Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities

Jędrzej Kaniewski
Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark

(Received 12 May 2016; published 11 August 2016)

Self-testing refers to the phenomenon that certain extremal quantum correlations (almost) uniquely identify the quantum system under consideration. For instance, observing the maximal violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality certifies that the two parties share a singlet. While self-testing results are known for several classes of states, in many cases they are only applicable if the observed statistics are almost perfect, which makes them unsuitable for practical applications. Practically relevant self-testing bounds are much less common and moreover they all result from a single numerical method (with one exception which we discuss in detail). In this work we present a new technique for proving analytic self-testing bounds of practically relevant robustness. We obtain improved bounds for the case of self-testing the singlet using the CHSH inequality (in particular we show that nontrivial fidelity with the singlet can be achieved as long as the violation exceeds $\beta^* = (16 + 14\sqrt{2})/17 \approx 2.11$). In the case of self-testing the tripartite Greenberger-Horne-Zeilinger state using the Mermin inequality, we derive a bound which not only improves on previously known results but turns out to be tight. We discuss other scenarios to which our technique can be immediately applied.

DOI: 10.1103/PhysRevLett.117.070402

Introduction.—In 1964 John Bell showed that correlations resulting from any classical theory are restricted by certain constraints (now known as *Bell inequalities*) [1] and moreover that these might be violated by quantum systems. Nowadays Bell nonlocality is an active field with numerous applications [2]. One of the most striking consequences of Bell's theorem is the fact that the nonclassical nature of two (or more) devices can be verified by a classical user. If we, moreover, assume quantum mechanics to be the underlying theory, we find that certain extremal quantum correlations (almost) uniquely identify the state and measurements under consideration, a phenomenon known as *self-testing*. For instance, the maximal violation of the Clauser-Horne-Shimony-Holt (CHSH) [3] inequality necessarily implies that the two parties share a singlet (up to local unitaries). While this was already pointed out by Popescu and Rohrlich in 1992 [4], it was not widely known until the works of Mayers and Yao [5,6]. Since then, self-testing has received substantial attention and led to the concept of *device independence*, important in quantum cryptography [7–11] and beyond [12].

The central question in self-testing is: Given a conditional probability distribution arising from measuring a (multipartite) quantum state, what can be deduced about the state and/or the measurements?

Most previous research has focused on the problem of certifying the quantum state shared between the devices. Among others we can self-test the singlet [13], graph states [14], high-dimensional maximally entangled states [15,16] or nonmaximally entangled states of two qubits [17]. The common feature of these results is that the robustness is extremely weak; i.e., we can only make a nontrivial statement if the observed statistics are ε-close to the ideal case (for $\varepsilon \approx 10^{-4}$). Self-testing statements of practically relevant robustness turn out to be significantly harder to prove and are currently restricted to a single analytic result [18] and one numerical technique known as the "swap trick" [19,20]. The swap trick relies on explicitly constructing a circuit extracting the desired state into an extra register and using the hierarchy for quantum correlations [21,22] to place a lower bound on the resulting fidelity. This is a versatile tool for obtaining robust self-testing statements for various entangled states but since the computational cost grows rapidly with dimensionality, so far it has only been applied to quantum systems of small dimensions [19,20,23,24].

Self-testing of measurements has received significantly less attention. Popescu and Rohrlich showed that the CHSH inequality is violated maximally only if the observables anticommute (which corresponds to maximal incompatibility) [4]. McKague and Mosca showed how to certify more than two binary observables [25], Miller and Shi investigated which Bell inequalities are well-suited for self-testing [26], Bamps and Pironio showed that nonmaximally anticommuting observables can be self-tested using the tilted CHSH inequality [17], while Šupić *et al.* showed that all measurements lying in a single plane of the Bloch sphere can be self-tested through chained inequalities [27]. Nothing is known about certifying measurements with more than two outcomes.

Some recent works that present a slightly different focus consider, e.g., self-testing in parallel [28,29], producing a complete list of self-tests (within a particular Bell scenario) [30], or analyzing semi-device independent scenarios [31–33].

In this Letter we present a new technique for proving analytic self-testing statements for quantum states. In the simplest case of self-testing the singlet using the CHSH inequality, we obtain a linear bound which improves on all the previously known results. We also consider self-testing the tripartite Greenberger-Horne-Zeilinger (GHZ) state [34] using the Mermin inequality [35] which yields the first tight self-testing statement ("tight" in the sense explained below, which is unrelated to the facet character of the corresponding Bell inequality). Our technique hinges on the idea that measurement operators can be used to construct local extraction maps. This gives rise to a family of operators and placing a lower bound on the spectrum of these operators immediately yields a self-testing statement. The technique can be straightforwardly applied to any Werner-Wolf-Żukowski-Brukner inequality [36,37] (all Bell scenarios with two settings and two outcomes per party) and we believe it is also applicable to more general scenarios.

Methods.—Suppose that two parties, usually referred to as Alice and Bob, share some quantum state. If they had access to trusted measurement devices, they could perform tomography to deduce precisely what state they share. However, we consider a more restrictive scenario in which Alice and Bob only have access to untrusted measurement devices. In other words, their actions are limited to choosing the measurement setting and observing the outcome and hence the only information available to them is the conditional probability distribution (i.e., the probability of observing outputs a, b for inputs x, y). In this case one cannot hope to exactly identify the state shared by the devices: the two inherent limitations of self-testing are the inability to see local unitaries and the inability to detect auxiliary systems (on which the measurements act trivially). To formalize the problem we must therefore generalize the notion of Alice and Bob *sharing* a particular state. A natural solution is to require that they are capable of locally (without communication) *extracting* the desired state, which leads directly to a quantitative measure first proposed by Bardyn *et al.* [18]. Let the *target state* $|\Psi\rangle_{A'B'}$ be an arbitrary bipartite pure state (we assume all the subsystems to be finite-dimensional), $\Psi_{A'B'} = |\Psi\rangle\langle\Psi|_{A'B'}$ be the corresponding density matrix and $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ be the fidelity ($\|\cdots\|_1$ is the trace norm). For an arbitrary bipartite *input state* ρ_{AB} we define the *extractability* of $\Psi_{A'B'}$ from ρ_{AB} as

$$\Xi(\rho_{AB} \to \Psi_{A'B'}) \coloneqq \max_{\Lambda_A, \Lambda_B} F((\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}),$$

where the maximum is taken over all quantum channels (completely positive trace-preserving maps) of appropriate input and output registers. Note that this is equivalent to first adding local ancillary registers (in an arbitrary state) and then performing local unitaries which extract the desired state into these registers. The extractability is convex in the input state and invariant under local unitaries (applied to either the input or the target state). Note that Alice and Bob can choose to discard their shares and replace them with some fixed states, which transforms ρ_{AB} into an arbitrary product state. In particular this could be the product state corresponding to the largest Schmidt coefficient of $|\Psi_{A'B'}\rangle$ denoted by $\lambda_{\max}$, which implies that $\Xi(\rho_{AB} \to \Psi_{A'B'}) \geq \lambda_{\max}^2$ (in fact this turns out to be optimal whenever ρ_{AB} is separable [38]). Computing the extractability for an arbitrary pair of states seems to be a hard optimization problem because the set of product channels is not convex. This is not a major obstacle, since we do not intend to study the quantity itself but to investigate the trade-off between extractability and nonlocality. It is worth pointing out that finding the maximal violation of a fixed Bell inequality for a particular state is (for similar reasons) also believed to be hard [39], which suggests that the two problems might be closely related.

In a self-testing problem we are given a target state $\Psi_{A'B'}$ and a Bell inequality $\mathcal{B}$. Let β_C and β_Q be the maximal values of the inequality $\mathcal{B}$ achieved within the classical and quantum theories, respectively, and for simplicity we assume that $\Psi_{A'B'}$ achieves the maximal quantum violation. The extractability violation trade-off is captured by a function $\mathcal{Q}_{\Psi,\mathcal{B}} : [\beta_C, \beta_Q] \to [0, 1]$ defined as

$$\mathcal{Q}_{\Psi,\mathcal{B}}(\beta) \coloneqq \inf_{\rho_{AB} \in \mathcal{S}_{\mathcal{B}}(\beta)} \Xi(\rho_{AB} \to \Psi_{A'B'}),$$

where $\mathcal{S}_{\mathcal{B}}(\beta)$ is the set of bipartite states (of arbitrary dimension) that achieve the value of (at least) β on the inequality $\mathcal{B}$. This formulation is convenient as it (trivially) implies that an observed violation of β guarantees that the shared state ρ_{AB} satisfies

$$\Xi(\rho_{AB} \to \Psi_{A'B'}) \geq \mathcal{Q}_{\Psi,\mathcal{B}}(\beta),$$

which is precisely a self-testing statement.

The lower bound on the extractability (based on the Schmidt decomposition of $\Psi_{A'B'}$) implies a trivial lower bound on the trade-off function: $\mathcal{Q}_{\Psi,\mathcal{B}}(\beta) \geq \lambda_{\max}^2$ (trivial in the sense that it exhibits no β-dependence). To derive an upper bound on $\mathcal{Q}_{\Psi,\mathcal{B}}(\beta)$ for a particular value of β we write

$$\beta = p\beta_Q + (1 - p)\beta_C \tag{1}$$

for some $p \in [0, 1]$. Then we consider the state

$$\rho_{XYAB} \coloneqq p|00\rangle\langle 00|_{XY} \otimes \Psi_{AB} + (1-p)|11\rangle\langle 11|_{XY} \otimes \sigma_{AB} \tag{2}$$

where Ψ_{AB} is the target state (we choose the dimensions of the registers A, B to be the same as A', B'), σ_{AB} is an arbitrary separable state and we consider the $XA|YB$ partition. By construction, this state achieves the violation of β so it suffices to place an upper bound on the extractability. We first use convexity and then apply the trivial bound of unity for $|00\rangle\langle 00|_{XY} \otimes \Psi_{AB}$ and the separable bound $\lambda_{\max}^2$ for $|11\rangle\langle 11|_{XY} \otimes \sigma_{AB}$ to obtain

$$\Xi(\rho_{XYAB} \to \Psi_{AB}) \leq p + (1 - p)\lambda_{\max}^2. \tag{3}$$

Combining Eqs. (1) and (3) leads to

$$\mathcal{Q}_{\Psi,\mathcal{B}}(\beta) \le \lambda_{\max}^2 + (1-\lambda_{\max}^2)\frac{\beta-\beta_C}{\beta_Q-\beta_C}. \qquad (4)$$

While the definition of extractability generalizes to any number of parties, upper and lower bounds do not follow trivially. For instance, the optimal β-independent lower bound for a multipartite state (sometimes referred to as the *entanglement eigenvalue*) is only known for some special classes of states [40,41] (the general problem is known to be NP-hard [42]). Often nontrivial bounds can be obtained by grouping parties and thus reducing it to a bipartite scenario.

Self-testing from operator inequalities.—The only analytic self-testing result with practically relevant robustness is due to Bardyn *et al.* [18] and exploits the fact that local observables can be used to determine local unitaries that should be applied to each subsystem in order to extract the singlet. In the case of two binary observables per party, we can use Jordan's lemma (for a precise statement and a simple proof we refer the reader to Oded Regev's lecture notes [43]) to write the observables in a block-diagonal form with blocks of size at most 2×2. After the unitary correction each (nontrivial) block is fully characterized by the angle between the observables. The goal is to show that a high CHSH violation implies high fidelity of the rotated state with the singlet and the main challenge is to derive a bound which is *uniform*; i.e., it holds *for all angles* between the observables of Alice and Bob. (If the angles were publicly announced, then Alice and Bob would effectively share a two-qubit state for which better bounds have been proven [18]). In the current work we use these ideas to develop a new method for proving analytic self-testing bounds.

Our goal is to self-test the target state $\Psi_{A'B'}$ using a particular Bell inequality $\mathcal{B}$ and here we show how to obtain linear self-testing statements of the form

$$\mathcal{Q}_{\Psi,\mathcal{B}}(\beta) \ge s\beta + \mu \qquad (5)$$

for some real parameters $s, \mu \in \mathbb{R}$. The Bell operator of $\mathcal{B}$ is defined as

$$W := \sum_{\text{xyab}} c_{ab}^{xy} P_a^x \otimes Q_b^y,$$

where $c_{ab}^{xy} \in \mathbb{R}$ are real coefficients and $\{P_a^x\}_a$ is the measurement performed by Alice on input x (and similarly for Bob). Let Λ_A and Λ_B be local extraction channels constructed from the local observables. Since the fidelity with a pure state can be written as the Hilbert-Schmidt inner product, we have

$$F((\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}) = \langle(\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}\rangle.$$

For every map Λ, there exists the dual map $\Lambda^\dagger$, which satisfies $\langle \Lambda(X), Y\rangle = \langle X, \Lambda^\dagger(Y)\rangle$ for all linear operators X, Y. Thus we can rewrite the fidelity as $tr(K\rho_{AB})$ for

$$K := (\Lambda_A^\dagger \otimes \Lambda_B^\dagger)(\Psi_{A'B'}).$$

For a real constant $s > 0$ (to be chosen later) consider the operator $K - sW$ and suppose that $\mu \in \mathbb{R}$ is a lower bound on its spectrum or equivalently that the operator inequality

$$K \ge sW + \mu\mathbb{1} \qquad (6)$$

holds. Then computing the trace of this inequality with ρ_{AB} leads directly to

$$F((\Lambda_A \otimes \Lambda_B)(\rho_{AB}), \Psi_{A'B'}) \ge s\beta + \mu. \qquad (7)$$

Proving the operator inequality Eq. (6) for a *particular choice* of measurement operators implies that the bound Eq. (7) holds for all states ρ_{AB} for *that particular choice* of measurement operators. Proving that the operator inequality Eq. (6) holds *for all* possible measurement operators (of arbitrary dimension) implies that the inequality Eq. (7) holds *for all* quantum setups, which is precisely the meaning of inequality Eq. (5). Since the measurement operators might be of arbitrary dimension, the operator $K - sW$ is difficult to analyze in general. Fortunately the analysis simplifies significantly whenever Jordan's lemma can be applied.

Qubit extraction maps.—Without loss of generality we can assume that the measurement operators of Alice and Bob are projective and that all the Jordan blocks are nontrivial (see Section I of the Supplemental Material [44] for details). We propose extraction maps that respect the block structure of the observables (i.e., we only consider qubit-to-qubit channels) and we use identical maps for each party. In the first step we rotate each two-dimensional block so that the observables of Alice can be written as

$$A_r = \cos a\sigma_x + (-1)^r \sin a\sigma_z \qquad (8)$$

for $r \in \{0,1\}$ and some $a \in [0, \pi/2]$. The observables of Bob are defined in the same manner with the angle denoted by $b \in [0, \pi/2]$. It is crucial to realize that this covers *all possible choices* of observables. Thus if the operator inequality Eq. (6) holds for qubit observables for all pairs (a, b), then it also holds for arbitrary observables (see Section I of the Supplemental Material [44] for details). The second part of the extraction map is a dephasing channel

$$[\Lambda(x)](\rho) = \frac{1+g(x)}{2}\rho + \frac{1-g(x)}{2}\Gamma(x)\rho\Gamma(x), \qquad (9)$$

where x is the angle (i.e. $x = a$ for Alice and $x = b$ for Bob), $g(x) = (1+\sqrt{2})(\sin x + \cos x - 1)$ and

$$\Gamma(x) = \begin{cases} \sigma_x & \text{for } x \in [0, \pi/4], \\ \sigma_z & \text{for } x \in (\pi/4, \pi/2]. \end{cases}$$

It is easy to check that $g(0) = g(\pi/2) = 0$ (full dephasing for compatible observables) and $g(\pi/4) = 1$ (no dephasing for maximally incompatible observables). Having explicitly defined the extraction maps, let us now assess their performance in two concrete self-testing scenarios.

The CHSH inequality.—The CHSH operator reads

$$W(a,b) = \sum_{j,k\in\{0,1\}} (-1)^{jk} A_j \otimes B_k.$$

The optimal violation of $\beta_Q = 2\sqrt{2}$ is achieved only for $a = b = \pi/4$ and let us denote the optimal state (the eigenvector corresponding to the largest eigenvalue) by Φ_{AB} (equivalent to the singlet $(|01\rangle - |10\rangle)/\sqrt{2}$ up to local unitaries). If Alice and Bob apply the extraction map, Eq. (9), we obtain the operator $K(a,b) = (\Lambda(a) \otimes \Lambda(b))(\Phi_{AB})$ (the dephasing map is self-dual) for which we prove the following proposition.

Proposition 1: Let $s = (4 + 5\sqrt{2})/16$ and $\mu = -(1 + 2\sqrt{2})/4$. Then the operator inequality

$$K(a,b) \geq sW(a,b) + \mu \mathbb{1}$$

holds for all $a, b \in [0, \pi/2]$.

The proof of this proposition is one of the main technical contributions of this Letter and can be found in Section II. A of the Supplemental Material [44]. As an immediate corollary we find that

$$\mathcal{Q}_{\Phi_{AB},\mathcal{B}_{\mathrm{CHSH}}}(\beta) \geq \frac{1}{2} + \frac{1}{2} \cdot \frac{\beta - \beta^*}{2\sqrt{2} - \beta^*}, \qquad (10)$$

where $\beta^* = (16 + 14\sqrt{2}/17) \approx 2.11$ is the threshold violation (for which the bound becomes nontrivial). This result improves upon all previously known results and also follows closely the upper bound of Eq. (4) as shown in Fig. 1. As argued in Section III of the Supplemental Material [44], the upper bound is unachievable in the interior $\beta \in (2, 2\sqrt{2})$, which might be related to the fact that the quantum value of the CHSH inequality does not reach its algebraic limit of 4. It was known previously that nontrivial fidelity with the singlet can be achieved if the violation exceeds ≈ 2.37 [19], which we currently improve to $\beta^* \approx 2.11$.

The Mermin inequality.—The Mermin operator reads

$$W(a,b,c) = \sum_{j,k \in \{0,1\}} (-1)^{jk} A_j \otimes B_k \otimes C_{j \oplus k}$$

and the observables of Charlie are defined analogous to Eq. (8) with the angle denoted by $c \in [0, \pi/2]$. The optimal quantum violation of $\beta_Q = 4$ is achieved only for $a = b = c = \pi/4$ and let us denote the corresponding state by Υ_{ABC} (equivalent to the tripartite GHZ state $(|000\rangle + |111\rangle)/\sqrt{2}$ up to local unitaries). By considering any nontrivial bipartite cut it is easy to see that the optimal β-independent lower bound is $\mathcal{Q}_{\Upsilon_{ABC},\mathcal{B}_{\mathrm{Mermin}}} \geq \frac{1}{2}$. To derive an upper bound we make two observations: (i) the violation up to $\gamma^* \coloneqq 2\sqrt{2}$ can be achieved by the state $|\nu\rangle_{ABC} = |\Phi\rangle_{AB}|0\rangle_C$ (Alice and Bob employ the CHSH strategy, while Charlie outputs a fixed outcome) and (ii) with respect to the $AB|C$ cut, the state $|\nu\rangle_{ABC}$ is separable and the state Υ_{ABC} is equivalent to a singlet thus $\Xi(\nu_{ABC} \to \Upsilon_{A'B'C'}) = \frac{1}{2}$. From (i) and (ii) we immediately see that $\mathcal{Q}_{\Upsilon_{ABC},\mathcal{B}_{\mathrm{Mermin}}}(\gamma) = \frac{1}{2}$ for $\gamma \in [2, \gamma^*]$. By considering mixtures of Υ_{ABC} and ν_{ABC} analogous to the state Eq. (2) we conclude that

$$\mathcal{Q}_{\Upsilon_{ABC},\mathcal{B}_{\mathrm{Mermin}}}(\gamma) \leq \frac{1}{2} + \frac{1}{2} \cdot \frac{\gamma - \gamma^*}{4 - \gamma^*} \qquad (11)$$

for $\gamma \in [\gamma^*, 4]$. To derive a nontrivial lower bound we choose the same extraction map, Eq. (9), for all three parties. This leads to $K(a,b,c) = (\Lambda(a) \otimes \Lambda(b) \otimes \Lambda(c))(\Upsilon_{ABC})$ for which we prove the following proposition (see Section II. B of the Supplemental Material [44]).

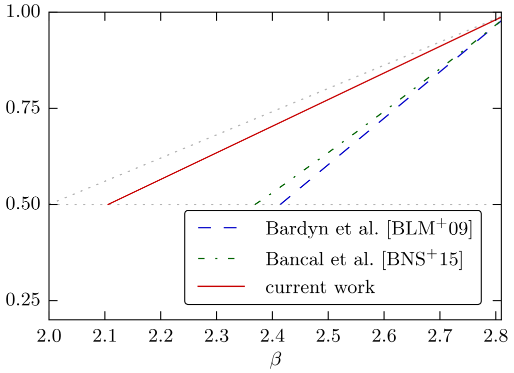

FIG. 1. Comparison of lower bounds on $\mathcal{Q}_{\Phi_{AB},\mathcal{B}_{\mathrm{CHSH}}}$. The gray dotted lines correspond to the trivial lower bound and the (unachievable) upper bound.

Proposition 2: Let $s = (2 + \sqrt{2})/8$ and $\mu = -1/\sqrt{2}$. Then the operator inequality

$$K(a,b,c) \geq sW(a,b,c) + \mu \mathbb{1}$$

holds for all $a, b, c \in [0, \pi/2]$.

The resulting lower bound matches exactly the upper bound [Eq. (11)], which implies that

$$\mathcal{Q}_{\Upsilon_{ABC},\mathcal{B}_{\mathrm{Mermin}}}(\gamma) = \frac{1}{2} + \frac{1}{2} \cdot \frac{\gamma - \gamma^*}{4 - \gamma^*}. \qquad (12)$$

It is worth pointing out that this constitutes the first self-testing statement which is provably tight. Comparison with the previously known bound is shown in Fig. 2.

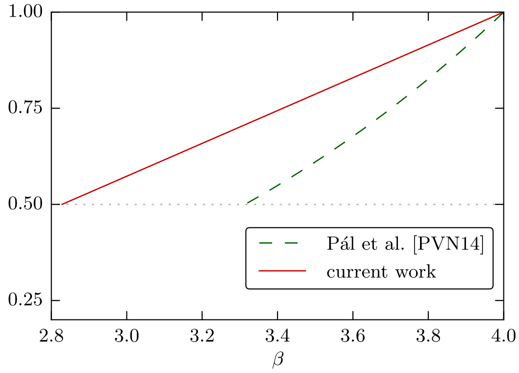

FIG. 2. Comparison of the previously known lower bound with the exact value of $\mathcal{Q}_{\Upsilon_{ABC},\mathcal{B}_{\mathrm{Mermin}}}$ derived in this work. The gray dotted line corresponds to the trivial lower bound.

Conclusions.—We have presented a new technique for proving self-testing statements which relies on: (i) understanding how to construct extraction channels from measurement operators and (ii) analyzing the resulting operator. We construct qubit extraction maps from two binary observables and derive analytic self-testing bounds for the CHSH and Mermin inequalities, which improve on previously known results.

To demonstrate the importance of these improvements consider the recent loophole-free Bell experiments [45,46], which report the CHSH value of $\beta \approx 2.4$. In this case the previous results yield the singlet fidelity of (at least) 0.53 [19], which only slightly exceeds the trivial value of $\frac{1}{2}$. In contrast, our results guarantee that the singlet fidelity is at least 0.70, which constitutes a significant improvement. This can be used to obtain a lower bound on the distillable entanglement of the unknown state: we first perform local extraction and then distill entanglement from the resulting two-qubit state using standard procedures [47].

An immediate follow-up problem is to certify the n-partite GHZ state using one of the Werner-Wolf-Żukowski-Brukner inequalities [36,37]. For a fixed inequality our approach leads to an explicit family of operators and it suffices to place a lower bound on their spectrum, which makes the problem purely technical. Alternatively, one could consider generalizations of the CHSH inequality [15,48] with more than two settings per party. These inequalities might lead to robust self-testing of (bipartite) high-dimensional maximally entangled states. Finally, one might attempt to construct extraction maps from measurements with more than two outcomes, e.g., for the Collins-Gisin-Linden-Massar-Popescu inequalities [49].

We would like to thank Jean-Daniel Bancal, Chris Majenz, Matthew McKague, Alexander Müller-Hermes, Chris Perry, and Marco Tomamichel for comments on an earlier version of this draft. We are grateful to Jean-Daniel Bancal and Tamás Vértesi for sharing their numerical data. We acknowledge stimulating discussions with Matthias Christandl, David Elkouss, Roberto Ferrara, Laura Mančinska, Marcin Pawłowski, Filip Rozpędek, and Valerio Scarani. Most importantly we thank Alessandro Bruno for inspiring discussions on decoherence. We acknowledge financial support from the European Research Council (ERC Grant Agreement No. 337603), the Danish Council for Independent Research (Sapere Aude) and the Swiss National Science Foundation (Project No. PP00P2_150734).

[1] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, Physics **1**, 195 (1964).

[2] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 1969.

[4] S. Popescu and D. Rohrlich, Which states violate Bell's inequality maximally?, Phys. Lett. A **169**, 411 (1992).

[5] D. Mayers and A. C.-C. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, 1998* (IEEE, New York, 1998).

[6] D. Mayers and A. C.-C. Yao, Self testing quantum apparatus, Quantum Inf. Comput. **4**, 273 (2004).

[7] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography Against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[8] A. Acín, N. Gisin, and L. Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. **97**, 120405 (2006).

[9] J. Barrett, L. Hardy, and A. Kent, No Signaling and Quantum Key Distribution, Phys. Rev. Lett. **95**, 010503 (2005).

[10] R. Colbeck, Ph.D. thesis, University of Cambridge, 2006.

[11] R. Colbeck and A. Kent, Private randomness expansion with untrusted devices, J. Phys. A **44**, 095305 (2011).

[12] V. Scarani, The device-independent outlook on quantum physics, Acta Phys. Slovaca **62**, 347 (2012).

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

[14] M. McKague, Self-testing graph states, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science Vol. 6745 (Springer, Berlin Heidelberg, 2014), pp. 104–120.

[15] W. Slofstra, Lower bounds on the entanglement needed to play XOR non-local games, J. Math. Phys. (N.Y.) **52**, 102202 (2011).

[16] T. H. Yang and M. Navascués, Robust self-testing of unknown quantum systems into any entangled two-qubit states, Phys. Rev. A **87**, 050102 (2013).

[17] C. Bamps and S. Pironio, Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing, Phys. Rev. A **91**, 052111 (2015).

[18] C. E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, Device-independent state estimation based on Bell's inequalities, Phys. Rev. A **80**, 062327 (2009).

[19] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Physical characterization of quantum devices from nonlocal correlations, Phys. Rev. A **91**, 022115 (2015).

[20] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Robust and Versatile Black-Box Certification of Quantum Devices, Phys. Rev. Lett. **113**, 040401 (2014).

[21] A. C. Doherty, Y.-C. Liang, B. F. Toner, and S. Wehner, *Proceedings IEEE Computational Complexity '08* (IEEE, New York, 2008).

[22] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, Phys. Rev. Lett. **98**, 010401 (2007).

[23] K. F. Pál, T. Vértesi, and M. Navascués, Device-independent tomography of multipartite quantum states, Phys. Rev. A **90**, 042340 (2014).

[24] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, Robust self-testing of the three-qubit W state, Phys. Rev. A **90**, 042339 (2014).

[25] M. McKague and M. Mosca, *Proceedings TQC '10, LNCS, 6519, 2011* (Springer-Verlag, Berlin, 2011).

[26] C. A. Miller and Y. Shi, Optimal robust quantum self-testing by binary nonlocal XOR games, arXiv:1207.1819.

[27] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, Self-testing protocols based on the chained Bell inequalities, New J. Phys. **18**, 035013 (2016).

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

[29] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, Device-independent parallel self-testing of two singlets, Phys. Rev. A **93**, 062121 (2016).

[30] Y. Wang, X. Wu, and V. Scarani, All the self-testings of the singlet for two binary measurements, New J. Phys. **18**, 025021 (2016).

[31] A. Gheorghiu, P. Wallden, and E. Kashefi, Rigidity of quantum steering and one-sided device-independent verifiable quantum computation, arXiv:1512.07401.

[32] K. T. Goh, J.-D. Bancal, and V. Scarani, Measurement-device-independent quantification of entanglement for given Hilbert space dimension, New J. Phys. **18**, 045022 (2016).

[33] I. Šupić and M. J. Hoban, Self-testing through EPR-steering, New J. Phys. **18**, 075006 (2016).

[34] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), pp. 69–72.

[35] N. D. Mermin, Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct State, Phys. Rev. Lett. **65**, 1838 (1990).

[36] R. F. Werner and M. M. Wolf, All multipartite Bell correlation inequalities for two dichotomic observables per site, Phys. Rev. A **64**, 032112 (2001).

[37] M. Żukowski and Č. Brukner, Bell's Theorem for General N-Qubit States, Phys. Rev. Lett. **88**, 210401 (2002).

[38] A. Shimony, Degree of entanglement, Ann. N.Y. Acad. Sci. **755**, 675 (1995).

[39] Y.-C. Liang and A. C. Doherty, Bounds on quantum correlations in Bell-inequality experiments, Phys. Rev. A **75**, 042103 (2007).

[40] H. N. Barnum and N. Linden, Monotones and invariants for multi-particle quantum states, J. Phys. A **34**, 6787 (2001).

[41] T.-C. Wei and P. M. Goldbart, Geometric measure of entanglement and applications to bipartite and multipartite quantum states, Phys. Rev. A **68**, 042307 (2003).

[42] C. J. Hillar and L.-H. Lim, Most tensor problems are NP-hard, J. ACM **60**, 45 (2013).

[43] O. Regev, Quantum Computation (lecture notes), 2006; http://www.cims.nyu.edu/~regev/teaching/quantum_fall_2005/ln/qma.pdf.

[44] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.117.070402 for detailed derivations of the results presented in the Letter.

[45] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twichen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature (London) **526**, 682 (2015).

[46] B. Hensen, N. Kalb, M. S. Blok, A. E. Dréau, A. Reiserer, R. F. L. Vermeulen, R. N. Schouten, M. Markham, D. J. Twitchen, K. Goodenough, D. Elkouss, S. Wehner, T. H. Taminiau, R. Hanson, T. H. Taminiau, and R. Hanson, Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis, arXiv:1603.05705.

[47] W. Dür and H. J. Briegel, Entanglement purification and quantum error correction, Rep. Prog. Phys. **70**, 1381 (2007).

[48] J. Oppenheim and S. Wehner, The uncertainty principle determines the nonlocality of quantum mechanics, Science **330**, 1072 (2010).

[49] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Bell Inequalities for Arbitrarily High-Dimensional Systems, Phys. Rev. Lett. **88**, 040404 (2002).