# Minimum Dimension of a Hilbert Space Needed to Generate a Quantum Correlation

Jamie Sikora,[1,2] Antonios Varvitsiotis,[1,2,3] and Zhaohui Wei[1,2,3,*]
[1]*Centre for Quantum Technologies, National University of Singapore, Singapore 117543*
[2]*MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, Singapore UMI 3654*
[3]*School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371*
(Received 6 October 2015; revised manuscript received 14 March 2016; published 4 August 2016)

Consider a two-party correlation that can be generated by performing local measurements on a bipartite quantum system. A question of fundamental importance is to understand how many resources, which we quantify by the dimension of the underlying quantum system, are needed to reproduce this correlation. In this Letter, we identify an easy-to-compute lower bound on the smallest Hilbert space dimension needed to generate a given two-party quantum correlation. We show that our bound is tight on many well-known correlations and discuss how it can rule out correlations of having a finite-dimensional quantum representation. We show that our bound is multiplicative under product correlations and also that it can witness the nonconvexity of certain restricted-dimensional quantum correlations.

DOI: 10.1103/PhysRevLett.117.060401

In what ranks as one of the most important achievements of modern physics, it was shown by John Bell in 1964 that some correlations generated within the framework of quantum mechanics can be *nonlocal*, in the sense that the statistics generated by quantum mechanics cannot always be reproduced by a local hidden-variable model [1,2]. Over the last 40 years, there have been significant efforts in trying to verify this fact experimentally. The first such experimental data [3] were published in 1972, and this remains an active area of research [4]. Moreover, as a central concept in quantum physics and quantum information theory, fully understanding quantum entanglement and nonlocality still remains a very interesting and important problem with far-reaching applications. Indeed, profound relationships between quantum nonlocality and other fundamental quantum concepts or phenomena such as entanglement measures [5,6], entanglement distillation [7,8], and teleportation [9] have been identified. Meanwhile, for many tasks, e.g., in cryptography [10,11], it has been realized that due to quantum nonlocality, quantum strategies enjoy remarkable advantages over their classical counterparts.

However, even though quantum nonlocal effects can lead to interesting and often surprising advantages in some applications, this does not paint the full picture. After all, for practical applications, it is just as important to understand the amount of quantum resources required for these advantages to manifest. For instance, if there is an exponential blowup in the amount of resources required, then whatever advantage gained by employing quantum mechanics may not be useful in practice. Quantifying the amount of quantum resources needed to perform a certain task is the central focus of this Letter.

We study quantum nonlocality from the viewpoint of two-party quantum correlations that arise from a Bell experiment. A two-party Bell experiment is performed between two parties, Alice and Bob, whose labs are set up in separate locations. Alice (respectively, Bob) has in her possession a measurement apparatus whose possible settings are labeled by the elements of a finite set $X$ (respectively, $Y$), and the possible measurement outcomes are labeled by a finite set $A$ (respectively, $B$). After repeating the experiment many times, Alice and Bob calculate the joint conditional probabilities $p(ab|xy)$, i.e., the probability that upon selecting measurement settings $(x,y) \in X \times Y$, they get outcomes $(a,b) \in A \times B$. The collection of all joint conditional probabilities is arranged in a vector $p = [p(ab|xy)]$ of length $|A \times B \times X \times Y|$, which we call a correlation.

Given a Bell experiment as described above, a natural problem is to characterize the correlations that can arise with respect to various physical models. The set of correlations generated by a local hidden-variable model forms a convex polytope, and its elements are called local correlations. A correlation $p = [p(ab|xy)]$ is called quantum if it can be generated by performing local measurements on a shared quantum system which is prepared in a state independent of the measurement choices. Formally, $p = [p(ab|xy)]$ is quantum if there exists a quantum state $\rho$ acting on the Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$ and local positive-operator valued measures (POVMs) $\{M_{xa} : a \in A\}$ and $\{N_{yb} : b \in B\}$ each acting on $\mathbb{C}^d$ such that

$$p(ab|xy) = \mathrm{Tr}[(M_{xa} \otimes N_{yb})\rho]. \quad (1)$$

For a correlation of the form (1), we say that $p$ admits a $d$-dimensional representation. Furthermore, we denote by $\mathcal{D}(p)$ the minimum integer $d \geq 1$ for which the correlation $p$ admits a $d$-dimensional representation. Note that the case $\mathcal{D}(p) = 1$ corresponds to local correlations where Alice and Bob only use private randomness.

 

As we only consider finite-dimensional Hilbert spaces, we can replace the tensor product structure with commutation relations and obtain an equivalent definition [12].

Considering the central role that quantum correlations play in many applications and the fact that Hilbert space dimension is a valuable resource, a natural and fundamental problem is as follows: Given a quantum correlation $p = [p(ab|xy)]$, what is the smallest dimension of a quantum system needed to generate $p$; i.e., what is $\mathcal{D}(p)$?

This problem is nondeterministic polynomial time (NP) hard to solve exactly in general [13], and limited progress has been reported; see Ref. [12] for a summary of results. One of the most successful approaches employs the notion of dimension witnesses [14] (see also Refs. [15–17]). Furthermore, the framework of dimension witnesses has been also used to derive dimension lower bounds in the prepare-and-measure scenario [18].

In the setting of Ref. [14], a $d$-dimensional representation of a correlation $p = [p(ab|xy)]$ is defined as a convex combination of correlations of the form (1). Operationally, this means that the preparations of the quantum states and the POVMs depend on the value of a public random variable, which they consider to be a free resource.

The assumption of free public randomness implies that the set of correlations admitting a $d$-dimensional representation, denoted by $\mathcal{Q}_d$, is convex. A $d$-dimensional witness is defined as a hyperplane $H$ that contains $\mathcal{Q}_d$ in one of its half-spaces. Consequently, for any correlation $p$ that lies strictly in the opposite half-space, $H$ witnesses that $p \notin \mathcal{Q}_d$. Note that since $\mathcal{Q}_d$ is convex, such a hyperplane exists for any $p \notin \mathcal{Q}_d$. On the negative side, finding such a hyperplane (for a given correlation and a fixed $d \geq 1$) is a challenging task.

On the other hand, if public randomness is not a free resource, i.e., it must be embedded into the entangled state $|\psi\rangle$, the set of quantum correlations admitting a $d$-dimensional representation [as defined in (1)] is not always convex [19]. The lack of convexity in this setting suggests that the problem of lower bounding the size of the quantum system needed to generate a correlation is more complicated. In particular, the approach of using separating hyperplanes is no longer applicable. Nevertheless, this is a realistic and interesting setting, e.g., when public randomness is not available, or when we need to compare the resources required by a classical scheme and those by a pure quantum scheme to generate a given correlation.

In this Letter, for the case that public randomness is not a free resource, we give an easy-to-compute lower bound on $\mathcal{D}(p)$ which only depends on the values of the joint conditional probabilities $p(ab|xy)$. To derive the bound, we use an approach that combines a novel geometric characterization for the set of quantum correlations given in Ref. [20] with techniques that were recently introduced to lower bound the positive semidefinite rank [see (19) for a definition] of an entrywise non-negative matrix [21], a fundamental quantity in both mathematical optimization and quantum communication theory [22,23]. We then apply our lower bound to show that it is tight on many well-known correlations. Afterwards, we also detail various other applications.

*Deriving our lower bound.*—The first ingredient in proving our lower bound on the Hilbert space dimension relies on the fact that, without loss of generality, we can assume Alice and Bob share a pure state on the Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$. To argue this, suppose $p = [p(ab|xy)]$ is generated by a mixed state $\rho$ acting on $\mathbb{C}^d \otimes \mathbb{C}^d$. Consider its purification $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathcal{Z}$, then look at its Schmidt decomposition $|\psi\rangle \coloneqq \sum_{i=1}^d \lambda_i |a_i\rangle_{\mathbb{C}^d} |b_i\rangle_{\mathbb{C}^d \otimes \mathcal{Z}}$, where we allow $\lambda_i = 0$ in the Schmidt decomposition for convenience. Note that since the first subsystem is $d$ dimensional, we have $d$ terms in the Schmidt decomposition. Consider the maps $U \coloneqq \sum_{j=1}^d |j\rangle\langle a_j|$ and $V \coloneqq \sum_{j=1}^d |j\rangle\langle b_j|$ and define the pure quantum state $|\psi'\rangle \coloneqq (U \otimes V)|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$, returning to the original Hilbert spaces. By adjusting the measurement operators using $U$ and $V$, we can construct a $d$-dimensional representation for $p$ using the pure state $|\psi'\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$. A similar proof shows that Alice and Bob's quantum systems can be of the same dimension (being the minimum dimension of the original two systems).

The second ingredient in proving our lower bound is a recent characterization for the correlations that admit a $d$-dimensional representation with a pure quantum state. Specifically, it was shown in Ref. [20] that a correlation $p = [p(ab|xy)]$ is generated by a pure quantum state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ if and only if there exist $d \times d$ Hermitian positive semidefinite matrices $\{E_{xa} : a \in A, x \in X\}$ and $\{F_{yb} : b \in B, y \in Y\}$ satisfying the following conditions:

$$p(ab|xy) = \mathrm{Tr}(E_{xa} F_{yb}) \quad \text{for all } a, b, x, y, \tag{2}$$

$$\sum_{a \in A} E_{xa} = \sum_{b \in B} F_{yb} \quad \text{for all } x, y. \tag{3}$$

Combining this with the fact that we can assume that a correlation is generated by a pure state, we have that for a quantum correlation $p = [p(ab|xy)]$, $\mathcal{D}(p)$ is equal to the smallest integer $d \geq 1$ for which there exist $d \times d$ Hermitian positive semidefinite matrices $\{E_{xa} : a \in A, x \in X\}$ and $\{F_{yb} : b \in B, y \in Y\}$ satisfying (2) and (3).

We now have all the necessary ingredients to derive our lower bound on $\mathcal{D}(p)$. For the remainder of this section, fix a correlation $p = [p(ab|xy)]$, set $d \coloneqq \mathcal{D}(p)$, and let $\{E_{xa} : a \in A, x \in X\}$ and $\{F_{yb} : b \in B, y \in Y\}$ be two families of $d \times d$ matrices satisfying (2) and (3). Notice that $\sum_a E_{xa}$ has full rank for any $x$ [otherwise, by restricting on its support, we can construct a new family of matrices of size strictly less than $d$ satisfying (2) and (3), which contradicts the minimality of $d$]. We first create a family of POVMs by defining the invertible matrix $U$ such that

$U(\sum_a E_{xa})U^\dagger = I_d$. Thus, $\{E'_{xa} := UE_{xa}U^\dagger : a \in A\}$ is a POVM for any choice of $x$. Notice we can write

$$p(ab|xy) = f_{yb}\mathrm{Tr}(E'_{xa}F'_{yb}), \tag{4}$$

for all $a$, $b$, $x$, $y$, where $F'_{yb} := (U^{-1})^\dagger F_{yb}U^{-1}/f_{yb}$ and $f_{yb}$ is the normalizing factor so that $F'_{yb}$ is a quantum state. Notice now that $p(ab|xy)/f_{yb}$ is the probability of outcome $a$ when $F'_{yb}$ is measured with the POVM $\{E'_{xa} : a \in A\}$ when $f_{yb} > 0$. Recall that the fidelity between two quantum states $\rho$ and $\sigma$ is defined as $\mathbf{F}(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$. Note that the fidelity can only increase after a measurement [24]; thus, we have

$$\mathbf{F}(F'_{y_1b_1}, F'_{y_2b_2}) \le \sum_a \sqrt{\frac{p(ab_1|xy_1)}{f_{y_1b_1}}}\sqrt{\frac{p(ab_2|xy_2)}{f_{y_2b_2}}} \tag{5}$$

for all $x$. Furthermore, we have that $\mathrm{Tr}(\rho\sigma) \le \mathbf{F}(\rho,\sigma)^2$, implying

$$\mathrm{Tr}(F'_{y_1b_1}F'_{y_2b_2}) \le \mathbf{F}(F'_{y_1b_1}, F'_{y_2b_2})^2. \tag{6}$$

Since $p(ab|xy)$ is a probability distribution for all $x$, $y$, it follows from (4) that $\sum_b f_{yb} = 1$ for all $y$. We now define the mixed state $\rho_y := \sum_b f_{yb}F'_{yb}$ for all $y$. Since $\sum_b F_{yb}$ is independent of $y$ from (3), we have that

$$\rho_{y_1} = \rho_{y_2}, \quad \text{for all } y_1, y_2. \tag{7}$$

Since $\rho_y$ is a mixed quantum state over $\mathbb{C}^d$, we have that

$$\mathrm{Tr}(\rho_y^2) \ge \frac{1}{d}, \quad \text{for all } y. \tag{8}$$

Combining Eqs. (5)–(8), it follows that $d$ is lower bounded by

$$\max_{y_1,y_2}\left[\sum\nolimits_{b_1,b_2}\min_x\left(\sum\nolimits_a \sqrt{p(ab_1|xy_1)}\sqrt{p(ab_2|xy_2)}\right)^2\right]^{-1}. \tag{9}$$

Note that we could have transformed the matrices $F_{yb}$ into the measurements instead of the matrices $E_{xa}$. Repeating the above analysis in this case, we arrive at

$$\max_{x_1,x_2}\left[\sum\nolimits_{a_1,a_2}\min_y\left(\sum\nolimits_b \sqrt{p(a_1b|x_1y)}\sqrt{p(a_2b|x_2y)}\right)^2\right]^{-1} \tag{10}$$

as another lower bound on $\mathcal{D}(p)$. We collect these two lower bounds on $\mathcal{D}(p)$ in the main theorem of this Letter, below.

**Theorem:** For any quantum correlation $p$, we have that

$$\mathcal{D}(p) \ge \lceil \max\{f_1(p), f_2(p)\}\rceil, \tag{11}$$

where $f_1(p)$ and $f_2(p)$ denote the expressions given in (9) and (10), respectively, and $\lceil a\rceil$ is the least integer $t$ such that $t \ge a$.

*Applications.*—In the rest of this Letter, we illustrate the usefulness of our lower bound for various applications.

*Several well-known correlations.*—We start by showing that the lower bound can be tight. Let $A = B = X = Y = \{0,1\}$, and consider the quantum correlation given by

$$p(ab|xy) = \begin{cases} (2+\sqrt{2})/8 & \text{if} \quad a \oplus b = xy \\ (2-\sqrt{2})/8 & \text{if} \quad a \oplus b \ne xy, \end{cases} \tag{12}$$

where $\oplus$ denotes the logical exclusive OR of two bits. This correlation corresponds to the optimal strategy for the Clauser-Horne-Shimony-Holt game [25], which can be generated using the quantum state $1/\sqrt{2}(|00\rangle + |11\rangle) \in \mathbb{C}^2 \otimes \mathbb{C}^2$. Applying our lower bound to the above correlation, we obtain $f_1(p) = 2$, which is tight.

We next consider a correlation in the setting $X = Y = \{1,2,3\}$, $A = B = \{0,1\}^3$ generated using the state $\frac{1}{2}(|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle) \in \mathbb{C}^4 \otimes \mathbb{C}^4$ given by

$$p(ab|xy) = \begin{cases} 1/8 & \text{if } a_y = b_x, a \text{ has even parity,} \\ & \text{and } b \text{ has odd parity} \\ 0 & \text{otherwise.} \end{cases} \tag{13}$$

This correlation is optimal for the magic square game [26–28]. Using (9), we can easily show that $f_1(p) = 4$, which is again tight.

In addition to the above examples of extremal correlations, we would now like to discuss some examples which are nonextremal. We now discuss correlations in connection to a Bell inequality [Eq. (5) in Ref. [14]], where $|X| = |B| = 2$ and $|A| = |Y| = 3$. It was shown in Ref. [14] that the maximal violations require a two-qutrit state to achieve. By trying our lower bound on some near maximally violating correlations (found numerically), we find that our lower bound yields $2 \pm \epsilon$ for small $\epsilon > 0$. Thus, after rounding up, it sometimes gives a tight result. Interestingly, there are some nonlocal correlations which do not violate the Bell inequality, but our lower bound is strictly greater than 2, yielding a tight bound once rounded up. This illustrates the fact that our bound is independent of any Bell inequalities and complements the approach of dimension witness.

As a last example, we study the I3322 Bell inequality [29]. The maximal value of I3322 is 0.25 when restricted to using qubit states, and numerical evidence shows that the maximal violation requires infinite-dimensional Hilbert spaces [30]. When evaluating our lower bound on some correlations with I3322 value greater than 0.25, we get values between 1 and 2, which is not tight. Indeed, as the correlations approach the maximum I3322 value, the probabilities in the numerical simulations are bounded away from 0, and thus our lower bound does not grow large.

*Witnessing the nonconvexity of restricted-dimensional quantum correlations.*—It is known that the extreme points of the set of quantum correlations in the $|X| = |Y| = |A| = |B| = 2$ setting can be generated using a two-qubit state [31]. It has been shown numerically that some correlations in this setting require at least a two-qutrit state to generate [19], thus implying that the set $D_2 \coloneqq \{p\colon \mathcal{D}(p) \le 2\}$ is not convex. Using our lower bound, we can give an analytical proof of this fact. Consider the following three deterministic correlations in $D_2$:

$$p_1(ab|xy) = 1 \quad \text{if } (a = 1 \quad \text{and} \quad b = 1); \quad 0 \text{ otherwise},$$
$$p_2(ab|xy) = 1 \quad \text{if } (a = 0 \quad \text{and} \quad b = 0); \quad 0 \text{ otherwise},$$
$$p_3(ab|xy) = 1 \quad \text{if } (a \neq x \quad \text{and} \quad b \neq y); \quad 0 \text{ otherwise}.$$

Setting $p = \frac{1}{3}p_1 + \frac{1}{3}p_2 + \frac{1}{3}p_3$, we have that $f_1(p) = 9/4 > 2$. Thus, $p \notin D_2$, witnessing the nonconvexity of $D_2$.

*Witnessing nonquantumness.*—We now consider a generalization of the Popescu-Rohrlich box [32,33] in the setting $X = Y = \{0,1\}$, $A = B = \{0, 1, \ldots, d-1\}$ given by

$$p(ab|xy) = \begin{cases} 1/d & \text{if} \quad xy = (b-a) \mod d \\ 0 & \text{if} \quad xy \neq (b-a) \mod d. \end{cases} \tag{14}$$

A sufficient condition was derived in Ref. [34], which witnesses that $p$ is not quantum (see also Ref. [35]). We can readily verify that $f_1(p) = +\infty$, yielding an alternative proof that it has no finite-dimensional quantum representation.

We proceed to show that a second family of correlations is not finite-dimensional quantum. In particular, in the setting $X = Y = A = B = \{0,1\}$, consider any correlation $p$ which satisfies

$$p(ab|xy) = 0 \quad \text{if } (x \vee a = y \vee b) \tag{15}$$

when $(x, y) \neq (1, 1)$, where $\vee$ denotes the logical OR of two bits. Such correlations correspond to perfect strategies for the Fortnow-Feige-Lovász game [36,37]. It follows from the computation of the entangled value of this game [38] that such a quantum correlation cannot exist. By examining the pattern of 0s in the correlation, we can apply the same argument as before to conclude that there is no finite-dimensional quantum representation of $p$.

*Multiplicity of the lower bound under product correlations.*—For $i \in \{1, \ldots, k\}$, consider quantum correlations $p_i$, on the settings $X_i$, $Y_i$, $A_i$, and $B_i$, respectively. Define the product correlation $p_{1,\ldots,k}$ on $X = \times_{i=1}^k X_i$, $Y = \times_{i=1}^k Y_i$, $A = \times_{i=1}^k A_i$, and $B = \times_{i=1}^k B_i$, given by

$$p_{1,\ldots,k}(ab|xy) \coloneqq \Pi_{i=1}^k p_i(a_i b_i | x_i y_i). \tag{16}$$

Clearly, since we can generate $p$ using $k$ separated subsystems, we have $\mathcal{D}(p_{1,\ldots,k}) \le \Pi_{i=1}^k \mathcal{D}(p_i)$. We now identify a sufficient condition for this to hold with equality.

It is straightforward to verify that $f_1$, defined in (9), multiplies under product correlations, i.e.,

$$f_1(p_{1,\ldots,k}) = \Pi_{i=1}^k f_1(p_i). \tag{17}$$

Thus, if $f_1(p_i) = \mathcal{D}(p_i)$ for all $i \in \{1, \ldots, k\}$, we get that

$$\mathcal{D}(p_{1,\ldots,k}) = \Pi_{i=1}^k \mathcal{D}(p_i). \tag{18}$$

Clearly, the same argument holds if we replace $f_1$ by $f_2$.

For a concrete example, let $p_1$ and $p_2$ be the correlations given in (12) and (13), respectively, and define $p_{1,2}$ to be the corresponding product correlation. Following the discussion above, to generate the correlation $p_{1,2}$, one would need a Hilbert space of (local) dimension eight, and there is no way to save on resources in this case. Note that using this idea, we can construct quantum correlations with various input and output sizes on which our lower bound is tight.

Also, if it happens to be the case that our lower bound witnesses that $p_i$ is not finite-dimensional quantum for some $i \in \{1, \ldots, k\}$, e.g., if $p_i$ is the example (14) for some $d \ge 1$, then $p_{1,\ldots,k}$ cannot be finite-dimensional quantum either.

*Relation to positive semidefinite rank (PSD rank).*—As our last example, we show that our lower bound on Hilbert space dimension has a close relationship with lower bounds for the PSD rank. The PSD rank of an entrywise nonnegative $n \times m$ matrix $X$ is the smallest integer $c \ge 1$ such that there exist $c \times c$ positive semidefinite matrices $A_1, \ldots, A_n$, $B_1, \ldots, B_m$ satisfying

$$X_{i,j} = \mathrm{Tr}(A_i B_j) \quad \text{for all } i, j. \tag{19}$$

Note the resemblance of (19) to condition (2). Now consider a Bell scenario where $|X| = |Y| = 1$; i.e., Alice and Bob each have only one choice of measurement. In this setting, we have that any correlation $p = [p(ab)]$ is quantum and $\mathcal{D}(p)$ is known as the quantum correlation complexity of $p$ [39]. In Ref. [40], it is shown that in this special case, $\mathcal{D}(p)$ is equal to the PSD rank of the corresponding correlation matrix $\sum_{a,b} p(ab)|a\rangle\langle b|$, where the vectors are in the computational basis. Thus, our lower bound specialized to the case $|X| = |Y| = 1$ becomes a lower bound for PSD rank itself, which was first given in Ref. [21]. We point out that lower bounding the PSD rank is an important task in mathematical optimization and quantum communication complexity theory [41].

For general Bell scenarios, we note that the PSD rank of the matrix $\sum_{a,b,x,y} p(ab|xy)|xa\rangle\langle yb|$ is a lower bound on $\mathcal{D}(p)$; thus, the lower bounds for the PSD rank can also be used to lower bound $\mathcal{D}(p)$. As an example, we consider the correlation given in (13). When viewed as a lower bound on $\mathcal{D}(p)$, the lower bound on the PSD rank from Ref. [21] is equal to 2, while our lower bound (11) gives 4.

*Conclusions.*—In this work, we derived a tractable lower bound for the minimum dimension of a Hilbert space needed to generate a given two-party quantum correlation and gave a variety of applications. Since quantum correlations constitute a fundamental concept in quantum physics and Hilbert space dimension is regarded as an expensive and valuable resource, we hope our results will provide new insights for studying quantum correlations and prove to be useful for their applications. As an example, our lower bound has the feature that it is composed of very simple functions of the probabilities $[p(ab|xy)]$. This is very useful for analyzing the effect of perturbations or uncertainty in the correlation data. Suppose two experimentalists create their estimate $p'$ for the actual value of the correlation $p$. Then, they can use the lower bounds (9) and (10) to get an estimate for the actual dimensions of their quantum systems, if they know that for all $a$, $b$, $x$, $y$, they have $|p(ab|xy) - p'(ab|xy)| \leq \epsilon$, for some small positive constant $\epsilon$. In other words, there is some threshold for the number of experiments needed such that the two parties are fairly confident that the dimensions of their quantum systems is at least one fewer than the value given by our lower bounds when applied to their experimental data. Thus, our bound is quite robust against experimental uncertainty.

We thank Carlos A. Pérez-Delgado, Sixia Yu, and Elie Wolfe for helpful discussions, and Károly F. Pál and Tamás Vértesi for sending us numerical data. J. S. is supported in part by NSERC Canada. A. V. and Z. W. are supported in part by the Singapore National Research Foundation under NRF RF Grant No. NRF-NRFF2013-13. Research at the Centre for Quantum Technologies is partially funded through the Tier 3 Grant “Random numbers from quantum processes” (MOE2012-T3-1-009).

*zhwei@ntu.edu.sg

[1] J. S. Bell, Physics **1**, 195 (1964).
[2] J. S. Bell, Rev. Mod. Phys. **38**, 447 (1966).
[3] S. Freedman and J. Clauser, Phys. Rev. Lett. **28**, 938 (1972).
[4] B. Hensen *et al.*, Nature (London) **526**, 682 (2015).
[5] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[6] A. Acín, T. Durt, N. Gisin, and J. I. Latorre, Phys. Rev. A **65**, 052325 (2002).
[7] A. Salles, D. Cavalcanti, and A. Acín, Phys. Rev. Lett. **101**, 040404 (2008).
[8] A. Acín, Phys. Rev. Lett. **88**, 027901 (2001).
[9] D. Cavalcanti, A. Acin, N. Brunner, and T. Vertesi, Phys. Rev. A **87**, 042104 (2013).
[10] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[11] J. Sikora, A. Chailloux, and I. Kerenidis, Phys. Rev. A **89**, 022334 (2014).
[12] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[13] C. Stark, arXiv:1510.02800.
[14] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Methot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).
[15] K. F. Pál and T. Vértesi, Phys. Rev. A **77**, 042105 (2008).
[16] S. Wehner, M. Christandl, and A. C. Doherty, Phys. Rev. A **78**, 062112 (2008).
[17] J. Briët, H. Buhrman, and B. Toner, Commun. Math. Phys. **305**, 827 (2011).
[18] R. Gallego, N. Brunner, C. Hadley, and A. Acin, Phys. Rev. Lett. **105**, 230501 (2010).
[19] J. M. Donohue and E. Wolfe, Phys. Rev. A **92**, 062120 (2015).
[20] J. Sikora and A. Varvitsiotis, arXiv:1506.07297 [Math. Program. (to be published)].
[21] T. Lee, Z. Wei, and R. de Wolf, arXiv:1407.4308 [Math. Program. (to be published)].
[22] S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary, and R. De Wolf, J. Assoc. Comput. Mach. **62**, 95 (2015).
[23] J. Gouveia, P. Parrilo, and R. Thomas, Math. Oper. Res. **38**, 248 (2013).
[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[25] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[26] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
[27] A. Peres, Phys. Lett. A **151**, 107 (1990).
[28] P. K. Aravind, Found. Phys. Lett. **15**, 397 (2002).
[29] M. Froissart, Nuovo Cimento Soc. Ital. Fis. **64B**, 241 (1981).
[30] K. F. Pál and T. Vértesi, Phys. Rev. A **82**, 022116 (2010).
[31] L. Masanes, Phys. Rev. Lett. **97**, 050503 (2006).
[32] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[33] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).
[34] J. I. de Vicente, Phys. Rev. A **92**, 032103 (2015).
[35] R. Ramanathan, J. Tuziemski, M. Horodecki, and P. Horodecki, Phys. Rev. Lett. **117**, 050401 (2016).
[36] U. Feige and L. Lovász, in Proceedings of the 24th ACM STOC, p. 733.
[37] L. Fortnow, PhD thesis, Massachusetts Institute of Technology [Technical Report No. MIT/LCS/TR-447, 1989 (unpublished)].
[38] J. Watrous (unpublished).
[39] S. Zhang, in Proceedings of the 3rd Innovations in Theoretical Computer Science, p. 39.
[40] R. Jain, Y. Shi, Z. Wei, and S. Zhang, IEEE Trans. Inf. Theory **59**, 5171 (2013).
[41] J. Lee, D. Steurer, and P. Raghavendra, in Proceedings of the 47th ACM STOC, p. 567.