Generalization of the Clauser-Horne-Shimony-Holt inequality self-testing maximally entangled states of any local dimension

Andrea Coladangelo*
Computing and Mathematical Sciences, Caltech, Pasadena, California 91125, USA

(Received 27 June 2018; published 13 November 2018)

The Clauser-Horne-Shimony-Holt inequality (CHSH) is one of the most popular and well-studied witnesses of Bell's theorem, separating classical from quantum correlations. In this work, for every $d \geqslant 2$, we present a generalization of the CHSH inequality with the property that maximal violation is achieved uniquely by the maximally entangled state of local dimension d. This provides an avenue for device-independent certification of maximally entangled states of arbitrary local dimension.

DOI: 10.1103/PhysRevA.98.052115

I. INTRODUCTION

In light of recent progress in quantum technologies, the problem of reliably certifying the correct functioning of quantum devices is rapidly gaining relevance. Certification procedures are most compelling when they can be carried out with minimal resources. The device-independent approach to certification is very desirable in this respect: it makes no assumption on the inner workings of the device being tested, other than a no-signaling constraint on the spatially separated components of a purported quantum device. Certification is based solely on the statistics, or correlations, of a Bell experiment. Device-independent self-testing refers to the most complete such certification, and it exploits the fact that certain correlations are sufficient to characterize exactly the quantum states and measurements that produce them, in a black-box fashion. The Clauser-Horne-Shimony-Holt (CHSH) inequality is the most well-studied example of such a device-independent self-test. In fact, maximal quantum violation of the CHSH inequality can be achieved uniquely by measuring a maximally entangled pair of qubits with specific measurements.

The full certification provided by device-independent self-testing is a powerful tool for a classical user trying to certify the behavior of noncommunicating untrusted quantum devices. For this reason, it has important applications in quantum cryptography, namely in quantum key distribution[1,2], randomness expansion [1], and delegated quantum computation [3–6]. Most of these applications rely on maximally entangled states as a resource. It is therefore crucial that we possess efficient ways to certify the presence of such a resource. In this paper, for any $d \geqslant 2$, we present a generalization of the CHSH inequality with the property that maximal violation self-tests the maximally entangled state of local dimension d. Previously, through various results in parallel self-testing, we knew of families self-testing maximally entangled states of local dimension d a power of 2 [7–11], or d^n for any $d \geqslant 2$ and for any $n \geqslant 2$ even [12]. Another relevant family of Bell inequalities, indexed by $d \geqslant 2$, was proposed by Salavrakos *et al.* [13]: there, the authors show that maximal violation is achieved by the maximally entangled state of local dimension d, but they leave open the question of whether the inequality self-tests the state (while giving numerical evidence for the case $d = 3$). For the family of Bell inequalities that we present, the self-testing property holds for arbitrary $d \geqslant 2$.

Our Bell inequality is inspired by the ideal correlations from Coladangelo *et al.* [14]. Informally, a correlation refers to the full data about the distribution of outcomes derived from measuring a bipartite state with certain local measurements. In [14], the authors show that for each pure bipartite entangled state there exists a quantum correlation that is uniquely attained by measuring that state, i.e., a correlation that self-tests the state. Here, our aim is to phrase this self-test in terms of maximal violation of some Bell inequality (instead of in terms of a correlation). In other words, we wish to find, for each such correlation, a Bell inequality whose maximal quantum violation is attained exclusively at that correlation, i.e., a hyperplane tangent to the set of quantum correlations only at that self-testing point. We succeed in the maximally entangled case, and this yields a generalization of the CHSH inequality.

Although our self-testing result is exact, we envision that, upon numerical or experimental analysis of the robustness of our result, our inequality could be employed to experimentally certify the presence of higher-dimensional maximally entangled states that are not necessarily a product of qubits, as is done in [15]. In particular, the authors of the experiment [15] certify fidelity with maximally entangled pairs of qudits by directly estimating the statistical closeness to the ideal correlations of [14]. Our inequality can potentially greatly simplify the process of estimation: estimating the value of the violation of an inequality requires a much smaller number of samples than estimating a full correlation table. Device-independent quantum cryptographic protocols that rely on maximally entangled states could see an increase in efficiency as a direct result of an increased efficiency in the certification procedure.

Our approach generalizes naturally also to the "tilted" case, and we present a candidate family of Bell inequalities generalizing the family of tilted CHSH inequalities [16].

*acoladan@caltech.edu

However, in the tilted case, the lack of symmetry seems to make the analysis surprisingly more complicated, and we can only conjecture that for each pure bipartite entangled state of any local dimension there is a corresponding inequality in the family whose maximal violation self-tests it.

We note that ours is not the first generalization of the CHSH inequality (or the CHSH game): a more natural algebraic generalization of the CHSH game over fields of order q was introduced by Buhrman and Massar [17], and studied by Bavarian and Shor [18]; another generalization was introduced by Tavakoli *et al.* and studied in the context of random access codes [19]. However, the self-testing properties of these generalizations are not known. Our generalization is unrelated to these, and in this paper we focus on establishing its self-testing properties.

The Bell operator for the maximally entangled case is presented in Sec. II, and concisely stated in Definition 2. The analytical quantum bound and self-testing results are stated in Theorems 5 and 6. Section III presents the candidate family for the tilted case, and the corresponding conjecture.

A. Notation and preliminaries

1. Correlations and strategies

Given sets $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$, a (bipartite) *correlation* is a collection of conditional probability distributions $\{p(a,b|x,y) : a \in \mathcal{A}, b \in \mathcal{B}\}_{(x,y)\in\mathcal{X}\times\mathcal{Y}}$. $\mathcal{X}$ and $\mathcal{Y}$ are referred to as the question sets, while $\mathcal{A}$ and $\mathcal{B}$ are the answer sets. Given question sets and answer sets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{A}$, $\mathcal{B}$, a *classical strategy* is specified by an integer k, a probability distribution $\{\lambda_i\}$ on $\{1,\dots,k\}$, a probability distribution $\{p^a_{x,i}\}$ on $\mathcal{A}$ for each $x \in \mathcal{X}$ and $1 \leqslant i \leqslant k$, and a probability distribution $\{q^b_{y,i}\}$ on $\mathcal{B}$ for each $y \in \mathcal{Y}$ and $1 \leqslant i \leqslant k$. It produces the correlation p such that

$$p(a,b|x,y) = \sum_{i=1}^{k} \lambda_i\, p^a_{x,i} q^b_{y,i} \quad \forall\, a \in \mathcal{A}, b \in \mathcal{B}, \; x \in \mathcal{X}, y \in \mathcal{Y}.$$

Given question sets and answer sets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{A}$, $\mathcal{B}$, a *quantum strategy* is specified by Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and projective measurements $\{\Pi^a_{A_x}\}_a$ on $\mathcal{H}_A$, $\{\Pi^b_{B_y}\}_b$ on $\mathcal{H}_B$ for $x \in \mathcal{X}$, $y \in \mathcal{Y}$. It produces the correlation p such that

$$p(a,b|x,y) = \langle\psi|\, \Pi^a_{A_x} \otimes \Pi^b_{B_y}\, |\psi\rangle \quad \forall\, a \in \mathcal{A}, b \in \mathcal{B}, \; x \in \mathcal{X}, y \in \mathcal{Y}.$$

Concisely, we refer to a quantum strategy as a triple $(|\psi\rangle, \{\Pi^a_{A_x}\}_a, \{\Pi^b_{B_y}\}_b)$. We take the measurements to be projective without loss of generality by appealing to Naimark's dilation theorem. We will sometimes describe a quantum strategy by specifying an observable for each question. The observables in turn specify the projectors through their eigenspaces. A correlation is said to be classical (quantum) if there exists a classical (quantum) strategy producing it. We denote by $\mathcal{C}_c^{m,n,r,s}$ and $\mathcal{C}_q^{m,n,r,s}$, respectively, the sets of classical and quantum correlations on question sets of sizes m, n and answer sets of sizes r, s.

2. Self-testing

We define self-testing formally:

Definition 1 (self-testing). We say that a correlation $\{p^*(a,b|x,y) : a \in \mathcal{A}, b \in \mathcal{B}\}_{x\in\mathcal{X}, y\in\mathcal{Y}}$ self-tests a strategy $(|\Psi\rangle, \{\tilde{\Pi}^a_{A_x}\}_a, \{\tilde{\Pi}^b_{B_y}\}_b)$ if, for any strategy $(|\psi\rangle, \{\Pi^a_{A_x}\}_a, \{\Pi^b_{B_y}\}_b)$ achieving p^*, there exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$ and an auxiliary state $|\text{aux}\rangle$ such that

$$\Phi(|\psi\rangle) = |\Psi\rangle \otimes |\text{aux}\rangle\,, \tag{1}$$

$$\Phi\big(\Pi^a_{A_x} \otimes \Pi^b_{B_y}\, |\psi\rangle\big) = \tilde{\Pi}^a_{A_x} \otimes \tilde{\Pi}^b_{B_y}\, |\Psi\rangle \otimes |\text{aux}\rangle \quad \forall\, a \in \mathcal{A}, b \in \mathcal{B}, x \in \mathcal{X}, y \in \mathcal{Y}. \tag{2}$$

Sometimes, we refer to *self-testing of the state* when we are only concerned with the guarantee of Eq. (1), and not (2). Moreover, we will informally say that "maximal violation of an inequality self-tests a state" to mean precisely that any correlation achieving maximal violation self-tests the state. There is also a notion of *robust* self-testing, when one can approximately characterize strategies that are close to achieving the ideal correlation [20,21]. For a precise definition, we refer the reader to [22]. We remark that, technically, we do not need to assume that the original strategy uses a pure state $|\psi\rangle$, but rather our proofs can be directly translated to the case of a mixed state (see [14] for a more precise account of this).

3. The family of tilted CHSH inequalities

We introduce the family of tilted CHSH inequalities [16]. Let A_0, A_1, B_0, B_1 be ±1-valued random variables. For a random variable X, let $\langle X\rangle$ denote its expectation. The tilted CHSH inequality [16], with parameter $\alpha \in [0,2]$, is the following generalization of the CHSH inequality:

$$\langle \alpha A_0 + A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1\rangle \leqslant 2 + \alpha, \tag{3}$$

which holds when the random variables are local. The maximal quantum violation is $I_\alpha := \sqrt{8+2\alpha^2}$ and is attained when the strategy of the two parties consists of sharing the joint state $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$, and measuring observables A_0, A_1 and B_0, B_1, respectively, where $A_0 = \sigma_z$, $A_1 = \sigma_x$, $B_0 = \cos\mu\sigma_Z + \sin\mu\sigma_X$, and $B_1 = \cos\mu\sigma_z + \sin\mu\sigma_x$, and $\sin 2\theta = \sqrt{\frac{4-\alpha^2}{4+\alpha^2}}$ [or $\alpha \equiv \alpha(\theta) = 2/\sqrt{1+2\tan^2 2\theta}$] and $\mu = \arctan\sin 2\theta$. Here σ_Z and σ_X are the usual Pauli matrices. The converse also holds, in the sense that maximal violation self-tests this strategy.

II. THE BELL INEQUALITY

The family of Bell inequalities that we are about to introduce is over question sets $\mathcal{X} = \{0,1,2\}$ and $\mathcal{Y} = \{0,1,2,3\}$, and answer sets $\mathcal{A} = \mathcal{B} = \{0,\dots,d-1\}$ (where $d \geqslant 2$ corresponds to the local dimension). We introduce some notation. For a correlation $p \in \mathcal{C}_q^{3,4,d,d}$ and $m \in \{0,1,\dots,\lfloor\frac{d}{2}\rfloor - 1\}$, define

$$[\text{CHSH}_m]_p := \sum_{\substack{x,y\in\{0,1\},\\ a,b\in\{2m,2m+1\}}} (-1)^{a\oplus b - xy}\, p(a,b|x,y), \tag{4}$$

where $a \oplus b - xy$ is intended modulo 2. Note that for $m = 0$, this is the usual CHSH Bell functional. For $m > 0$ the form

is the same, but the answers are in $\{2m, 2m+1\}$. In what follows, we will use the term "standard CHSH" to refer to the standard CHSH inequality or Bell functional on binary question and answer sets. This is to distinguish it from the new functionals we have just defined. We will also use the terms Bell operator and Bell functional interchangeably. We can define a similar functional to (4) for questions $x \in \{0, 2\}$ and $y \in \{2, 3\}$ and answers in $\{2m+1, 2m+2\}$. Here questions $x \in \{0, 2\}$ and $y \in \{2, 3\}$ take the role of the $\{0, 1\}$ questions in (4). So, for convenience of notation, define a relabeling map $f : \{0, 2\} \to \{0, 1\}$ to be such that $f(0) = 0$, $f(2) = 1$, and a relabeling map $g : \{2, 3\} \to \{0, 1\}$ to be such that $g(2) = 0$, $g(3) = 1$. Then, define

$$[\mathrm{CHSH}'_m]_p := \sum_{\substack{x\in\{0,2\}, y\in\{2,3\},\\ a,b\in\{2m+1,2m+2\}}} (-1)^{a\oplus b - f(x)g(y)} p(a,b|x,y).$$

Here the answers are intended "mod d," but we omit writing it for ease of notation. Denote by $\mathcal{C}$ and $\mathcal{C}'$ the sets

$$\mathcal{C} = \Big\{(a,b,x,y) : (x,y) \in \{0,1\}\times\{0,1\} \wedge (a,b) \notin \bigcup_{m=0}^{\lfloor \frac{d}{2}\rfloor -1} \{2m, 2m+1\}^2\Big\},$$

$$\mathcal{C}' = \Big\{(a,b,x,y) : (x,y) \in \{0,2\}\times\{2,3\} \wedge (a,b) \notin \bigcup_{m=0}^{\lfloor \frac{d}{2}\rfloor -1} \{2m+1, 2m+2\}^2\Big\}.$$

Then, define the cross-terms

$$[\mathrm{CROSS}]_p := \sum_{a,b,x,y:(a,b,x,y)\in\mathcal{C}} p(a,b|x,y),$$

$$[\mathrm{CROSS}']_p := \sum_{a,b,x,y:(a,b,x,y)\in\mathcal{C}'} p(a,b|x,y).$$

We are ready to define the family of Bell operators for our inequalities.

Definition 2 (The Bell operator). Let $d \geqslant 2 \in \mathbb{Z}$ and $\mathbb{1}_{\{d>2\}}$ and $\mathbb{1}_{\{d \text{ odd}\}}$ be the indicator functions for the cases $d > 2$ and d odd respectively. Let $\epsilon > 0$ be a constant. For a correlation p, the Bell operator takes the form

$$\begin{aligned}[\mathcal{B}]_p := &\sum_{m=0}^{\lfloor \frac{d}{2}\rfloor -1} [\mathrm{CHSH}_m]_p + \mathbb{1}_{\{d>2\}} \sum_{m=0}^{\lfloor \frac{d}{2}\rfloor -1} [\mathrm{CHSH}'_m]_p \\ &- \epsilon([\mathrm{CROSS}]_p + [\mathrm{CROSS}']_p) \\ &+ \mathbb{1}_{\{d \text{ odd}\}} \frac{\sqrt{2}}{2}\left(\sum_{x,y\in\{0,1\}} p(d-1, d-1|x,y) \right. \\ &\left. + \sum_{\substack{x\in\{0,2\},\\ y\in\{2,3\}}} p(0,0|x,y)\right). \end{aligned} \tag{5}$$

Intuitively the terms CROSS and CROSS′ can be thought of as "penalty" terms: they are meant to enforce that any correlation maximizing the value of the Bell operator must put zero probability mass on the cross-terms from $\mathcal{C}$ and $\mathcal{C}'$. We will argue that it is enough to multiply these penalty terms by any arbitrarily small but positive constant ϵ to ensure that maximal violation is attained exclusively by the maximally entangled state. On the other hand, with a zero penalty it is still the case that the corresponding Bell inequality can be maximally violated using a maximally entangled state, but we are unable to show that the self-testing result still holds true (i.e., the converse).

Theorem 1 (classical bound). For any $d \geqslant 2$ and any $p \in \mathcal{C}_c^{3,4,d,d}$:

$$[\mathcal{B}]_p \leqslant 2(1 + \mathbb{1}_{\{d>2\}}).$$

Proof. The proof is straightforward and the details are not particularly instructive. We refer the interested reader to the Appendix for the full proof. We turn to quantum correlations. We establish the following two theorems:

Theorem 2 (Quantum bound). For any d even and any $p \in \mathcal{C}_q^{3,4,d,d}$:

$$[\mathcal{B}]_p \leqslant 2\sqrt{2}(1 + \mathbb{1}_{\{d>2\}}).(A1) \tag{6}$$

Theorem 3 (Exact self-testing). For any $d \geqslant 2$, there is a unique correlation that achieves the quantum bound of $\mathcal{B}$, and it self-tests the state $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$.

Proof overview. At a high level, the proof of Theorems 5 and 6 goes through the following steps:

(i) The correlation from [14] (in the maximally entangled case) achieves the right-hand side of (A1) (Lemma 1).

(ii) Any correlation achieving the maximal quantum value of the Bell operator must have zero probability mass on the cross-terms. This is proved by starting from a correlation that achieves the maximum but has nonzero cross-terms, and modifying this into a strategy for qubit CHSH that achieves a value strictly higher than $2\sqrt{2}$, which is a contradiction. (See Lemma 2 in the Appendix.)

(iii) Having zero cross-terms forces the correlations to have the block-diagonal form of [14]. The 2×2 blocks are across pairs of answers $\{2m, 2m+1\}$ for questions $x, y \in \{0, 1\}$ and across pairs of answers $\{2m+1, 2m+2\}$ for questions $x \in \{0, 2\}$, $y \in \{2, 3\}$ (Lemma 3 in the Appendix).

(iv) Finally, the freedom in the value of the weights of the blocks is fixed by the requirement that the block-diagonal structure is both over pairs of answers $\{2m, 2m+1\}$, for $x, y \in \{0, 1\}$, and also over pairs of answers $\{2m+1, 2m+2\}$, for $x \in \{0, 2\}$, $y \in \{2, 3\}$, and these two subsets of questions have in common the question $x = 0$.

For the full details of the proof, we refer the reader to the Appendix. We will describe here the ideal correlations achieving the quantum bound of (A1). For a single-qubit observable A, we denote by $(A)_m$ the observable defined with respect to the basis $(|2m\rangle, |2m+1\rangle)$. For example, $(\sigma_Z)_m = |2m\rangle\langle 2m| - |2m+1\rangle\langle 2m+1|$. Similarly, we denote by $(A)'_m$ the observable defined with respect to the basis $(|2m+1\rangle, |2m+2\rangle)$.

Lemma 1 (ideal correlation from [14] achieving the quantum bound). The correlation $p^* \in \mathcal{C}_q^{3,4,d,d}$ specified by the following quantum strategy $(|\Psi\rangle, \{\Pi^a_{A_x}\}_a, \{\Pi^b_{B_y}\}_b)$ achieves the right-hand side of (A1):

(i) $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$.

(ii) For $m = 0, \ldots, \lfloor \frac{d}{2} \rfloor - 1$.

(a) $\Pi_{A_0}^{2m}$, $\Pi_{A_0}^{2m+1}$ are the projectors, respectively, onto the $+1, -1$ eigenspaces of $(\sigma_Z)_m$ (in other words, the measurement for $x = 0$ is in the computational basis).

(b) $\Pi_{A_1}^{2m}$, $\Pi_{A_1}^{2m+1}$ onto the $+1, -1$ eigenspaces of $(\sigma_X)_m$. If d is odd, $\Pi_{A_1}^{d-1} = |d-1\rangle\langle d-1|$.

(c) $\Pi_{A_2}^{2m+1}$, $\Pi_{A_2}^{2m+2}$ onto the $+1, -1$ eigenspaces of $(\sigma_X)'_m$. If d is odd, $\Pi_{A_2}^{0} = |0\rangle\langle 0|$.

(iii) For $m = 0, \ldots, \lfloor \frac{d}{2} \rfloor - 1$,

(a) For $y \in \{0, 1\}$, $\Pi_{B_y}^{2m}$, $\Pi_{B_y}^{2m+1}$ are the projectors, respectively, onto the $+1, -1$ eigenspaces of $(\frac{\sigma_Z + (-1)^y \sigma_X}{\sqrt{2}})_m$. If d is odd, $\Pi_{B_y}^{d-1} = |d-1\rangle\langle d-1|$.

(b) For $y \in \{2, 3\}$, $\Pi_{B_y}^{2m+1}$, $\Pi_{B_y}^{2m+2}$ onto the $+1, -1$ eigenspaces of $(\frac{\sigma_Z + (-1)^y \sigma_X}{\sqrt{2}})'_m$. If d is odd, $\Pi_{B_y}^{0} = |0\rangle\langle 0|$.

Proof. This is a straightforward check.

III. GENERALIZING THE TILTED CHSH INEQUALITIES (A CONJECTURE)

Let $I_\alpha = \sqrt{8 + 2\alpha^2}$ be the maximal quantum violation of the tilted CHSH inequality for coefficient α. The family of candidate Bell inequalities that we will describe is a very natural generalization of the Bell inequality from the previous section to the tilted case. We introduce some notation. For a correlation $p \in \mathcal{C}_q^{3,4,d,d}$, define

$$[\mathrm{tCHSH}_m(\alpha)]_p := \alpha[p(a = 2m|x = 0) - p(a = 2m+1|x = 0)] + [\mathrm{CHSH}_m]_p,$$

where $[\mathrm{CHSH}_m]_p$ was defined earlier. This can be thought of as a tilted CHSH Bell operator restricted to answers in $\{2m, 2m+1\}$. Note that the above involves only questions $x, y \in \{0, 1\}$. We can define a similar term for questions in $x \in \{0, 2\}$ and $y \in \{2, 3\}$ and answers in $\{2m+1, 2m+2\}$. Let

$$[\mathrm{tCHSH}'_m(\alpha)]_p := \alpha[p(a = 2m+1|x = 0) - p(a = 2m+2|x = 0)] + [\mathrm{CHSH}'_m]_p.$$

The sets $\mathcal{C}$ and $\mathcal{C}'$ of questions and answers corresponding to cross-terms are defined as in the previous section. Then our candidate family of Bell operators generalizing the family of tilted CHSH inequalities is the following:

Definition 3 (the family of Bell operators). Each inequality in the family is specified by

(i) $0 < c_i < 1 \in \mathbb{R}$, $i = 0, \ldots, d-1$ with $\sum_{i=0}^{d-1} c_i^2 = 1$.

(ii) $d \geqslant 2 \in \mathbb{N}$.

Let $\theta_m = \arctan \frac{c_{2m+1}}{c_{2m}}$, $\alpha_m \equiv \alpha_m(\theta_m) \in [0, 2)$ be defined by $\sin 2\theta_m = \sqrt{\frac{4-\alpha_m^2}{4+\alpha_m^2}}$, $\theta'_m = \arctan \frac{c_{2m+2}}{c_{2m+1}}$, $\alpha'_m \equiv \alpha'_m(\theta'_m) \in [0, 2)$ defined by $\sin 2\theta'_m = \sqrt{\frac{4-\alpha'^2_m}{4+\alpha'^2_m}}$. Let $\epsilon > 0$ be a constant. For a correlation $p \in \mathcal{C}_q^{3,4,d,d}$, the Bell operator is

$$\begin{aligned}
&[t\mathcal{B}(c_0, \ldots, c_{d-1})]_p \\
&:= \sum_{m=0}^{\lfloor \frac{d}{2} \rfloor - 1} \frac{1}{I_{\alpha_m}} [\mathrm{tCHSH}_m(\alpha_m)]_p \\
&+ \mathbb{1}_{\{d>2\}} \sum_{m=0}^{\lfloor \frac{d}{2} \rfloor - 1} \frac{1}{I_{\alpha'_m}} [\mathrm{tCHSH}'_m(\alpha'_m)]_p \\
&- \epsilon([\mathrm{CROSS}]_p + [\mathrm{CROSS}']_p) \\
&+ \mathbb{1}_{\{d \text{ odd}\}} \frac{1}{4} \left(\sum_{x,y \in \{0,1\}} p(d-1, d-1|x, y) \right. \\
&\left. + \sum_{\substack{x \in \{0,2\}, \\ y \in \{2,3\}}} p(0, 0|x, y) \right). \qquad (7)
\end{aligned}$$

Note that to put the Bell operator for the maximally entangled case in this form, one just needs to divide (5) by $2\sqrt{2}$.

Conjecture 1 (quantum bound and self-testing). For any d even and any $p \in \mathcal{C}_q^{3,4,d,d}$:

$$[t\mathcal{B}(c_0, \ldots, c_{d-1})]_p \leqslant 1 + \mathbb{1}_{\{d>2\}}.$$

Moreover, there is a unique quantum correlation achieving the bound, and it self-tests the state $|\Psi\rangle = \sum_{i=0}^{d-1} c_i |ii\rangle$.

The lack of symmetry in the tilted case seems to make the analysis surprisingly less straightforward, and the arguments we employed in the maximally entangled case do not directly carry over.

An open question that applies to both the maximally entangled and the tilted Bell operators is to determine if cross-terms are necessary for the self-testing property to hold true [i.e., whether, in (5) and (7), $\epsilon > 0$ is necessary or $\epsilon = 0$ suffices].

IV. CONCLUSION

In this work, we have presented a generalization of the CHSH inequality with the property that the unique state achieving the maximal violation of the inequality is a maximally entangled pair of qudits. This is an example of a Bell inequality that exhibits such a property for any local dimension $d \geqslant 2$. Certifying high-dimensional maximally entangled states is a building block for many device-independent tasks in quantum cryptography [1,2,6]. Thus, the efficiency of procedures for certifying such a resource has a direct impact on the efficiency of these tasks. Estimating the value of the violation of our inequality is a simple procedure that can bound the fidelity with an ideal pair of maximally entangled qudits. An experimental analysis is required to quantify these bounds, in the style of [15,23]. We envision that our inequality could simplify the estimation procedure in these experiments, and reduce the sample complexity.

ACKNOWLEDGMENTS

The author thanks Koon Tong Goh and Thomas Vidick for helpful discussions, and thanks the latter for useful comments on an earlier version of this work. The author appreciates support from the Kortschak Scholars program, and AFOSR YIP Award No. FA9550-16-1-0495.

APPENDIX

We provide the proofs of the technical Theorems. We also restate these Theorems to facilitate reading.

Theorem 4 (classical bound). For any $d \geqslant 2$ and any $p \in \mathcal{C}_c^{3,4,d,d}$,

$$[\mathcal{B}]_p \leqslant 2(1 + \mathbb{1}_{\{d>2\}}).$$

Proof. For $d = 2$, we recover the classical case of the standard CHSH inequality, so assume $d > 2$ from now on. Finding the best classical strategy is equivalent to finding the best deterministic strategy. Let $f_A : \{0, 1, 2\} \to \{0, \ldots, d-1\}$ and $f_B : \{0, 1, 2, 3\} \to \{0, \ldots, d-1\}$ be functions specifying a deterministic strategy. Now, suppose $f_A(0) \in \{2k, 2k+1\}$, $f_A(1) \in \{2l, 2l+1\}$ and $f_A(2) \in \{2l', 2l'+1\}$.

(i) If $k = l$, it is easy to see that the best choice for $f_B(0)$ and $f_B(1)$ is to have also $f_B(0)$, $f_B(1) \in \{2k, 2k+1\}$ and get a contribution of at most 2 (this is from the standard CHSH classical bound).

(ii) If $k \neq l$, it is also easy to see that the best choice for $f_B(0)$ and $f_B(1)$ is to have one of three possibilities: $f_B(0)$, $f_B(1) \in \{2k, 2k+1\}$; $f_B(0)$, $f_B(1) \in \{2l, 2l+1\}$; or one in $\{2k, 2k+1\}$ and the other in $\{2l, 2l+1\}$. They all achieve a contribution of at most 2.

Similarly, the best possible choice for $f_B(2)$ and $f_B(3)$ gives a contribution of 2. This yields the desired bound.

Theorem 5 (quantum bound). For any d even and any $p \in \mathcal{C}_q^{3,4,d,d}$:

$$[\mathcal{B}]_p \leqslant 2\sqrt{2} \times (1 + \mathbb{1}_{\{d>2\}}). \tag{A1}$$

Theorem 6 (exact self-testing). For any $d \geqslant 2$, there is a unique correlation that achieves the quantum bound of $\mathcal{B}$, and it self-tests the state $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$.

The proof of Theorems 5 and 6 requires the following technical lemmas.

Lemma 2 (zero mass on the cross terms). Let $p \in \mathcal{C}_q^{3,4,d,d}$ be a quantum correlation achieving the maximal quantum value of $\mathcal{B}$. Then, $p(a, b|x, y) = 0 \, \forall (a, b, x, y) \in \mathcal{C} \cup \mathcal{C}'$.

This establishes that any correlation maximally violating the Bell inequality must have the same block-diagonal form of the self-testing correlation from Lemma 1 of the main text.

Proof. We argue first for the case of d even. We will show that any correlation achieving the maximal value of $\mathcal{B}$ must have $p(a, b|x, y) = 0 \ \forall (a, b, x, y) \in \mathcal{C} \cup \mathcal{C}'$. Suppose for a contradiction that a correlation $p \in \mathcal{C}_q^{3,4,d,d}$ achieves the maximal value of $\mathcal{B}$ and $p(a, b|x, y) = \gamma > 0$ for some $(a, b, x, y) \in \mathcal{C} \cup \mathcal{C}'$. To compensate for the negative contribution due to the presence of the cross-terms in the Bell operator [Eq. (5) from the main text], which are multiplied by an arbitrarily small but positive constant ϵ, it must be the case that either $\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}_m]_p > 2\sqrt{2}$ or $\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}'_m]_p > 2\sqrt{2}$ (since we know from Lemma 1 of the main text that the maximal value of $\mathcal{B}$ is at least $2 \times 2\sqrt{2}$). Assume the former (the other case being similar).

Let $S = (|\psi\rangle, \Pi_{A_x}^a, \Pi_{B_y}^b)$ be a quantum strategy producing correlation p. We will use this to construct a correlation $\tilde{p} \in \mathcal{C}_q^{2,2,2,2}$ that achieves a value of CHSH greater than $2\sqrt{2}$, which would be a contradiction. This is achieved by starting from strategy S and mapping each pair of answers $(2k, 2k+1)$ in $\{2, \ldots, d-1\}$ to either their parity or the opposite of their parity, i.e., either $(2k, 2k+1) \mapsto (0, 1)$ or $(2k, 2k+1) \mapsto (1, 0)$. More precisely, for $\vec{o} \in \{0, 1\}^{\frac{d}{2}-1}$ let $\vec{o}[m]$ denote the mth bit of $\vec{o}$, and define a new quantum strategy for standard CHSH $S^{(\vec{o})} = (|\psi\rangle, \{\tilde{\Pi}_{A_x}^a\}_{a,x\in\{0,1\}}, \{\tilde{\Pi}_{B_y}^b\}_{b,y\in\{0,1\}})$ on the same state $|\psi\rangle$, with projectors, for $x, y \in \{0, 1\}$,

$$\begin{aligned}
\tilde{\Pi}_{A_x}^0 &= \Pi_{A_x}^0 + \sum_{m=1}^{\frac{d}{2}-1} \Pi_{A_x}^{2m+\vec{o}[m]}, \\
\tilde{\Pi}_{A_x}^1 &= \Pi_{A_x}^1 + \sum_{m=1}^{\frac{d}{2}-1} \Pi_{A_x}^{2m+1-\vec{o}[m]}, \qquad \text{(A2)} \\
\tilde{\Pi}_{B_y}^0 &= \Pi_{B_y}^0 + \sum_{m=1}^{\frac{d}{2}-1} \Pi_{B_y}^{2m+\vec{o}[m]}, \\
\tilde{\Pi}_{B_y}^1 &= \Pi_{B_y}^1 + \sum_{m=1}^{\frac{d}{2}-1} \Pi_{B_y}^{2m+1-\vec{o}[m]}. \qquad \text{(A3)}
\end{aligned}$$

Let $\tilde{p}^{(\vec{o})}$ be the resulting correlation. Now, let $[\mathrm{CHSH}]_{\tilde{p}^{(\vec{o})}}$ be the CHSH value of correlation $\tilde{p}^{(\vec{o})}$. Since CHSH is an XOR game (i.e., only the XOR of the answers matters), it is easy to see that for any $\vec{o} \in \{0, 1\}^{\frac{d}{2}-1}$,

$$[\mathrm{CHSH}]_{\tilde{p}^{(\vec{o})}} = \sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}_m]_p + C, \tag{A4}$$

where C is a (possibly negative) contribution that comes from the cross-terms of the form $\langle\psi| \Pi_{A_x}^a \otimes \Pi_{B_y}^b |\psi\rangle$ for $(a, b, x, y) \in \mathcal{C}$. However, there exists a choice of $\vec{o} \in \{0, 1\}^{\frac{d}{2}-1}$ such that $C \geqslant 0$. In fact, notice that the contributions to C coming from cross-terms involving $(2m, 2m+1)$ when one chooses $\vec{o}[m] = 0$ or $\vec{o}[m] = 1$ (and keeps the other choices fixed) are the negative of each other. Hence at least one of the two choices gives a non-negative contribution. Then, pick $\vec{o} \in \{0, 1\}^{\frac{d}{2}-1}$ as follows: for $m = 1, \ldots, \frac{d}{2} - 1$, in this order, choose a value of $\vec{o}[m]$ for which the contribution from cross-terms involving pairs $(2m, 2m+1)$ and $(2m', 2m'+1)$ for $m' < m$ is non-negative. This gives $C \geqslant 0$. So, for this choice of $\vec{o}$, one gets $[\mathrm{CHSH}]_{\tilde{p}^{(\vec{o})}} > 2\sqrt{2}$, which is the desired contradiction.

The case of d odd is similar but requires slightly more effort. Suppose $p \in \mathcal{C}_q^{3,4,d,d}$ achieves the maximal value of $\mathcal{B}$ and $p(a, b|x, y) = \gamma > 0$ for some $(a, b, x, y) \in \mathcal{C} \cup \mathcal{C}'$. Then it must be the case that either $\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}_m]_p + \frac{\sqrt{2}}{2} \sum_{x,y\in\{0,1\}} p(d-1, d-1|x, y) > 2\sqrt{2}$ or $\sum_{m=0}^{\frac{d}{2}-1} [\mathrm{CHSH}'_m]_p + \frac{\sqrt{2}}{2} \sum_{x\in\{0,2\},y\in\{2,3\}} p(0, 0|x, y) > 2\sqrt{2}$. Suppose the former (the latter case being similar). Let $S = (|\psi\rangle, \Pi_{A_x}^a, \Pi_{B_y}^b)$ be a quantum strategy producing correlation p. For a string $\vec{o} \in \{0, 1\}^{\frac{d}{2}-1}$, we construct the following strategy for CHSH $S^{(\vec{o})} = (|\tilde{\psi}\rangle, \{\tilde{\Pi}_{A_x}^a\}_{a,x\in\{0,1\}}, \{\tilde{\Pi}_{B_y}^b\}_{b,y\in\{0,1\}})$: intuitively, the two parties share the original state tensored with an EPR pair. They map outcomes $\{0, \ldots, d-2\}$ to outcomes in $\{0, 1\}$ (similarly

as before). If one sees outcome $d-1$, they measure the shared EPR pair with an appropriate ideal CHSH measurement. More precisely, let $\{P^a_{A_x}\}_{a,x\in\{0,1\}}, \{P^b_{B_y}\}_{b,y\in\{0,1\}}$ be the ideal CHSH qubit measurements. Then, $|\tilde{\psi}\rangle = |\psi\rangle \otimes |\mathrm{EPR}\rangle$, and

$$\tilde{\Pi}^0_{A_x} = \left[\Pi^0_{A_x} + \sum_{m=1}^{\lfloor \frac{d}{2}\rfloor -1} \Pi^{2m+\vec{o}[m]}_{A_x}\right] \otimes I + \Pi^{d-1}_{A_x} \otimes P^0_{A_x},$$

$$\tilde{\Pi}^1_{A_x} = \left[\Pi^1_{A_x} + \sum_{m=1}^{\lfloor \frac{d}{2}\rfloor -1} \Pi^{2m+1-\vec{o}[m]}_{A_x}\right] \otimes I + \Pi^{d-1}_{A_x} \otimes P^1_{A_x},$$

$$\tilde{\Pi}^0_{B_y} = \left[\Pi^0_{B_y} + \sum_{m=1}^{\lfloor \frac{d}{2}\rfloor -1} \Pi^{2m+\vec{o}[m]}_{B_y}\right] \otimes I + \Pi^{d-1}_{B_y} \otimes P^0_{B_y},$$

$$\tilde{\Pi}^1_{B_y} = \left[\Pi^1_{B_y} + \sum_{m=1}^{\lfloor \frac{d}{2}\rfloor -1} \Pi^{2m+1-\vec{o}[m]}_{B_y}\right] \otimes I + \Pi^{d-1}_{B_y} \otimes P^1_{B_y}.$$

One can check, then, that with the appropriate choice of $\vec{o}$ (chosen similarly to the d even case), this gives a strategy for CHSH that achieves a value strictly greater than $2\sqrt{2}$.

The following lemma establishes that if a correlation p has zero cross-terms, then this implies that the restriction of p to the subset of questions $(x, y) \in \{0, 1\}^2$ and to answers $a, b \in \{2m, 2m+1\}$ is still a correlation (multiplied by some weight). Likewise for the restriction to the subset of questions $(x, y) \in \{0, 2\} \times \{2, 3\}$ and to answers $a, b \in \{2m+1, 2m+2\}$.

Lemma 3. Any correlation $p \in \mathcal{C}_q^{3,4,d,d}$ with zero cross-terms (i.e., of the form of Lemma 2) satisfies the following:

(i) If d is even, for each $m = 0, \ldots, \frac{d}{2}-1$, there exist weights $w_m, w'_m \geqslant 0$ with $\sum_m w_m = 1$, $\sum_m w'_m = 1$ and correlations $p_m, p'_m \in \mathcal{C}_q^{2,2,2,2}$ (with questions in $\{0,1\}^2$ and $\{0,2\}\times\{2,3\}$, respectively, and answers in $\{0,1\}$) such that $\forall\, m$, $\forall\, a, b \in \{2m, 2m+1\}$, $x, y \in \{0,1\}$:

$$p(a, b|x, y) = w_m\, p_m(a \mod 2, b \mod 2|x, y)$$

and $\forall\, m$, $\forall\, a, b \in \{2m+1, 2m+2\}$, $x \in \{0,2\}$, $y \in \{2,3\}$:

$$p(a, b|x, y) = w'_m \cdot p'_m(a \mod 2, b \mod 2|x, y).$$

(ii) If d is odd, the analogous statement holds, except that the weights w_m, w'_m are such that $\sum_m w_m + p(d-1, d-1|0, 0) = \sum_m w'_m + p(0, 0|2, 2) = 1$, AND

(a) $p(d-1, d-1|x, y) = p(d-1, d-1|x', y') \forall\ x, y, x'y' \in \{0,1\}$.

(b) $p(0, 0|x, y) = p(0, 0|x', y')\ \forall\ x, x' \in \{0,2\}, y, y' \in \{2,3\}$.

Proof. Let $p \in \mathcal{C}_q^{3,4,d,d}$ be of the form of Lemma 2, and let $(|\psi\rangle, \{\Pi^a_{A_x}\}, \{\Pi^b_{B_y}\})$ be a strategy reproducing p. Then, for $m = 0, \ldots, \frac{d}{2}-1$ define the following:

(i) for $x, y \in \{0,1\}$, $A^{(m)}_x = \Pi^{2m}_{A_x} - \Pi^{2m+1}_{A_x}$ and $B^{(m)}_y = \Pi^{2m}_{B_y} - \Pi^{2m+1}_{B_y}$,

(ii) for $x \in \{0,2\}$, $y \in \{2,3\}$, $A'^{(m)}_x = \Pi^{2m+1}_{A_x} - \Pi^{2m+2}_{A_x}$ and $B'^{(m)}_y = \Pi^{2m+1}_{B_y} - \Pi^{2m+2}_{B_y}$.

Define the subspaces $\mathcal{U}_m = \mathrm{Range}(A^{(m)}_0) + \mathrm{Range}(A^{(m)}_1)$ and $\mathcal{V}_m = \mathrm{Range}(B^{(m)}_0) + \mathrm{Range}(B^{(m)}_1)$, and let $\mathbb{1}_{\mathcal{U}_m}$ and $\mathbb{1}_{\mathcal{V}_m}$ be projections onto these subspaces. Let $|\psi_m\rangle = \mathbb{1}_{\mathcal{U}_m}\mathbb{1}_{\mathcal{V}_m}|\psi\rangle$.

We will check that $\mathbb{1}_{\mathcal{U}_m}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(A^{(m)}_0)}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle = \mathbb{1}_{\mathcal{V}_m}|\psi\rangle = |\psi_m\rangle$. We compute

$$\mathbb{1}_{\mathrm{Range}(A^{(m)}_0)}|\psi\rangle = \left(\Pi^{2m}_{A_0} + \Pi^{2m+1}_{A_0}\right)|\psi\rangle \tag{A5}$$

$$= \left(\Pi^{2m}_{A_0} + \Pi^{2m+1}_{A_0}\right)\sum_{l=0}^{d-1}\Pi^l_{B_0}|\psi\rangle \tag{A6}$$

$$= \left(\Pi^{2m}_{A_0} + \Pi^{2m+1}_{A_0}\right)\left(\Pi^{2m}_{B_0} + \Pi^{2m+1}_{B_0}\right)|\psi\rangle \tag{A7}$$

$$= \mathbb{1}_{\mathrm{Range}(A^{(m)}_0)}\mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle, \tag{A8}$$

where the third line follows from the hypothesis that the correlation has the form of Lemma 2. The same calculation starting from $\mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle$ gives $\mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(A^{(m)}_0)}\mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle$, which, together with (A8), implies $\mathbb{1}_{\mathrm{Range}(A^{(m)}_0)}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle$. With similar calculations, we also deduce $\mathbb{1}_{\mathrm{Range}(A^{(m)}_1)}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle$, which implies $\mathbb{1}_{\mathrm{Range}(A^{(m)}_0)}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(A^{(m)}_1)}|\psi\rangle$, and hence $\mathbb{1}_{\mathcal{U}_m}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(A^{(m)}_0)}|\psi\rangle$. Similarly, $\mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(B^{(m)}_1)}|\psi\rangle$, and hence $\mathbb{1}_{\mathcal{V}_m}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle$. Altogether, we have deduced that $\mathbb{1}_{\mathcal{U}_m}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(A^{(m)}_0)}|\psi\rangle = \mathbb{1}_{\mathrm{Range}(B^{(m)}_0)}|\psi\rangle = \mathbb{1}_{\mathcal{V}_m}|\psi\rangle = |\psi_m\rangle$.

Hence, setting $w_m = \| |\psi_m\rangle \|^2$ gives the desired weights, and it is clear what the correlations p_m are. We argue similarly for the weights w'_m and the correlations p'_m. A very similar argument yields the conclusion for the case of odd d.

Corollary 1. Any correlation $p \in \mathcal{C}_q^{3,4,d,d}$ with zero cross-terms (i.e., of the form of Lemma 2) satisfies the following:

(i) If d is even, there exist weights $w_m, w'_m \geqslant 0$, $m = 0, \ldots, \frac{d}{2}-1$, with $\sum_m w_m = 1$, $\sum_m w'_m = 1$, such that, for all m,

$$[\mathrm{CHSH}_m]_p \leqslant w_m 2\sqrt{2}$$

and

$$[\mathrm{CHSH}'_m]_p \leqslant w'_m 2\sqrt{2}.$$

(ii) If d is odd, the analogous statement holds, except that the weights w_m, w'_m are such that $\sum_m w_m + p(d, d|0, 0) = 1$, $\sum_m w'_m + p(0, 0|2, 2) = 1$.

Proof. This follows immediately from Lemma 3.

Proof of Theorems 5 and 6. Assume $d > 2$, as the $d = 2$ case corresponds to standard CHSH. We start with d even (the odd case being similar). Let $p \in \mathcal{C}_q^{3,4,d,d}$ be a correlation that achieves the maximal quantum value of $\mathcal{B}$. By Lemma 2, p must have zero cross-terms. Then, from Lemma 3, we deduce, for $m = 0, \ldots, \frac{d}{2}-1$, the existence of weights w_m, w'_m and correlations p_m, p'_m satisfying the statement of the Lemma. This implies

$$\sum_{m=0}^{\frac{d}{2}-1}[\mathrm{CHSH}_m]_p = \sum_{m=0}^{\frac{d}{2}-1} w_m[\mathrm{CHSH}]_{p_m} \leqslant 2\sqrt{2}, \tag{A9}$$

where we have bounded each term with the standard CHSH bound. Similarly, we also get $\sum_{m=0}^{\frac{d}{2}-1}[\mathrm{CHSH}'_m]_p \leqslant 2\sqrt{2}$, which implies the desired upper bound of Theorem 5.

Such an upper bound is achieved if and only if $[\mathrm{CHSH}]_{p_m} = w_m 2\sqrt{2}$ for all m, and $[\mathrm{CHSH}'_m]_p = w'_m 2\sqrt{2}$ for all m. This is if and only if

(i) for all m, $w_m = 0$ OR p_m is the ideal qubit CHSH correlation, AND

(ii) for all m, $w'_m = 0$ OR p'_m is the ideal qubit CHSH correlation.

We want to argue that the only way that this can happen is if the weights are all equal (and nonzero). Once we have shown this, we notice that we have specified the correlation p completely for the two subsets of questions $x, y \in \{0, 1\}$ and $x \in \{0, 2\}$, $y \in \{2, 3\}$. From [14], we know this is enough to uniquely determine the self-testing correlation for the maximally entangled state of local dimension d presented in [14] (and in Lemma 1 of the main text), and we thus deduce that maximal violation of the Bell inequality self-tests $|\Psi\rangle$.

Let $|\psi\rangle$, $\{\Pi^a_{A_x}\}_a$, $\{\Pi^b_{B_y}\}_b$ be a quantum strategy for p (which achieves the upper bound). Then, by what we have argued above, for all m we have $\|\Pi^{2m+1}_{A_0}|\psi\rangle\|^2 = w_m \frac{1}{2}$, and this holds both when $w_m \neq 0$ (and p_m is the ideal qubit CHSH correlation) and when $w_m = 0$. Likewise, we have that $\|\Pi^{2m+1}_{A_0}|\psi\rangle\|^2 = w'_m \frac{1}{2}$. And similarly $\|\Pi^{2m}_{A_0}|\psi\rangle\|^2 = w_m \frac{1}{2}$ and $\|\Pi^{2m}_{A_0}|\psi\rangle\|^2 = w'_{m-1}\frac{1}{2}$. Clearly this, together with the constraint $\sum_m w_m = \sum_m w'_m = 1$, implies $w_m = w'_m = \frac{2}{d}$ $\forall\, m$.

The proof is similar for the case of d odd, where we instead deduce $w_m = w'_m = \frac{2}{d}$ $\forall$ m (there are $\frac{d-1}{2}$ values of m) and $p(d-1, d-1|x, y) = p(0, 0|x', y') = \frac{1}{d}$ $\forall\, x, y \in \{0, 1\}$, $x' \in \{0, 2\}$, $y' \in \{2, 3\}$.

[1] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, J. ACM **63**, 33 (2016).

[2] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (2014).

[3] A. Coladangelo, A. Grilo, S. Jeffery, and T. Vidick, Verifier-on-a-leash: New schemes for verifiable delegated quantum computation, with quasilinear resources, arXiv:1708.07359.

[4] A. Gheorghiu, E. Kashefi, and P. Wallden, Robustness and device independence of verifiable blind quantum computing, New J. Phys. **17**, 083040 (2015).

[5] M. McKague, Interactive proofs for bqp via self-tested graph states, Theor. Comput. **12**, 1 (2016).

[6] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, Nature (London) **496**, 456 (2013), full version arXiv:1209.0448.

[7] R. Chao, B. W. Reichardt, C. Sutherland, and T. Vidick, Test for a large amount of entanglement, using few measurements, Quantum **2**, 92 (2018).

[8] A. Coladangelo, Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game, Quantum Inf. Comput. **17**, 831 (2017).

[9] M. Coudron and A. Natarajan, The parallel-repeated magic square game is rigid, arXiv:1609.06306.

[10] M. McKague, Self-testing in parallel, New J. Phys. **18**, 045013 (2016).

[11] A. Natarajan and T. Vidick, Robust self-testing of many-qubit states, Proc. of STOC **17**, 1003 (2017).

[12] A. Coladangelo and J. Stark, Robust self-testing for linear constraint system games, arXiv:1709.09267.

[13] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, Bell Inequalities Tailored to Maximally Entangled States, Phys. Rev. Lett. **119**, 040402 (2017).

[14] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. **8**, 15485 (2017).

[15] W.-H. Zhang, G. Chen, X.-X. Peng, X.-M. Hu, Z.-B. Hou, S. Yu, X.-J. Ye, Z.-Q. Zou, X.-Y. Xu, J.-S. Tang *et al.*, Experimental self-testing of entangled states, arXiv:1803.10961.

[16] A. Acín, S. Massar, and S. Pironio, Randomness Versus Nonlocality and Entanglement, Phys. Rev. Lett. **108**, 100402 (2012).

[17] H. Buhrman and S. Massar, Causality and Tsirelson's bounds, Phys. Rev. A **72**, 052103 (2005).

[18] M. Bavarian and P. W. Shor, Information causality, Szemerédi-Trotter and algebraic variants of CHSH, *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science* (ACM, 2015), pp. 123–132.

[19] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes Using Single D-Level Systems, Phys. Rev. Lett. **114**, 170502 (2015).

[20] J. Kaniewski, Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities, Phys. Rev. Lett. **117**, 070402 (2016).

[21] M. McKague, T. H. Yang, and V. Scarani, Robust self-testing of the singlet, J. Phys. A **45**, 455304 (2012).

[22] A. Coladangelo and J. Stark, Separation of finite and infinite-dimensional quantum correlations, with infinite question or answer sets, arXiv:1708.06522.

[23] W.-H. Zhang, G. Chen, X.-X. Peng, X.-J. Ye, P. Yin, Y. Xiao, Z.-B. Hou, Z.-D. Cheng, Y.-C. Wu, J.-S. Xu *et al.*, Experimentally robust self-testing for bipartite and tripartite entangled states, arXiv:1804.01375.