Rapid Communications

Maximal randomness from partially entangled states

Erik Woodhead,[1,2,*] Jędrzej Kaniewski,[3,†] Boris Bourdoncle,[2] Alexia Salavrakos,[2] Joseph Bowles,[2] Antonio Acín,[2,4] and Remigiusz Augusiak[3]

[1] *Laboratoire d'Information Quantique, CP 225, Université libre de Bruxelles, Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium*
[2] *ICFO–Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain*
[3] *Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland*
[4] *ICREA–Institucio Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain*

(Received 16 June 2020; accepted 15 September 2020; published 13 November 2020)

We investigate how much randomness can be extracted from a generic partially entangled pure state of two qubits in a device-independent setting, where a Bell test is used to certify the correct functioning of the apparatus. For any such state, we first show that two bits of randomness are always attainable both if projective measurements are used to generate the randomness globally or if a nonprojective measurement is used to generate the randomness locally. We then prove that the maximum amount of randomness that can be generated using nonprojective measurements globally is restricted to between approximately 3.58 and 3.96 bits. The upper limit rules out that a bound of four bits potentially obtainable with extremal qubit measurements can be attained. We point out this is a consequence of the fact that nonprojective qubit measurements with four outcomes can only be self-tested to a limited degree in a Bell experiment.

DOI: 10.1103/PhysRevResearch.2.042028

Although it was not the original motivation [1], Bell's theorem [2] allows for a very strong test of quantum randomness. By preparing an entangled quantum system and exhibiting a Bell inequality violation with it, we can immediately know that the measurement outcomes were not the result of an underlying deterministic process. This observation is the basis of a class of quantum cryptography protocols, called *device independent*, that incorporate a Bell test as a self-test of the correct functioning of the apparatus. The class includes device-independent versions of quantum key distribution and random number generation [3–6].

This perspective prompts an obvious question: How much randomness can we extract from a given quantum system, and how might this depend on the degree of entanglement? Previous work (see Table I) has indicated that the two do not seem strongly related; we cannot necessarily get more randomness from a maximally entangled state than a weakly entangled one of the same dimension. This point was first made in Ref. [7], where it was shown that, with the help of a suitable Bell test, a uniformly random bit could be generated from the result of a projective measurement performed on one part of any partially entangled pure state of two qubits. Reference [7] also considered the possibility of generating more randomness from the joint outcomes of projective measurements performed on both subsystems. In this case, Ref. [7] found that the maximum of two uniformly random bits could be generated, but only confirmed that this was attainable using a maximally entangled state $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ or one could get arbitrarily close to it using a very weakly entangled state of the form $|\psi_\theta\rangle = \cos(\theta/2)|00\rangle + \sin(\theta/2)|11\rangle$ in the limit $\theta \to 0$ where it becomes separable. Between these two extremes, determining the amount of randomness that can be generated remains an open problem.

As well as projective measurements, it is also possible to perform nonprojective measurements on quantum systems. Nonprojective measurements can potentially generate more randomness as they can have more outcomes than the dimension of the quantum system they act on. Extremal qubit measurements in particular may have up to four outcomes [9]. In a bipartite Bell-type experiment this means that potentially up to two bits of randomness could be generated locally or up to four bits globally using nonprojective measurements. The first limit is known to be attainable: Reference [8] describes a way in which two bits of randomness can be generated locally using a single measurement on one side. But it is currently an open question whether the second limit of four bits is attainable globally. The same work, Ref. [8], only confirmed numerically that at least around 2.8997 bits of randomness can be generated this way. Both results were established only for the maximally entangled state.

In this Rapid Communication, we solve the question of how much randomness can be generated using projective measurements from a generic pure entangled state of two qubits and show that the upper limit of two bits is always attainable regardless of how strong or weak the entanglement is. We also show that, alternatively, two bits of randomness can

[*] erik.woodhead@ulb.ac.be
[†] jkaniewski@fuw.edu.pl

TABLE I. Maximum amount of randomness (quantified by the min-entropy) extractable from one (local) or jointly from two (global) projective (PROJ) or nonprojective (POVM) measurements from the maximally ($|\phi_+\rangle$) and any partially ($|\psi_\theta\rangle$) entangled two-qubit pure state. Square brackets indicate a range (rounded outward) within which the optimal amount of randomness is known to lie. Results that were previously known appear with citations to the works in which they first appeared.

		$\|\phi_+\rangle$	$\|\psi_\theta\rangle$
Local	PROJ	1 bit [5]	1 bit [7]
	POVM	2 bits [8]	2 bits
Global	PROJ	2 bits [7]	2 bits
	POVM	[3.58, 3.96] bits	[3.58, 3.96] bits

be extracted locally from any such state using a nonprojective measurement. It turns out however, as we will detail below, that nonprojective measurements can only be reconstructed to a limited degree from the correlations observed in a Bell experiment and this limits the amount of randomness that can be generated globally. We rule out that any scheme can generate more than about 3.9527 bits of randomness in this way, proving that the potential upper limit of four bits is not attainable. We nevertheless show that at least around 3.5850 bits of randomness can be generated globally with suitable nonprojective measurements from any partially entangled state.

The Bell test. To introduce the problem, we begin by considering the form of an arbitrary partially entangled state of two qubits. Such a state can always be expressed in its Schmidt decomposition as

$$|\psi_\theta\rangle = \cos\left(\frac{\theta}{2}\right)|00\rangle + \sin\left(\frac{\theta}{2}\right)|11\rangle \tag{1}$$

for an angle θ that, without loss of generality, we can and hereafter will take to be in the range $0 < \theta \leqslant \frac{\pi}{2}$. The same state is equivalently represented by its density operator $\psi_\theta = |\psi_\theta\rangle\langle\psi_\theta|$, which we can express as

$$\psi_\theta = \frac{1}{4}\big[\mathbb{1}\otimes\mathbb{1} + \cos(\theta)(\mathbb{1}\otimes \mathrm{Z} + \mathrm{Z}\otimes\mathbb{1}) \\ + \sin(\theta)(\mathrm{X}\otimes\mathrm{X} - \mathrm{Y}\otimes\mathrm{Y}) + \mathrm{Z}\otimes\mathrm{Z}\big] \tag{2}$$

in terms of the identity and Pauli operators $\mathbb{1}$, X, Y, and Z acting on each subsystem. We can see that Alice and Bob will have to perform measurements in the X-Y plane, for example, $A = \mathrm{X}$ and $B = \mathrm{Y}$, in order to extract two uniformly random bits from this state, since this is the only way to have $\langle A\rangle = \langle A\otimes B\rangle = \langle B\rangle = 0$. We would, however, intuitively expect the maximum violation of a Bell inequality on ψ_θ to be attained with measurements having a component in the Z direction, since the correlation terms involving Z in (2) are larger in magnitude than the analogous terms involving X and Y. As such, we anticipate that we will need a Bell experiment engineered to exploit the entire Bloch sphere.

To this end, we propose the following Bell test in which Alice and Bob perform ± 1-valued measurements A_x, $x = 1, 2, 3$ and B_y, $y = 1, \dots, 6$, in each round. They use the statistics to estimate the values of three Bell expressions. The first two,

$$I_\beta = \langle \beta A_1 + A_1(B_1 + B_2) + A_2(B_1 - B_2)\rangle, \tag{3}$$

$$J_\beta = \langle \beta A_1 + A_1(B_3 + B_4) + A_3(B_3 - B_4)\rangle, \tag{4}$$

are modified Clauser-Horne-Shimony-Holt (CHSH) expressions of the kind introduced in Ref. [7], while the third,

$$S = \langle A_2(B_5 + B_6) + A_3(B_5 - B_6)\rangle, \tag{5}$$

is an ordinary CHSH [10,11] expression. We choose

$$\beta = \frac{2\cos(\theta)}{\sqrt{1 + \sin(\theta)^2}} \tag{6}$$

for the value of the parameter β in the definitions of I_β and J_β, depending on the angle θ that identifies the intended state $|\psi_\theta\rangle$. Alice and Bob should in particular check that these Bell expressions attain the values

$$I_\beta = 2\sqrt{2}\sqrt{1 + \beta^2/4}, \tag{7}$$

$$J_\beta = 2\sqrt{2}\sqrt{1 + \beta^2/4}, \tag{8}$$

$$S = 2\sqrt{2}\sin(\theta). \tag{9}$$

The Bell expectation values (7)–(9) can be attained by measuring

$$A_1 = \mathrm{Z}, \quad A_2 = \mathrm{X}, \quad A_3 = \pm\mathrm{Y} \tag{10}$$

on Alice's side and performing suitable measurements on Bob's side on $|\psi_\theta\rangle$ [7]. Crucially for the intended application to randomness generation, this is, up to trivial modifications such as local changes of bases and extensions to higher dimension, essentially the only way to attain these expectation values. More precisely, in Supplemental Material A [12] we establish the following, which holds regardless of the Hilbert-space dimension.

Lemma 1. The conditions $I_\beta = J_\beta = 2\sqrt{2}\sqrt{1 + \beta^2/4}$ and $S = 2\sqrt{2}\sin(\theta)$ identify an extremal point in the quantum set and if they are attained there is a choice of local bases in which:

(i) the underlying state has the form

$$\rho = \psi_\theta \otimes \sigma_{\mathrm{A'B'}}, \tag{11}$$

where ψ_θ is the partially entangled state (2) and $\sigma_{\mathrm{A'B'}}$ is an ancillary state which may be of any dimension;

(ii) Alice's measurements act on the state according to

$$A_1 = \mathrm{Z}\otimes\mathbb{1}_{\mathrm{A'}}, \tag{12}$$

$$A_2 = \mathrm{X}\otimes\mathbb{1}_{\mathrm{A'}}, \tag{13}$$

$$A_3 = \mathrm{Y}\otimes A', \tag{14}$$

where A' is a ± 1-valued Hermitian operator;

(iii) Bob's measurements act on the state according to

$$\frac{B_1 + B_2}{\sqrt{2\lambda_+}} = \frac{B_3 + B_4}{\sqrt{2\lambda_+}} = \mathrm{Z}\otimes\mathbb{1}_{\mathrm{B'}}, \tag{15}$$

$$\frac{B_1 - B_2}{\sqrt{2\lambda_-}} = \frac{B_5 + B_6}{\sqrt{2}} = \mathrm{X}\otimes\mathbb{1}_{\mathrm{B'}}, \tag{16}$$

$$-\frac{B_3 - B_4}{\sqrt{2\lambda_-}} = -\frac{B_5 - B_6}{\sqrt{2}} = \mathrm{Y} \otimes B', \tag{17}$$

where $\lambda_\pm = 1 \pm \beta^2/4$ and B' is a ± 1-valued Hermitian operator;

(iv) the ancillary state $\sigma_{\mathrm{A'B'}}$ in (11) and operators A' and B' are related in such a way that

$$\langle A' \otimes B' \rangle_{\sigma_{\mathrm{A'B'}}} = 1. \tag{18}$$

The operators A' and B' appearing in Lemma 1 are inevitable and reflect the fact that we cannot distinguish a set of qubit measurements from their complex conjugates on both sides [13]. We should also remark that, strictly speaking, (ii) and (iii) give the form of Alice's and Bob's measurements only on the supports of the respective marginals $\rho_{\mathrm{A}} = \mathrm{Tr}_{\mathrm{B}}[\rho]$ and $\rho_{\mathrm{B}} = \mathrm{Tr}_{\mathrm{A}}[\rho]$ of the underlying state. This is not a problem for us since any action the measurements may have on part of the Hilbert space not containing the state cannot have any impact on the correlations. In the following we will assume, for simplicity, that the marginals are of full rank.

Randomness with projective measurements. Lemma 1 makes it straightforward to show that we can device-independently extract up to two bits of randomness using projective measurements. To do this, we simply add a seventh measurement, B_7, to the Bell test on Bob's side and check that its correlation with A_2 is

$$\langle A_2 B_7 \rangle = \sin(\theta). \tag{19}$$

Using $A_2 = \mathrm{X} \otimes \mathbb{1}_{\mathrm{A'}}$ and $\rho = \psi_\theta \otimes \sigma_{\mathrm{A'B'}}$ from Lemma 1 and tracing out everything on Alice's side, we can rewrite the correlation on the left as

$$\langle A_2 B_7 \rangle = \sin(\theta) \mathrm{Tr}\big[B_7 \tfrac{1}{2} \mathrm{X} \otimes \sigma_{\mathrm{B'}}\big]. \tag{20}$$

The operator $\frac{1}{2}\mathrm{X} \otimes \sigma_{\mathrm{B'}}$ has a trace norm of 1 and, since we are assuming $\sigma_{\mathrm{B'}}$ is of full rank, the only way for the right-hand sides of (19) and (20) to be equal is with

$$B_7 = \mathrm{X} \otimes \mathbb{1}_{\mathrm{B'}}. \tag{21}$$

With this information we can prove that the results of measuring A_3 and B_7 are maximally random. The probabilities of the four possible outcomes are

$$P(ab|37) = \tfrac{1}{4} \langle (\mathbb{1} + aA_3) \otimes (\mathbb{1} + bB_7) \rangle, \tag{22}$$

$a, b \in \{\pm 1\}$. Direct calculation with $A_3 = \mathrm{Y} \otimes A'$ and $B_7 = \mathrm{X} \otimes \mathbb{1}$ gives

$$P(ab|37) = \tfrac{1}{4}. \tag{23}$$

Importantly, the fact that we can derive $P(ab|37) = 1/4$ from $I_\beta = J_\beta = 2\sqrt{2}\sqrt{1 + \beta^2/4}$, $S = 2\sqrt{2}\sin(\theta)$, and $\langle A_2 B_7 \rangle = \sin(\theta)$ shows that these conditions together are extremal, i.e., they cannot be attained by averaging quantum strategies that give different values of these quantities. This rules out the possibility of a more detailed underlying explanation of the correlations that might allow better predictions to be made about A_3 and B_7.

Tomographic reconstruction of POVMs. POVMs performed on qubit systems can have more than two outcomes and can potentially be used to generate more randomness than projective measurements. The nature of the device-independent scenario means we will only be interested in POVMs that are extremal, i.e., that cannot be expressed as convex combinations of other POVMs. The extremal qubit POVMs were classified in Ref. [9] and the only nontrivial ones consist of at most four rank-one elements $\alpha_a = |\alpha_a\rangle\langle\alpha_a|$ that are linearly independent.

We can certify the randomness of *some* POVMs device-independently by using a form of tomography to partially reconstruct them. To see how this works note first that, in the device-dependent setting, we can reconstruct any extremal *qubit* POVM $\{\alpha_a\}$ on (for example) Alice's side from the correlations it produces with the Pauli operators on Bob's side. That is, it turns out that the expectation values $\langle \alpha_a \otimes \sigma_\nu \rangle_{\psi_\theta}$, for $\sigma_\nu = (\mathbb{1}, \mathrm{X}, \mathrm{Y}, \mathrm{Z})$ on Bob's side, contain sufficient information to uniquely identify $\{\alpha_a\}$ on Alice's side provided that the underlying state $|\psi_\theta\rangle$ is known.

In the device-independent scenario, we do not know that the quantum system we are manipulating is limited to a pair of qubits. However, according to Lemma 1 we can verify that Alice is performing Pauli-type measurements up to complex conjugation, and the linear combinations of Bob's measurements in (15)–(17) effectively give us such operators on Bob's side. With this, we can check that a POVM $\{R_a\}$ on (for example, again) Alice's side produces correlations consistent with an extremal qubit one, i.e., that

$$\langle R_a \otimes B_\nu \rangle_{\psi_\theta \otimes \sigma} = \langle \alpha_a \otimes \sigma_\nu \rangle_{\psi_\theta}, \tag{24}$$

with $B_\nu = (\mathbb{1} \otimes \mathbb{1}, \mathrm{X} \otimes \mathbb{1}, \mathrm{Y} \otimes B', \mathrm{Z} \otimes \mathbb{1})$, where $\{\alpha_a\}$ is some ideal reference qubit POVM. In Supplemental Material B [12], we prove that this allows us to infer the following on the form of $\{R_a\}$.

Lemma 2. If the correlations obtained from a POVM $\{R_a\}$ match those obtainable from an extremal reference qubit POVM $\{\alpha_a\}$ according to (24), then the elements R_a must be of the form

$$\begin{aligned} R_a = {} & \alpha_a \otimes A'_+ + \alpha_a^* \otimes A'_- \\ & + |\alpha_a\rangle\langle\alpha_a^*| \otimes K'_a + |\alpha_a^*\rangle\langle\alpha_a| \otimes K'^{\dagger}_a, \end{aligned} \tag{25}$$

where $|\alpha_a^*\rangle$ is the complex conjugate of $|\alpha_a\rangle$, $A'_\pm = (\mathbb{1} \pm A')/2$ are projectors on the positive and negative parts of A' from Lemma 1, and the K'_a satisfy the operator inequalities

$$K'_a K'^{\dagger}_a \leqslant A'_+, \quad K'^{\dagger}_a K'_a \leqslant A'_-, \tag{26}$$

and the condition

$$\sum_a |\alpha_a\rangle\langle\alpha_a^*| \otimes K'_a = 0. \tag{27}$$

Furthermore, if $\{R_a\}$ has three outcomes or less, then $K'_a = 0$ and (25) simplifies to

$$R_a = \alpha_a \otimes A'_+ + \alpha_a^* \otimes A'_-. \tag{28}$$

In other words, our Bell test allows us to reconstruct, up to complex conjugation, extremal POVMs with two or three outcomes but we can only partially constrain the form of POVMs with four outcomes. As we elaborate on in the Supplemental Material [12], the place where the number of outcomes makes a difference is in the condition (27): when there are three outcomes or less, the off-diagonal $|\alpha_a\rangle\langle\alpha_a^*|$ terms in (25) are always linearly independent and thus (27) can only be satisfied with $K'_a = 0$. On the other hand, a simple calculation shows that $\langle\alpha^*|\mathrm{Y}|\alpha\rangle = 0$ for any qubit state vector; this means that the $|\alpha_a\rangle\langle\alpha_a^*|$'s are restricted to the three-dimensional space of operators spanned by $\{\mathbb{1}, \mathrm{X}, \mathrm{Z}\}$ and they can never be linearly independent if there are four of them. In that case it is always possible to satisfy (27) with nonzero K'_as.

Randomness with POVMs. As we stated earlier, the maximum amount of randomness that could potentially be generated if both parties use extremal POVMs is limited to four bits. It is indeed possible to find extremal qubit POVMs that can generate arbitrarily close to this amount of randomness from any partially entangled state $|\psi_\theta\rangle$. Unfortunately, the fact that we cannot fully self-test POVMs means that this bound is not attainable in the device-independent setting. To see this, let us suppose that Alice and Bob unknowingly try to generate their random results using four-outcome POVMs $\{R_a\}$ and $\{S_b\}$ which are related to some ideal extremal qubit POVMs $\{\alpha_a\}$ and $\{\beta_b\}$ by

$$\begin{aligned} R_a = {} & \alpha_a \otimes |{+}\rangle\langle{+}|_{\mathrm{A}'} + \alpha_a^* \otimes |{-}\rangle\langle{-}|_{\mathrm{A}'} \\ & + \lambda_a |\alpha_a\rangle\langle\alpha_a^*| \otimes |{+}\rangle\langle{-}|_{\mathrm{A}'} \\ & + \lambda_a^* |\alpha_a^*\rangle\langle\alpha_a| \otimes |{-}\rangle\langle{+}|_{\mathrm{A}'}, \end{aligned} \tag{29}$$

$$\begin{aligned} S_b = {} & \beta_b \otimes |{+}\rangle\langle{+}|_{\mathrm{B}'} + \beta_b^* \otimes |{-}\rangle\langle{-}|_{\mathrm{B}'} \\ & + \mu_b |\beta_b\rangle\langle\beta_b^*| \otimes |{+}\rangle\langle{-}|_{\mathrm{B}'} \\ & + \mu_b^* |\beta_b^*\rangle\langle\beta_b| \otimes |{-}\rangle\langle{+}|_{\mathrm{B}'}, \end{aligned} \tag{30}$$

where λ_a and μ_b are some complex coefficients with magnitudes less than 1, while an eavesdropper at each round randomly and equiprobably chooses and prepares one of two states $\psi_\theta \otimes \chi'_+$ or $\psi_\theta \otimes \chi'_-$ with different ancillary parts $|\chi'_\pm\rangle = (|{+}{+}\rangle \pm |{-}{-}\rangle)/\sqrt{2}$. Using that $\langle\alpha^*\beta^*|\psi_\theta\rangle = \langle\alpha\beta|\psi_\theta\rangle^*$, we can work out that the joint probability of Alice's and Bob's outcomes, conditioned on either ancillary state being chosen by Eve, is

$$\langle R_a \otimes S_b\rangle_{\psi_\theta\otimes\chi'_\pm} = |\langle\alpha_a\beta_b|\psi_\theta\rangle|^2 \pm \mathrm{Re}[\lambda_a^*\mu_b^*\langle\alpha_a\beta_b|\psi_\theta\rangle^2]. \tag{31}$$

These probabilities average out to the ideal joint probabilities $|\langle\alpha_a\beta_b|\psi_\theta\rangle|^2$ that would be obtained from the reference qubit POVMs on $|\psi_\theta\rangle$; hence, Alice and Bob have no way to detect, device independently, that they are measuring $\{R_a\}$ and $\{S_b\}$ rather than $\{\alpha_a\}$ and $\{\beta_b\}$. Eve, however, knowing which ancilla state she chose, also knows which of the two joint distributions in (31) was actually prepared in each round and can use this to make a more informed guess about what the outcome will be.

Let us see how this could help Eve in the worst case. As we pointed out above, the off-diagonal terms $|\alpha_a\rangle\langle\alpha_a^*|$ and $|\beta_b\rangle\langle\beta_b^*|$ are never linearly independent and, thus, the coefficients λ_a and μ_b can be chosen nonzero. We are free to scale them such that the largest coefficient on each side is of magnitude one. By also exploiting the freedom to choose their phases we can arrange that, for at least one pair (a, b) of outputs, $\mathrm{Re}[\lambda_a^*\mu_b^*\langle\alpha_a\beta_b|\psi_\theta\rangle^2] = |\langle\alpha_a\beta_b|\psi_\theta\rangle|^2$. In other words, we are certain we can arrange for at least one of the probabilities $\langle R_a \otimes S_b\rangle_{\psi_\theta\otimes\chi'_-}$ to be zero. This means that the probability of the most likely joint outcome, conditioned on Eve choosing $|\chi'_-\rangle$, cannot be lower than $1/15$. It follows that the randomness that can be certified device-independently for the entire protocol can never be higher than

$$-\log_2\left[\frac{1}{2}\left(\frac{1}{15} + \frac{1}{16}\right)\right] \approx 3.9527 \text{ bits} \tag{32}$$

regardless of the state and POVMs that Alice and Bob try to use.

On a more positive note, the above-described complication does not manifest if only one of the parties uses a measurement with four outcomes and, in that case, the amount of randomness that can be generated device-independently is the same as the amount of randomness that can be generated using extremal qubit POVMs performed on $|\psi_\theta\rangle$. This means it is potentially possible to generate up to two bits of randomness locally, or alternatively potentially up to

$$-\log_2(1/12) \approx 3.5850 \text{ bits} \tag{33}$$

of randomness globally using a four-outcome POVM on one side and a three-outcome POVM on the other. We give explicit constructions of POVMs that yield these amounts of randomness (or arbitrarily close) in Supplemental Material C [12].

Conclusion. Our work reinforces the observation that the amount of randomness obtainable from a quantum system does not in general increase with the degree of entanglement. In two versions of the problem, we have confirmed that an upper limit of two bits of randomness is always obtainable from any partially entangled pure state of two qubits. In the global case using POVMs, although we do not know the optimal amount of extractable randomness we have significantly narrowed the range to between about 3.58 and 3.96 bits for any state. The nontrivial latter limit establishes that the upper bound of four bits is not attainable in this case.

Our results rely on the fact that we can reconstruct the underlying quantum state and measurements in our Bell test sufficiently well to conclude that the outcomes are genuinely random. This adds to a growing literature showing that we can often infer substantial information about the quantum resources available from a Bell test [14–18]. Previous work has notably shown that the partially entangled state [19,20] or measurements spanning the entire Bloch sphere (up to complex conjugation) [8,21,22] can be self-tested, although before now not together in the same test.

Our work also led us to investigate whether it is possible to self-test nonprojective measurements in quantum physics and we found that qubit POVMs with four outcomes can only be self-tested to a limited extent. The ambiguity with respect to complex conjugation can thus, as we found here, make a significant difference in the device-independent setting. It will be interesting to further explore this problem, both for qubit systems and in higher dimension. In particular, closing the gap on optimal randomness generation with POVMs is likely to require developing a better understanding of the general form that we found POVMs may take in lemma 2.

Note added. Previously, we became aware that the authors of Ref. [23] had independently found using a similar approach that two bits of randomness can be generated globally using projective measurements from the partially entangled state.

This work was supported by the Spanish MINECO (Severo Ochoa Grant No. SEV-2015-0522), the Generalitat de Catalunya (CERCA Program and SGR 1381), the Fundació Privada Cellex and Mir-Puig, the AXA Chair in Quantum Information Science, the ERC AdG CERQUTE and CoG QITBOX, and the EU Quantum Flagship project QRANGE. J.K. acknowledges support from the National Science Centre, Poland (Grant No. 2016/23/P/ST2/02122). This project is carried out under POLONEZ programme which has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No. 665778. B.B. acknowledges support from the Secretaria d'Universitats i Recerca del Departament d'Economia i Coneixement de la Generalitat de Catalunya and the European Social Fund (FEDER). R.A. acknowledges support from the Foundation for Polish Science through the First Team project (First TEAM/2017-4/31) cofinanced by the European Union under the European Regional Development Fund.

[1] T. Norsen, John S. Bell's concept of local causality, Am. J. Phys. **79**, 1261 (2011).

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

[3] 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).

[4] R. Colbeck, Quantum and relativistic protocols for secure multiparty computation, Ph.D. thesis, University of Cambridge, 2006, arXiv:0911.3814.

[5] S. Pironio, A. Acín, S. Massar, A. Boyer de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

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

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

[8] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A **93**, 040102(R) (2016).

[9] G. M. D'Ariano, P. Lo Presti, and P. Perinotti, Classical randomness in quantum measurements, J. Phys. A: Math. Gen. **38**, 5979 (2005).

[10] 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).

[11] B. S. Cirel'son, Quantum generalizations of Bell's inequality, Lett. Math. Phys. **4**, 93 (1980).

[12] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevResearch.2.042028 for proofs of Lemmas 1 and 2 and an explicit strategy attaining $-\log_2(1/12)$ bits of global randomness.

[13] M. McKague and M. Mosca, Generalized self-testing and the security of the 6-state protocol, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science Vol. 6519 (Springer, Berlin, 2011), pp. 113–130.

[14] L. A. Khalfin and B. S. Tsirelson, Quantum and quasi-classical analogs of Bell inequalities, in *Symposium on the Foundations of Modern Physics* (World Scientific, Singapore, 1985), pp. 441–460.

[15] S. L. Braunstein, A. Mann, and M. Revzen, Maximal Violation of Bell Inequalities for Mixed States, Phys. Rev. Lett. **68**, 3259 (1992).

[16] V. Scarani and N. Gisin, Spectral decomposition of Bell's operators for qubits, J. Phys. A: Math. Gen. **34**, 6043 (2001).

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

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

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

[20] 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).

[21] J. Kaniewski, Self-testing of binary observables based on commutation, Phys. Rev. A **95**, 062323 (2017).

[22] O. Andersson, P. Badziąg, I. Bengtsson, I. Dumitru, and A. Cabello, Self-testing properties of Gisin's elegant Bell inequality, Phys. Rev. A **96**, 032119 (2017).

[23] R. Ramanathan and S. Pironio (unpublished).