}_{01} \cdot \vec{T}_1 & \vec{S}_{23} \cdot \vec{T}_1 \end{vmatrix} = (\vec{S}_{01} \times \vec{S}_{23}) \cdot (\vec{T}_0 \times \vec{T}_1) \leq 1 \tag{8}$$

since $|\vec{S}_{01} \times \vec{S}_{23}| \leq 1$ and $|\vec{T}_0 \times \vec{T}_1| \leq 1$. This bound for qubit strategies is tight, and can be reached as follows:

choose the preparations to be the pure qubit states given by $\vec{s}_0 = -\vec{s}_1 = \hat{z}$, $\vec{s}_2 = -\vec{s}_3 = \hat{x}$, and the measurements by the vectors $\vec{T}_0 = \cos\theta\hat{z} + \sin\theta\hat{x}$ and $\vec{T}_1 = \sin\theta\hat{z} - \cos\theta\hat{x}$. Notice that we are free to choose any angle θ here, due to the rotational invariance of the cross product in the plane. For $\theta = 0$ we get the usual BB84 states and measurements.

It is relevant to note that essentially any qubit strategy achieves $|W_2| > 0$. Only very specific alignments of the qubit preparations and measurements (a set of measure zero) achieve $W_2 = 0$. Therefore, a generic qubit strategy always outperforms the most general strategy involving a bit.

This suggests that our witness is well suited for distinguishing data involving classical bits and qubits. To illustrate the robustness of our witness, we investigate the effect of technical imperfections, such as background noise and limited detection efficiency (of the detector inside the measurement device), on a generic qubit strategy given by the data $p_Q(x,y)$ achieving $|W_2| = Q > 0$. Say that an error occurs with probability $1-\eta$, for instance the emitted particle is lost. Hence the observed statistics is given by

$$p(x,y) = \eta p_Q(x,y) + (1-\eta)p_N(y), \tag{9}$$

where we consider a noise model of the form $p_N(x,y) = p_N(y)$; i.e., the noise is independent of the choice of preparation x. The difference in probabilities entering the witness is then independent of the noise term: $p(x,y) - p(x',y) = \eta[p_Q(x,y) - p_Q(x',y)]$, and thus the observed value of the witness is $W_2 = \eta^2 Q$, which is strictly positive whenever $Q > 0$. Hence, for an arbitrary amount of background noise and/or an arbitrarily low efficiency, a generic qubit strategy will outperform any classical bit strategy; see Ref. [20] for a related result. This is indeed in stark contrast with previous witnesses, which can only tolerate a finite amount of noise and require a high efficiency [11].

Finally, we comment on strategies involving higher dimensional systems. Using a classical trit one achieves $|W_2| \leq 1$ [21], while numerical analysis shows that $|W_2| \leq 1.299$ for qutrit strategies. This shows that the value of W_2 is useful to assess dimension. To reach the algebraic maximum of $W_2 = 2$, systems of dimension (at least) $d = 4$ (either classical or quantum) are required.

Determinant witness for all dimensions.—We now generalize the above witness for testing classical and quantum systems of arbitrary dimension. Consider a scenario with $2k$ preparations and k binary measurements. Construct the $k \times k$ matrix

$$\mathbf{W}_k(i,j) = p(2j,i) - p(2j+1,i) \tag{10}$$

with $0 \leq i,j \leq k-1$. As above, the witness is given by $W_k = |\det(\mathbf{W}_k)|$. We will see that, for classical systems of dimension d, one has that

$$W_k = 0 \quad \text{for } d \leq k, \tag{11}$$

while one can have $W_k \geq 1$ for $d > k$. For quantum systems of dimension d, we get

$$W_k = 0 \quad \text{for } d \leq \sqrt{k}, \tag{12}$$

while $W_k > 0$ is possible whenever $d > \sqrt{k}$. Hence we obtain a quadratic separation between classical and quantum dimensions, using a number of preparations and measurements that grows only linearly.

To prove the above claims, it is enough to focus on quantum strategies. Consider matrices of the form

$$\rho_x = \frac{1}{d}(\mathbb{1}_d + \phi_d \vec{s}_x \cdot \vec{\lambda}), \tag{13}$$

with $\vec{s}_x \in \mathbb{R}^{d^2-1}$, $|\vec{s}_x| \leq 1$, $\vec{\lambda}$ the vector of the d^2-1 Gell-Mann matrices (generalized Pauli matrices, satisfying $\mathrm{tr}(\lambda_i) = 0$ and $\mathrm{tr}(\lambda_i\lambda_j) = 2\delta_{ij}$) and $\phi_d = \sqrt{[d(d-1)]/2}$. While all matrices of the above form are valid quantum density matrices for $|\vec{s}_x| \leq 2/d$ [22], this is not the case in general (although this will not affect our argument). Similarly we write measurement operators as $M_{0|y} = c_y\mathbb{1}_d + \phi_d\vec{T}_y \cdot \vec{\lambda}/d$ with $\vec{T}_y \in \mathbb{R}^{d^2-1}$, $|\vec{T}_y|$,$|c_y| \leq 1$[19], and get that

$$\mathbf{W}_k(i,j) = \mathrm{Tr}[(\rho_{2j} - \rho_{2j+1})M_{0|i}] = \vec{S}_j \cdot \vec{T}_i \tag{14}$$

with $\vec{S}_j = (1-(1/d))(\vec{s}_{2j} - \vec{s}_{2j+1})$. Thus, as before, the entries of the matrix $\mathbf{W}_k$ are given by scalar products of vectors. Similarly to the qubit construction of Eq. (8), the witness W_k can be expressed using cross products, generalized here to arbitrary dimensions.

Specifically, the cross product $\vec{S}_0 \times \vec{S}_1 \times \cdots \times \vec{S}_{k-1}$ of k vectors in $\mathbb{R}^{k+1}$ is defined as the unique vector $\vec{u} \in \mathbb{R}^{k+1}$ such that $\vec{V} \cdot \vec{u} = \det(\vec{S}_0, \vec{S}_1, \cdots, \vec{S}_{k-1})$ for all $\vec{V} \in \mathbb{R}^{k+1}$ (see, e.g., Ref. [23]). It follows that $\vec{S}_0 \times \cdots \times \vec{S}_{k-1} = 0$ iff $\vec{S}_0, \cdots, \vec{S}_{k-1}$ are linearly dependent. Furthermore, similarly to Eq. (8), we have that

$$\begin{aligned} W_k &= |\det(\mathbf{W}_k)| \\ &= |(\vec{S}_0 \times \cdots \times \vec{S}_{k-1}) \cdot (\vec{T}_0 \times \cdots \times \vec{T}_{k-1})|. \end{aligned}$$

To conclude, we relate the dimension of the quantum systems to the linear (in)dependence of the set of vectors $\vec{S}_j$ and $\vec{T}_i$. Note that we must ensure here that the vectors $\vec{S}_j$, $\vec{T}_i$ are in $\mathbb{R}^{k+1}$, via an embedding or by using only a restricted set of parameters. As d-dimensional quantum systems have d^2-1 parameters, we see that the vectors $\vec{S}_j$ (and similarly for $\vec{T}_i$) can span a subspace of dimension at most d^2-1.

Hence, if $d \leq \sqrt{k}$, the vectors $\vec{S}_j$ cannot be linearly independent, and we get $W_k = 0$. On the contrary if $d > \sqrt{k}$, the vectors $\vec{S}_j$ and $\vec{T}_i$ can be chosen to be linearly independent, and we have $W_k > 0$. Take for instance $\vec{S}_j$ to be parallel to $\vec{T}_i$, and $|\vec{s}_j|$, $|\vec{T}_i| \leq 2/d$ ensuring that all preparations and measurements are represented by valid operators. Note, however, that this construction is suboptimal in general, as one can obtain $W_k = 1$ with quantum states of dimension $d > \sqrt{k}$ (with d an integer prime power), using a mutually unbiased basis (see Supplemental Material [18]).

The proof for classical systems can be derived by noting that any classical strategy using d-dimensional states can be recast as a quantum strategy using diagonal density matrices acting on $\mathbb{C}^d$. Since we have only $d-1$ parameters in this case, it follows from the above that $W_k = 0$ when $d \leq k$. For $d > k$, one can get $W_k \geq 1$. The lower bound is obtained by considering the following strategy: if x is even, then send $m = x/2$, else send $m = d$; for the measurement device, output $b = 0$ iff $y = m$. Note that for this strategy, we get $\mathbf{W}_k = \mathbb{1}_k$, hence $W_k = 1$. An interesting question is to find the algebraic maximum of W_k, and the minimal dimension for classical and quantum systems required to attain it. Note that this problem is related to that of finding the determinant of a Hadamard matrix. Hence we get the bound $W_k \leq k^{k/2}$, which is tight iff there exists a Hadamard matrix of size $k \times k$.

Certifying randomness.—The fact that the determinant witness can distinguish between classical and quantum systems (given a bound on the dimension) suggests applications in randomness certification. Here we investigate the connection between the amount of violation of the witness W_2 and the intrinsic randomness of the of the underlying statistics, assuming that the preparation device emits qubit states.

Consider the quantity

$$\bar{p} = \frac{1}{4} \sum_{x,y=0,1} \max_b p(b|x,y), \tag{15}$$

i.e., the average guessing probability of the outcome b for preparations $x = 0$, 1. Randomness can be quantified by the min-entropy of $\bar{p}$, i.e., $H_{\min}(\bar{p}) = -\log_2(\bar{p})$, which gives the number of random bits extractable from the experiment (per run). Now for a given amount of violation of the witness $W_2 = Q > 0$, we want to find out the maximal value of $\bar{p}$ over all qubit strategies which are compatible with the value $W_2 = Q > 0$. In other words, what is the minimal amount of randomness compatible with a certain violation of the witness? To answer this question, we solve numerically the following problem. We maximize $\bar{p}$ subject to the constraints: $W_2 = Q$, $p(b|x,y) = \mathrm{Tr}(\rho_x M_{b|y})$ where ρ_x, $M_{b|y}$ are arbitrary qubit states and measurement operators.

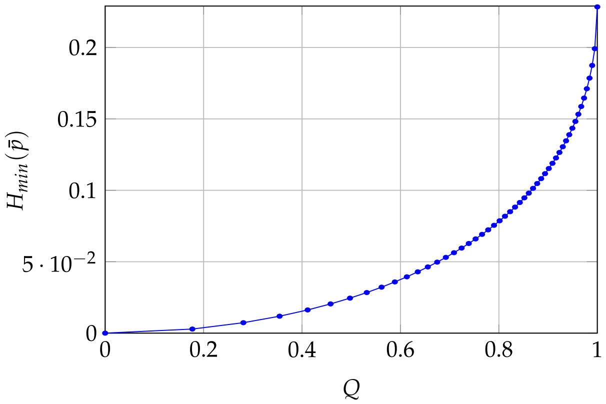

FIG. 2 (color online). Average certifiable randomness $H_{\min}(\bar{p})$ using the witness W_2. For any amount of violation of the witness $W_2 = Q > 0$, randomness can be certified.

In Figure 2, we plot the amount of randomness $H_{\min}(\bar{p})$ as a function of the value Q of the witness W_2. We see that for any amount of violation, randomness can be certified. In other words, from the sole knowledge of the value of W_2, one can upper bound the probability of correctly guessing the output b, for any observer knowing the detailed qubit strategy that is being used. Importantly, the quantity $H_{\min}(\bar{p})$ captures here the intrinsic quantum randomness of the experiment, but is independent of any randomness generated locally in the devices (used, e.g., to create mixed state preparations). These issues will be discussed in detail in a forthcoming work [24], where a protocol for randomness certification will be presented.

Discussion.—We have presented a method for testing the dimension of classical and quantum systems of arbitrary dimension. Moreover, the simplest of our witnesses is highly robust to noise and can be used to certify randomness without the need of high visibilities and efficiencies. Hence we believe these ideas are relevant in practice. In this perspective, it will be necessary to make a statistical analysis in the spirit of Refs. [25] for taking finite size effects into account [24]. Finally, from a more abstract point of view, the ideas presented here could be useful in other nonconvex problems involving independent variables, such as Bell tests with independent sources [26,27], and more general marginal problems [28].

We thank J. B. Brask, Ci Wen Lim, M. Pawłowski, S. Pironio, E. Woodhead, and H. Zbinden for discussions, and acknowledge financial support from the Swiss National Science Foundation (Grant No. PP00P2_138917) and the EU DIQIP.

[1] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, Phys. Rev. Lett. 100, 210503 (2008).
[2] K. F. Pál and T. Vértesi, Phys. Rev. A 77, 042105 (2008).

[3] D. Pérez-García, M. M. Wolf, C. Palazuelos, I. Villanueva, and M. Junge, Commun. Math. Phys. **279**, 455 (2008).

[4] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Phys. Rev. Lett. **111**, 030501 (2013).

[5] C. Eltschka and J. Siewert, Phys. Rev. Lett. **111**, 100503 (2013).

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

[7] S. Wehner, M. Christandl, and A. C. Doherty, Phys. Rev. A **78**, 062112 (2008).

[8] M. M. Wolf and D. Pérez-García, Phys. Rev. Lett. **102**, 190504 (2009).

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

[10] N. Brunner, M. Navascués, and T. Vértesi, Phys. Rev. Lett. **110**, 150501 (2013).

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

[12] C. Stark, arXiv:1209.5737.

[13] N. Harrigan, T. Rudolph, and S. Aaronson, arXiv:0709.1149.

[14] M. Hendrych, R. Gallego, M. Micuda, N. Brunner, A. Acín, and J. Torres, Nat. Phys. **8**, 588 (2012).

[15] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Nat. Phys. **8**, 592 (2012).

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

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

[18] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.112.140407 for tightness of witness W_2; quantum strategy with MUBs.

[19] Note that not all matrices with $|c_y| \leq 1$ are valid measurement operators since c_y is in general dependant $\vec{T}_y$.

[20] M. Dall'Arno, E. Passaro, R. Gallego, M. Pawlowski, and A. Acin, arXiv:1210.1272.

[21] Although qubits and classical trits perform equally for the witness W_2, qubits are able to outperform trits for W_3 (defined later).

[22] G. Kimura, Phys. Lett. A **314**, 339 (2003)

[23] A. Dittmer, Am. Math. Mon. **101**, 887 (1994).

[24] J. Bowles *et al.* (to be published).

[25] R. Gill, arXiv:1207.5103; Y. Zhang, S. Glancy, and E. Knill, Phys. Rev. A **88**, 052119 (2013).

[26] C. Branciard, N. Gisin, and S. Pironio, Phys. Rev. Lett. **104**, 170401 (2010).

[27] T. Fritz, New J. Phys. **14**, 103001 (2012).

[28] J. Pearl, *Models, Reasoning and Inference* (Cambridge University Press, Cambridge, England, 2000).