ARTICLE OPEN

Self-testing quantum systems of arbitrary local dimension with minimal number of measurements

Shubhayan Sarkar^{1✉}, Debashis Saha¹, Jędrzej Kaniewski² and Remigiusz Augusiak¹

Bell nonlocality as a resource for device-independent certification schemes has been studied extensively in recent years. The strongest form of device-independent certification is referred to as self-testing, which given a device, certifies the promised quantum state as well as quantum measurements performed on it without any knowledge of the internal workings of the device. In spite of various results on self-testing protocols, it remains a highly nontrivial problem to propose a certification scheme of qudit–qudit entangled states based on violation of a single d -outcome Bell inequality. Here we address this problem and propose a self-testing protocol for the maximally entangled state of any local dimension using the minimum number of measurements possible, i.e., two per subsystem. Our self-testing result can be used to establish unbounded randomness expansion, $\log_2 d$ perfect random bits, while it requires only one random bit to encode the measurement choice.

npj Quantum Information (2021)7:151; <https://doi.org/10.1038/s41534-021-00490-3>

INTRODUCTION

The advent of quantum theory has not just changed the understanding of physics but has also given rise to new phenomena that would have never been possible in the classical world. Arguably, one of the most interesting features of quantum theory is the existence of quantum correlations, which cannot be explained by any local hidden-variable model, a phenomenon commonly referred to as Bell nonlocality^{1,2}. It has been understood that apart from its fundamental significance, nonlocality is a powerful resource for certain device-independent applications such as quantum cryptography³, randomness generation^{4,5}, or, more recently, for device-independent certification methods^{3–6}.

The strength of the device-independent (DI) certification methods lies in the fact that given an unknown quantum system, one can make nontrivial statements on some of its key features based solely on the nonlocal correlations obtained from it. They are advantageous over standard certification methods such as those based on quantum tomography (cf. Ref.⁷) because they do not require making assumptions on the system under study, apart from that, it is governed by quantum mechanics. An example of such a DI-certification scheme would be verifying whether a quantum device produces entanglement⁸ or certification of the dimension of a quantum system⁹, both based on a violation of some Bell inequality by the corresponding quantum system.

The strongest form of DI certification is self-testing. First introduced in⁶, it allows one to provide a full description, up to certain well-understood equivalences, of the considered quantum system and also the measurements performed on it based on observing the maximal violation of some Bell inequality. Such a form of certification is particularly interesting from the application point of view as it provides a way of verifying that a given quantum device functions properly without the need of knowing its internal working.

A lot of attention has thus been devoted to proposing self-testing schemes for entangled quantum states^{10–14}. However, most of the obtained results focus on states that are locally qubits, such as, for instance, the self-testing statement for any two-qubit

entangled state^{11,12} based on a violation of the tilted version of the famous Clauser–Horne–Shimony–Holt (CHSH) Bell inequality^{15,16}. At the same time, quantum systems of higher local dimension remain mostly unexplored and, in fact, few results are devoted to them^{11,17–19}. In particular, in Ref.¹⁷, the two-qubit results^{11,12} were combined to design a self-testing protocol for any entangled state of arbitrary local dimension. Still, these results are based on a violation of many two–outcome Bell inequalities and the question whether one can design a self-testing statement for qudit quantum systems relying on violation of a single and truly d -outcome Bell inequality remains open. Moreover, the self-testing statement of Refs.^{11,17} is not optimal in terms of the number of measurements that the observers need to perform (three and four, respectively) to certify the state and the corresponding measurements. Taking into account the possibility of experimental implementations of self-testing, it is a highly relevant question whether alternative protocols can be derived, which rely on the minimal number of two measurements per observer.

The main aim of this work is to address the above questions. We provide a self-testing statement for a maximally entangled state of local dimension d :

$$|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle \quad (1)$$

from a violation of a truly d -outcome Bell inequality exploiting the minimal possible number of measurements per party, which is two. To this end, we use the Bell inequality introduced in Ref.²⁰ as a generalization of the well-known CHSH Bell inequality to d -outcome Bell scenarios. A straightforward implication of our self-testing statement is a novel and simpler, as compared with the previous approaches^{21,22}, scheme for parallel self-testing of N copies of the two-qubit maximally entangled state $|\phi_2^+\rangle$. Another implication is that the outcomes of local measurements maximally violating the respective Bell inequality are perfectly random, which allows us to propose a quantum protocol for unbounded expansion of quantum randomness.

¹Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland. ²Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warsaw, Poland. ✉email: sarkar@cft.edu.pl

RESULTS

Preliminaries

Before presenting our results, let us set up the scenario and introduce the relevant notions.

Bell scenario. The simplest experimental setup exhibiting quantum nonlocality, namely, the bipartite Bell setup, comprises one preparation and two measurement devices. The latter are possessed by distant and noncommunicating parties, Alice and Bob, and can in general perform one of m measurements, denoted by M_x and N_y with $x, y = 1, \dots, m$. In each run of the experiment, a bipartite quantum system ρ_{AB} is prepared by the preparation device and subsequently each measurement device performs a measurement on one of its subsystems, yielding an outcome a and b , respectively, with $a, b \in \{0, \dots, d-1\}$.

Correlations obtained in this experiment are captured by a vector of probability distributions

$$\mathbf{p} = \{p(a, b|x, y)\} \in \mathbb{R}^{(md)^2}. \quad (2)$$

Here, $p(a, b|x, y)$ is the probability of obtaining outcomes a and b by Alice and Bob after performing measurements M_x and N_y , respectively, and it is given by the well-known formula

$$p(a, b|x, y) = \text{Tr}[\rho_{AB}(M_x^{(a)} \otimes N_y^{(b)})], \quad (3)$$

where $M_x^{(a)}$ and $N_y^{(b)}$ are the measurement operators defining the measurements M_x and N_y , respectively. In what follows, we also refer to the vector $\mathbf{p}$ as correlations.

In a fixed Bell scenario with md -outcome measurements, such quantum correlations, that is, those obtained by performing local measurements on composite quantum systems, form a convex set $\mathcal{Q}$. For further purposes, it is important to recall that any point $\mathbf{p} \in \mathcal{Q}$ can be achieved with a pure state $|\psi_{AB}\rangle$, whose local dimensions might in general be higher than those of ρ_{AB} , and projective measurements $M_x = \{P_x^{(a)}\}$ and $N_y = \{Q_y^{(b)}\}$.

It turns out that the quantum set $\mathcal{Q}$ contains correlations that even if obtained from a quantum state, can be simulated by Alice and Bob in a purely classical way. Such correlations are said to admit a local-realistic description, and for brevity, we refer to them as local or classical. More formally, local correlations are those for which $p(a, b|x, y)$ can be represented as a convex combination of product-deterministic correlations

$$p(a, b|x, y) = \sum_{\lambda} \mu(\lambda) p(a|x, \lambda) p(b|y, \lambda), \quad (4)$$

where λ is a random variable distributed according to a distribution $\mu(\lambda)$ and $p(a|x, \lambda), p(b|y, \lambda) \in \{0, 1\}$ for every x, y, a, b . For any m and d , such local correlations form a convex polytope that we denote $\mathcal{L}$.

Bell inequalities. As proven by Bell, the local set $\mathcal{L}$ is a proper subset of $\mathcal{Q}$ ¹ and those quantum points that are outside $\mathcal{L}$ are termed nonlocal. The most natural way to show that a given point $\mathbf{p} \in \mathcal{Q}$ is not an element of $\mathcal{L}$, is to use Bell inequalities. Recall their generic form to be

$$\mathcal{I} := \mathbf{t} \cdot \mathbf{p} \leq \beta_L, \quad (5)$$

where $\mathbf{t} = \{t_{abxy}\}$ is a collection of some real coefficients t_{abxy} and $\beta_L = \max_{\mathbf{p} \in \mathcal{L}} \mathcal{I}$ is the local bound of inequality (5). Analogously, the quantum or the Tsirelson bound of (5) is defined as $\beta_Q = \sup_{\mathbf{p} \in \mathcal{Q}} \mathcal{I}$.

Clearly, violation of a Bell inequality by correlation $\mathbf{p}$ implies that it is nonlocal. Moreover, any point $\mathbf{p}$ violating maximally some Bell inequality (or, equivalently, achieving its Tsirelson bound) necessarily belongs to the boundary of the quantum set $\mathcal{Q}$.

Correlation picture. Let us finally notice that it is often beneficial to describe correlations obtained in the Bell experiment by

expectation values instead of probability distributions. A convenient way to do so in Bell scenarios involving d -outcome measurements is to consider the two-dimensional Fourier transform of the conditional probabilities $p(a, b|x, y)$

$$\langle A_x^{(k)} B_y^{(l)} \rangle = \sum_{a, b=0}^{d-1} \omega^{ak+bl} p(a, b|x, y), \quad (6)$$

where ω is the d th root of unity $\omega = \exp(2\pi i/d)$ and $k, l = 0, \dots, d-1$. Importantly, for any quantum point $\mathbf{p}$, the expectation values (6) can be represented as $\langle A_x^{(k)} B_y^{(l)} \rangle = \langle \psi_{AB} | A_x^{(k)} \otimes B_y^{(l)} | \psi_{AB} \rangle$ with $\{A_x^{(k)}\}$ and $\{B_y^{(l)}\}$ being collections of unitary operators with eigenvalues $\omega^i (i = 0, \dots, d-1)$ defined as the Fourier transforms of the corresponding projective measurements

$$A_x^{(k)} = \sum_{a=0}^{d-1} \omega^{ak} P_x^{(a)}, \quad B_y^{(l)} = \sum_{b=0}^{d-1} \omega^{bl} Q_y^{(b)}. \quad (7)$$

It is not difficult to see that $A_x^{(k)}$ is simply the k th power of A_x (and similarly for Bob's operators), and thus, in what follows, we simply write A_x^k . In this correlator picture, the unitary operators A_x and B_y are d -outcome observables measured in the Bell setup.

Self-testing. We are now ready to present our main result: the self-testing statement for the two-qudit maximally entangled state and certain d -outcome measurements usually referred to as Collins–Gisin–Linden–Massar–Popescu (CGLMP) measurements^{23–25} (see Supplementary Methods for their explicit form).

To recall the task of self-testing, or more generally, DI certification, let us consider a quantum device performing a Bell experiment on some state $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ with some quantum d -outcome observables A_x and B_y , where the dimensions of the $\mathcal{H}_A$ and $\mathcal{H}_B$ are unknown but finite. The only information accessible to the user about how this device functions is the observed correlation $\mathbf{p}$. The aim of DI certification is to reveal the form of the state and observables from violation of some Bell inequality by $\mathbf{p}$ (given that the observed correlations violate some Bell inequality). However, there are two degrees of freedom, which can never be detected from the observed statistics. One is the set of local unitaries U_A, U_B that act on $\mathcal{H}_A, \mathcal{H}_B$, that is, the state $U_A \otimes U_B |\psi_{AB}\rangle$ together with $\{U_A A_x U_A^\dagger\}, \{U_B B_y U_B^\dagger\}$ will generate the same $\mathbf{p}$. Another one is the presence of an auxiliary system on which the measurements act trivially. A particular instance of such DI certification, termed self-testing, infers a unique state and two sets of unique measurements up to these equivalences.

Clearly, a necessary condition to derive an exact self-testing statement for a state and measurements is that the obtained correlation $\mathbf{p}$ lies on the boundary of $\mathcal{Q}$, and thus violates some Bell inequality maximally. Consequently, in order to derive a self-testing statement for $|\phi_d^+\rangle$ for any d , the first task is to identify a class of Bell inequalities in the bipartite scenario with the minimum number of measurements for which β_Q is achieved by it for any d . The only known Bell inequality meeting these requirements is the Salavrakos–Augusiak–Tura–Wittek–Acín–Pironio (SATWAP) Bell inequality²⁰, which in the correlator picture reads

$$\mathcal{I}_d := \sum_{k=1}^{d-1} (a_k \langle A_1^k B_1^{d-k} \rangle + a_k^* \omega^k \langle A_1^k B_2^{d-k} \rangle + a_k^* \langle A_2^k B_1^{d-k} \rangle + a_k \langle A_2^k B_2^{d-k} \rangle) \leq \beta_L, \quad (8)$$

where $a_k = (1 - i)\omega^{k/4}/2$ and the classical value is given by $\beta_L = (1/2)[3 \cot(\pi/4d) - \cot(3\pi/4d)] - 2$.

As proven in Ref.²⁰, the maximal quantum value of this inequality is $\beta_Q = 2(d-1)$ and it is achieved by the maximally entangled state of two qudits $|\phi_d^+\rangle$ and the aforementioned optimal CGLMP measurements (cf. Supplementary Methods). In what follows, we show that this is in fact the only quantum system,

Fig. 1 The self-testing scenario. Alice and Bob receive an unknown quantum system from the preparation device. They have two input buttons, each denoted by 1, 2 specifying two different measurements that they choose at random. The measurements point at one, out of the d outcomes denoted by $\{0, 1, \dots, d-1\}$. Alice and Bob repeat the experiment to collect statistics. They compare their statistics and find the joint probability distribution for different outcomes and measurements denoted by $p(a, b|x, y)$. From the statistics, we self-test the maximally entangled state (1) and two pairs of d -outcome measurements (10, 11).

up to additional freedoms as discussed above, realizing the maximal quantum violation of inequality (8) (Fig. 1).

Self-testing of maximally entangled state of arbitrary local dimension

Let us first introduce $Z_d = \text{diag}[1, \omega, \dots, \omega^{d-1}]$ to be the d -dimensional generalization of the σ_z -Pauli matrix in the standard basis and T_d to be the following matrix:

$$T_d = \sum_{i=0}^{d-1} \omega^{i+\frac{1}{2}} |i\rangle \langle i| - \frac{2}{d} \sum_{i,j=0}^{d-1} (-1)^{\delta_{i,0}+\delta_{j,0}} \omega^{\frac{i+j+1}{2}} |i\rangle \langle j|, \quad (9)$$

where δ_{ij} is the Kronecker delta: $\delta_{ij}=1$ for $i=j$ and $\delta_{ij}=0$ otherwise. It is not difficult to see that both matrices are unitary and have eigenvalues $\omega^i (i=0, \dots, d-1)$ (see Supplementary Methods) and thus represent d -outcome quantum observables.

Now, we can state our main theorem.

Theorem 1. Assume that the SATWAP Bell inequality (8) is maximally violated by a state $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and unitary observables $A_x, B_y (x \in \{1, 2\})$. Then, for any d , $\mathcal{H}_A = \mathbb{C}^d \otimes \mathcal{H}_{A'}$ as well as $\mathcal{H}_B = \mathbb{C}^d \otimes \mathcal{H}_{B'}$ with some auxiliary Hilbert spaces $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ of unknown but finite dimensions. Moreover, there exist local unitary transformations $U_A : \mathbb{C}^d \otimes \mathcal{H}_{A'} \rightarrow \mathbb{C}^d \otimes \mathcal{H}_A$ and $U_B : \mathbb{C}^d \otimes \mathcal{H}_{B'} \rightarrow \mathbb{C}^d \otimes \mathcal{H}_B$, such that

$$U_B B_1 U_B^\dagger = Z_d \otimes \mathbb{1}_{B'}, \quad U_B B_2 U_B^\dagger = T_d \otimes \mathbb{1}_{B'}, \quad (10)$$

and

$$\begin{aligned} U_A A_1 U_A^\dagger &= (a_1^* Z_d + 2(a_1^*)^3 T_d) \otimes \mathbb{1}_{A'}, \\ U_A A_2 U_A^\dagger &= (a_1 Z_d - a_1^* T_d) \otimes \mathbb{1}_{A'}, \end{aligned} \quad (11)$$

where $a_1 = (1 + i)\omega^{1/4}/2$, Z_d and T_d are defined above, and $\mathbb{1}_{A'}, \mathbb{1}_{B'}$ are identity matrices acting on $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$. Finally, the state $|\psi_{AB}\rangle$ is equivalent to $|\phi_d^+\rangle$ in the following sense:

$$U_A \otimes U_B |\psi_{AB}\rangle = |\phi_d^+\rangle \otimes |\text{aux}_{A'B'}\rangle, \quad (12)$$

where $|\text{aux}_{A'B'}\rangle$ is some auxiliary state from $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$.

Before proving this theorem, a few comments are in order. First, as proven in Supplementary Methods, the observables Z_d and T_d are unitarily equivalent to the CGLMP measurements. Second, our self-testing statement exploits a single Bell inequality involving the minimal number of two measurements per observer for which one can observe nonlocality in quantum systems. The number of local observables one needs to measure in order to self-test a state is of key importance from the application point of view. Finally, in the case of $d = 2^N$, the theorem implies a parallel self-testing protocol for $|\phi_2^+\rangle^{\otimes N}$, i.e., N copies of maximally two-qubit entangled state (see Refs. 21,22 for the previous approaches).

Proof. The proof is quite technical and thus is deferred to the Supplemental Information (cf. Supplementary Methods). Here we only sketch its main ingredients. Let a state $|\psi_{AB}\rangle$ and observables A_x and B_y maximally violate the SATWAP Bell inequality. Without loss of generality, we can assume that the reduced states of $|\psi_{AB}\rangle$ are full rank. Exploiting the sum-of-squares decomposition of the corresponding Bell operator, we can establish that Alice's and Bob's observables satisfy

$$\text{Tr}(A_x^n) = \text{Tr}(B_y^n) = 0 \quad (13)$$

for $x, y = 1, 2$ and any $n < d$, which is a divisor of the number of outcomes d . These conditions imply that the multiplicities of the eigenvalues of all the observables A_x and B_y are equal, which has two consequences. First, their matrix dimensions are a multiple of d , meaning that they act on, respectively, $\mathcal{H}_A = \mathbb{C}^d \otimes \mathcal{H}_{A'}$ and $\mathcal{H}_B = \mathbb{C}^d \otimes \mathcal{H}_{B'}$ with $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ being some auxiliary Hilbert spaces of unknown but finite dimensions. Second, there exist unitary operations $U_A : \mathcal{H}_A \rightarrow \mathcal{H}_A$ and $U_B : \mathcal{H}_B \rightarrow \mathcal{H}_B$ which allow us to bring Alice's and Bob's observables to the form given in Eqs. (10) and (11).

Finally, to obtain an analogous statement for the state we again employ the sum-of-squares decomposition, which in virtue of relations (10) and (11), imposes the following conditions on the state $|\psi\rangle_{AB}$:

$$\begin{aligned} [(Z_d^*)^k \otimes Z_d^k \otimes \mathbb{1}_{A'B'}] \hat{\psi}_{AB} &= |\hat{\psi}_{AB}\rangle, \\ [(T_d^*)^k \otimes T_d^k \otimes \mathbb{1}_{A'B'}] \hat{\psi}_{AB} &= |\hat{\psi}_{AB}\rangle, \end{aligned} \quad (14)$$

where we have denoted $|\psi_{AB}\rangle = U_A \otimes U_B |\psi_{AB}\rangle$. These conditions can easily be solved, leading to Eq. (12), which completes the proof. $\square$

Applications to randomness expansion

An interesting application of our self-testing statement is DI randomness certification⁵. Let us consider the distrustful scenario where one of the observers performing the Bell test, say Bob, wants to generate random bits from the outcomes of his measurements, and Eve who supplies the measurement devices wants to access that outcome.

We show with the aid of the above self-testing result that the maximal violation of the SATWAP Bell inequality certifies $\log_2 d$ bits of perfect randomness in the outcomes of Alice's and Bob's measurements. Without loss of generality, we can focus on Bob's measurements. One quantifies the randomness obtained in a Bell experiment as $-\log_2 G(x, \mathbf{p})$, where $G(x, \mathbf{p})$ is the local guessing probability defined through the following formula:

$$G(y, \mathbf{p}) = \sup_{S_p} \sum_b \langle \psi_{ABE} | 1 \otimes Q_y^{(b)} \otimes E^{(b)} | \psi_{ABE} \rangle, \quad (15)$$

where $|\psi_{ABE}\rangle$ is a three-partite state shared by Alice, Bob, and Eve, $\{Q_y^{(b)}\}$ is a projective measurement performed by Bob, and $E = \{E^{(c)}\}$ is a d -outcome measurement on $\mathcal{H}_E$ whose result is Eve's best guess of Bob's outcome. Finally, S_p is the set of all possible strategies that Eve implements to guess the outcome of Bob's measurements, consisting of the state $|\psi_{ABE}\rangle$ and the measurement E , which reproduce the correlation $\mathbf{p}$ observed by Alice and Bob, i.e.,

$$p(a, b|x, y) = \langle \psi_{ABE} | P_x^{(a)} \otimes Q_y^{(b)} \otimes 1_E | \psi_{ABE} \rangle. \quad (16)$$

Assume now that inequality (8) is maximally violated by $\mathbf{p}$. This means that, up to local unitary operations, $|\psi_{ABE}\rangle = |\phi_d^+\rangle |aux_{A'B'E}\rangle$ as well as $P_x^{(a)} = \bar{P}_x^{(a)} \otimes 1_{A'}$ and $Q_y^{(b)} = \bar{Q}_y^{(b)} \otimes 1_{B'}$, where $\bar{P}_x^{(a)}$ and $\bar{Q}_y^{(b)}$ are eigenprojectors of the observables in Eqs. (10) and (11), respectively. Taking all this into account along with the fact that Bob's observables are traceless, one finally finds that $G(y, \mathbf{p}) = 1/d$.

Thus, $-\log_2 G(x, \mathbf{p}) = \log_2 d$ bits of randomness can be certified using our self-testing statement. This is the maximum randomness that could be extracted from a system of local dimension d , whereas it requires one bit of randomness to encode the inputs. This gives rise to unbounded randomness expansion as d can be arbitrarily large.

DISCUSSIONS

We propose a self-testing statement for quantum system of arbitrary local dimension that unlike the previous approaches^{11,17} does not rely on self-testing results for qubit states and exploits a truly d -outcome Bell inequality. Moreover, our self-testing result exploits only two measurements per party, which is the minimal number allowing the parties to observe nonlocal correlations. This makes our results interesting from the experimental point of view. In fact, violation of the SATWAP Bell inequality has already been experimentally tested in Ref. ²⁶.

Several follow-up questions arise from our work. The robustness of the above self-testing statement has been previously studied numerically in²⁰ for local dimension three. However, there does not exist any analytical method for deriving robustness bounds for local dimension greater than two. Finding a general methodology for deriving analytical robustness bounds for any arbitrary local dimension and then comparing it to that of the scheme of^{11,17} could be an interesting follow-up question. Another interesting direction is to explore whether the d -outcome SATWAP Bell inequality can be modified to be maximally violated by a partially entangled state and whether the resulting modifications can be used to make self-testing statements for those states, again with the minimal number of measurements per observer. Finally, it is

also interesting to investigate whether, analogously to Refs. ^{27,28}, our self-testing statement can be used to establish certification of the optimal amount of $2\log_2 d$ bits of local or global randomness from the maximally entangled state of two qudits with the aid of a local POVM or two projective measurements, respectively. From a more general perspective, our self-testing result might provide nontrivial insights into the structure of the set of quantum correlations along the lines of²⁹, or might find applications in delegated quantum computation³⁰.

Note added—While working on this project, we became aware of the work³¹ exploring parallel self-testing with minimal number of measurements.

DATA AVAILABILITY

No data set was generated or analyzed in the current study.

CODE AVAILABILITY

No codes were generated or used in the current study.

Received: 30 April 2021; Accepted: 22 September 2021;

Published online: 14 October 2021

REFERENCES

1. Bell, J. S. On the Einstein Podolsky Rosen paradox. *Physics* **1**, 195 (1964).
2. Bell, J. S. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.* **38**, 447 (1966).
3. Acín, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
4. Colbeck, R. & Renner, R. No extension of quantum theory can have improved predictive power. *Nat. Commun.* **2**, 411 (2011).
5. Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
6. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus, Proceedings 39th Annual Symposium on Foundations of Computer Science (FOCS), 503 (IEEE, 1998) <https://ieeexplore.ieee.org/document/743501>.
7. Nielsen, M. & Chuang, I. Quantum Computation and Quantum Information (Cambridge University Press, 2000) <http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf>.
8. Bancal, J.-D. et al. Device-independent witnesses of genuine multipartite entanglement. *Phys. Rev. Lett.* **106**, 250404 (2011).
9. Brunner, N. et al. Testing the dimension of Hilbert spaces. *Phys. Rev. Lett.* **100**, 210503 (2008).
10. McKague, M., Yang, T. H. & Scarani, V. Robust self-testing of the singlet. *J. Phys. A Math. Theor.* **45**, 455304 (2012).
11. Yang, T. H. & Navascués, M. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A* **87**, 050102(R) (2013).
12. Bamps, C. & Pironio, S. 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).
13. Wang, Y., Wu, X. & Scarani, V. All the self-testings of the singlet for two binary measurements. *New J. Phys.* **18**, 025021 (2016).
14. Šupić, I., Augusiak, R., Salavrakos, A. & Acín, A. Self-testing protocols based on the chained Bell inequalities. *New J. Phys.* **18**, 035013 (2016).
15. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880 (1969).
16. Acín, A., Massar, S. & Pironio, S. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.* **108**, 100402 (2012).
17. Coladangelo, A., Goh, K. T. & Scarani, V. All pure bipartite entangled states can be self-tested. *Nat. Commun.* **8**, 15485 (2017).
18. Coladangelo, A. Generalization of the Clauser-Horne-Shimony-Holt inequality self-testing maximally entangled states of any local dimension. *Phys. Rev. A* **98**, 052115 (2018).
19. Kaniowski, J. et al. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. *Quantum* **3**, 198 (2019).
20. Salavrakos, A. et al. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.* **119**, 040402 (2017).

21. Wu, X., Bancal, J.-D., McKague, M. & Scarani, V. Device-independent parallel self-testing of two singlets. *Phys. Rev. A* **93**, 062121 (2016).
22. McKague, M. Self-testing in parallel. *New J. Phys.* **18**, 045013 (2016).
23. Collins, D., Gisin, N., Linden, N., Massar, S. & Popescu, S. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.* **88**, 040404 (2002).
24. Barrett, J., Kent, A. & Pironio, S. Maximally nonlocal and monogamous quantum correlations. *Phys. Rev. Lett.* **97**, 170409 (2006).
25. Żukowski, M., Zeilinger, A. & Horne, M. A. Realizable higher-dimensional two-particle entanglements via multiport beam splitters. *Phys. Rev. A* **55**, 2564 (1997).
26. Wang, J. et al. Multidimensional quantum entanglement with large-scale integrated optics. *Science* **360**, 285–291 (2018).
27. Acín, A., Pironio, S., Vértesi, T. & Wittek, P. Optimal randomness certification from one entangled bit. *Phys. Rev. A* **93**, 040102(R) (2016).
28. Woodhead, E. et al. Maximal randomness from partially entangled states. *Phys. Rev. Res.* **2**, 042028(R) (2020).
29. Coladangelo, A. A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations. *Quantum* **4**, 282 (2020).
30. Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496**, 456–460 (2013).
31. Šupić, I., Cavalcanti, D. & Bowles, J. Device-independent certification of tensor products of quantum states using single-copy self-testing protocols. *Quantum* **5**, 418 (2021).

ACKNOWLEDGEMENTS

We would like to thank A. Acín, P. Nurowski, and A. Sawicki for useful discussions. This work is supported by Foundation for Polish Science through the First Team project (No First TEAM/2017-4/31) cofinanced by the European Union under the European Regional Development Fund. JK acknowledges support from the Homing programme of the Foundation for Polish Science (grant agreement no. POIR.04.04.00-00-5F4F/18-00) cofinanced by the European Union under the European Regional Development Fund.

AUTHOR CONTRIBUTIONS

S.S., D.S., J.K., and R.A. conceived the idea, designed the proofs, and prepared the paper.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s41534-021-00490-3>.

Correspondence and requests for materials should be addressed to Shubhayan Sarkar.

Reprints and permission information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2021