Optimal randomness certification from one entangled bit

Antonio Acín,[1,2] Stefano Pironio,[3] Tamás Vértesi,[4] and Peter Wittek[1,5]

[1]*ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*
[2]*ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain*
[3]*Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), 1050 Brussels, Belgium*
[4]*Institute for Nuclear Research, Hungarian Academy of Sciences, H-4001 Debrecen, P.O. Box 51, Hungary*
[5]*University of Borås, 50190 Borås, Sweden*

(Received 19 June 2015; published 18 April 2016)

By performing local projective measurements on a two-qubit entangled state one can certify in a device-independent way up to one bit of randomness. We show here that general measurements, defined by positive-operator-valued measures, can certify up to two bits of randomness, which is the optimal amount of randomness that can be certified from an entangled bit. General measurements thus provide an advantage over projective ones for device-independent randomness certification.

DOI: 10.1103/PhysRevA.93.040102

Introduction. The nonlocal correlations observed when measuring entangled quantum particles certify the presence of intrinsic randomness in the measurement outputs in a way that is independent of the underlying physical realization of these correlations. While this relation between nonlocality and randomness had been noted by different authors since the seminal work by Bell [1,2], it is only recently that the tools to quantify the intrinsic randomness produced in Bell setups were provided [3–5]. These tools were initially introduced in the context of device-independent randomness generation [3,6–8], but have also allowed us to obtain a much better understanding of the relation between randomness and Bell violations, two of the most fundamental properties of quantum theory. For instance, today we know that maximal randomness can be certified from arbitrarily small amounts of nonlocality or entanglement [9], or that maximal randomness certification is possible in quantum theory, but not in general theories restricted only by the no-signaling principle [10].

Despite all this progress, there are still fundamental questions on the relation between randomness, nonlocality, and entanglement that remain completely unexplored. In this work we consider and solve one of them: we obtain the maximal amount of randomness that can be certified in a standard Bell scenario involving local measurements on one entangled bit or *ebit*. In order to achieve this maximum the use of general measurement beyond projective ones, often known as positive-operator-valued measures (POVMs), is necessary. Thus, our results and techniques are also interesting because they provide one of the few examples in the context of Bell nonlocality where the use of these general measurements provides an advantage over standard projective measurements (other examples can be found in Refs. [11,12]).

We formulate the relation between randomness and nonlocality in the setting of *nonlocal guessing games* as considered in Ref. [4]. Such games consist of two users, Alice and Bob, and an adversary Eve. Alice and Bob perform local measurements on two separate quantum systems, labeled by A and B. There are m_A and m_B possible measurements on particles A and B, each producing r_A and r_B possible results. Measurement choices are labeled by x and y, with $x = 1,\dots,m_A$ and $y = 1,\dots,m_B$, while the corresponding results are labeled by a and b, with $a = 1,\dots,r_A$ and $b = 1,\dots,r_B$, respectively. Alice and Bob's systems are then characterized by the finite set of $m_A \times m_B \times r_A \times r_B$ probabilities $P = \{P(ab|xy)\}$, where $P(ab|xy)$ is the probability that outcomes a and b are obtained when performing measurements x and y on particles A and B. We refer in the following to any such set P of probabilities as a *behavior*. In our nonlocal guessing game, P is assumed to be given, i.e., it is a promise on the behavior of Alice's and Bob's systems. The aim is for Eve to guess as well as possible Alice's outcome for a certain input $\bar{x}$. To achieve this, Eve can prepare Alice's and Bob's system in any way compatible with the given behavior P and the laws of quantum physics. A strategy S for Eve consists in (i) a tripartite quantum state $|\Psi\rangle_{ABE}$ on a composite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ of arbitrary dimension, this state allowing for possible correlations between Alice's, Bob's, and Eve's system; (ii) for each value of x, a POVM A_x on $\mathcal{H}_A$ with elements $A_{a|x}$ and for each value of y, a POVM B_y on $\mathcal{H}_B$ with elements $B_{b|y}$ characterizing the local measurements of Alice and Bob; and (iii) a POVM Z on $\mathcal{H}_E$ with elements Z_a whose result is Eve's best guess on Alice's outcome. Such a strategy is compatible with P if

$$P(ab|xy) = \langle\Psi_{ABE}|A_{a|x} \otimes B_{b|y} \otimes I|\Psi_{ABE}\rangle. \tag{1}$$

The figure of merit of the game is the probability that Alice's output and Eve's guess coincide, maximized over all strategies S compatible with P (a set which we denote $\mathcal{S}_P$):

$$G(\bar{x},P) = \max_{S\in\mathcal{S}_P} \sum_a \langle\Psi_{ABE}|A_{a|\bar{x}} \otimes I \otimes Z_a|\Psi_{ABE}\rangle. \tag{2}$$

We refer to this quantity as the *local guessing probability*.

We can also introduce a variant of the game in which Eve attempts to guess both Alice's and Bob's outputs for a given pair of inputs $(\bar{x},\bar{y})$ in which case her strategies involve a POVM Z with elements Z_{ab} and the figure of merit is

$$G(\bar{x},\bar{y},P) = \max_{S\in\mathcal{S}_P} \sum_{ab} \langle\Psi_{ABE}|A_{a|\bar{x}} \otimes B_{b|\bar{y}} \otimes Z_{ab}|\Psi_{ABE}\rangle. \tag{3}$$

We refer to this quantity as the *global guessing probability*.

The local and global guessing probabilities quantify the predictability of the result of measurement $\bar{x}$, or of a pair of measurements $\bar{x}$ and $\bar{y}$, by a quantum observer with an optimal description of the experiment. Taking minus the logarithm in base two of these quantities gives a measure of randomness expressed in bits, which defines the optimal amount of randomness that can be certified in a device-independent way from the given correlations. A bound on these quantities is often a central element in the analysis of actual randomness generation of expansion protocols, such as [3,7], where it directly determines (up to statistical corrections) the final amount of randomness generated.

Note that we always have $G(\bar{x},P) \geqslant \max_a P(a|\bar{x})$ and $G(\bar{x},\bar{y},P) \geqslant \max_{ab} P(ab|\bar{x}\bar{y})$ since a simple strategy is for Eve to simply guess the most probable outcomes of Alice's and Bob's measurements without exploiting any further detailed information about Alice's and Bob's systems. However, in general a nontrivial strategy performs strictly better than these trivial bounds. Note that the guessing probabilities satisfy a convexity property in the sense that if P admits the convex decomposition $P = \sum_\lambda q_\lambda P_\lambda$, then $G(\bar{x},P) \geqslant \sum_\lambda q_\lambda G(\bar{x},P_\lambda)$ and similarly for $G(\bar{x},\bar{y},P)$. This follows from the fact that a strategy that Eve can follow is to prepare Alice's and Bob's system with probability q_λ according to the behavior P_λ and use the optimal guessing strategy associated to P_λ. In particular, in the case in which the given correlations P can be described by a local model, they can be written down as a convex mixture of deterministic behaviors [2], and one has $G(x) = 1$ and $G(x,y) = 1$ for any measurement x and y. However, the violation of Bell inequalities does not necessarily imply that $G(\bar{x}) < 1$ or $G(\bar{x},\bar{y}) < 1$. Upper bounds on the guessing probabilities can be computed using the Navascués-Pironio-Acín (NPA) hierarchy for quantum correlations [13], as shown in Refs. [4,5].

In this work, our goal is to compute the maximal randomness that one can certify from one ebit. That is, our goal is to identify the correlations minimizing the local guessing probability among all those attainable by measuring an entangled two-qubit state. The obtained quantity defines the optimal amount of randomness that can be certified in a device-independent way using an entangled qubit.

Local measurements on such a state can always be viewed as POVMs acting on a qubit since the local Schmidt dimension is 2. In the case where the local qubit measurements are projective, it is known that one bit of local randomness [3] and two bits of global randomness [14,15] can be certified from an ebit. This is also the maximum that can be achieved under such measurements, since a qubit projective measurement has only two possible outcomes. Beating those bounds thus requires considering more general measurements, beyond projective.

We start by stating a rather straightforward observation: no more than $2\log_2 d$ bits of local randomness and $4\log_2 d$ bits of global randomness can be certified by measuring an entangled state of dimension $d \times d$. This follows from the convexity property of the guessing probabilities mentioned above and the fact that a POVM acting on a space of dimension d can always be decomposed as a convex sum of POVMs of at most d^2 outputs [16], which can evidently contain at most $2\log_2 d$ bits of randomness. In the case of qubits, no more than two bits of local randomness and four bits of global randomness can be certified, i.e., twice as much than using projective measurements.

Our main result is to construct two examples of qubit correlations saturating this bound on the local randomness. They thus provide examples of optimal local randomness certification from one ebit. In the first example we prove analytically that the local randomness is two bits, while in the second we have to resort to semidefinite programming (SDP) techniques.

First optimal construction. Our first construction is based on nonlocal correlations obtained by measuring the two-qubit maximally entangled state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ with measurements $x = 1,2,3$ on Alice's side corresponding to $\sigma_x,\sigma_y,\sigma_z$ and with measurements $y = 1,\ldots,6$ on Bob's side corresponding to $(\sigma_x \pm \sigma_y)/\sqrt{2},(\sigma_x \pm \sigma_z)/\sqrt{2},(\sigma_y \pm \sigma_z)/\sqrt{2}$. These measurements are chosen so that they produce the maximal violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality [17] with all the possible pairs of measurements on the first particle, that is, $\mathcal{B}(1,2;1,2) = \mathcal{B}(1,3;3,4) = \mathcal{B}(2,3;5,6) = 2\sqrt{2}$, where

$$\mathcal{B}(i,j;k,l) = E_{ik} + E_{il} + E_{jk} - E_{jl}$$

and $E_{ik} = \sum_{ab}(-1)^{ab}P(ab|ik)$. Finally a four-output measurement $y = 7$ is included on the second particle. This seventh measurement by Bob plays a special role in our construction as it is the one used to certify the two random bits. We denote it by R, for random, and its measurement operators by R_b, with $b = 1,\ldots,4$. This measurement is rather generic but has to satisfy two requirements: (i) it is extremal in the set of qubit measurements and (ii) its measurement operators are such that $\mathrm{Tr}(R_b) = 1/4, \forall b$. An example of such a measurement is given by a POVM where $R_b = 1/4|\psi_b\rangle\langle\psi_b|$ and the Bloch vectors corresponding to $|\psi_b\rangle$ point to the direction of a tetrahedron.

The measurements described above define the behavior P which Eve has to reproduce (possibly using other quantum realizations of arbitrary dimension). Clearly, the four-output measurement R, when acting on half of a maximally entangled state, gives $P(b|y = 7) = 1/4$ for all b and thus $G(y = 7,P) \geqslant 1/4$. As mentioned previously, this is only a trivial upper bound on the amount of intrinsic randomness, which is generally far from being tight. However, we prove that for the correlations P defined above the bound is tight and, therefore, $G(y = 7,P) = 1/4$ and hence two bits of local randomness can be certified from P.

To understand the main intuition behind the choice of state and measurements in our construction, the idea is to exploit the fact that, roughly speaking, the only quantum way of getting the maximal quantum violation of the CHSH inequality, also known as the Tsirelson's bound, is by performing anticommuting measurements on a two-qubit maximally entangled state. We refer to these quantum correlations, which are unique, as Tsirelson correlations. The correlations generated in the previous quantum setup contain three blocks of Tsirelson correlations for the different pairs of settings on particle A and corresponding measurements on B. This suggests that the only state and measurements that could have produced these correlations should be, up to local unitary transformations, precisely Pauli measurements X, Y, and Z on A acting on a two-qubit maximally entangled state. Now, these three measurements when acting on half of a maximally entangled state allow reconstructing any measurement implemented on the other half. In fact, they remotely project particle B onto the eigenstates of these three observables, which are tomographically complete. Therefore, it should be possible from the observed correlations to reconstruct and certify the POVM elements implemented on B and conclude that they certify the desired amount of randomness. As show below, this intuition is not entirely true due to a problem with complex conjugation, but it is enough to prove the desired result. In fact, we believe this construction is interesting per se and may find applications in other problems of certification and self-testing of quantum devices.

After providing this intuition, let us now show that the given setup indeed certifies two bits of local randomness. As described earlier, any quantum strategy of Eve corresponds to a tripartite state $|\Psi\rangle_{ABE}$, a set of three observables A_1,A_2,A_3 for Alice, six two-output observables $B_1,\ldots,B_6$, and one four-output measurement B_7. This strategy should reproduce the given correlations P, as expressed in Eq. (1), and thus also the CHSH expectations $\mathcal{B}(1,2;1,2) = \mathcal{B}(1,3;3,4) = \mathcal{B}(2,3;5,6) = 2\sqrt{2}$. This implies, given the self-testing property of the CHSH inequality [18] and following Mosca-McKague [19], that up to a local isometry $|\Psi_{ABE}\rangle = |\phi^+\rangle_{AB}|\psi\rangle_{A'B'E}$. In addition, $A_1|\Psi_{ABE}\rangle = (X_A \otimes I_{A'})|\phi^+\rangle_{AB}|\psi\rangle_{A'B'E}$ and similarly $A_3|\Psi_{ABE}\rangle = (Z_A \otimes I_{A'})|\phi^+\rangle_{AB}|\psi\rangle_{A'B'E}$. On the other hand, $A_2|\Psi_{ABE}\rangle = (Y_A \otimes M_{A'})|\phi^+\rangle_{AB}|\psi\rangle_{A'B'E}$ where $M_{A'}$ is Hermitian and unitary. Basically this states that the three observables A_1,A_2,A_3 are necessarily the Pauli measurements X,Y,Z acting on Alice's system, except for A_2 for which a correction $M_{A'}$ is needed. This correction reflects the fact that the optimal measurements leading to the three maximal CHSH expectations given above are only defined up to a complex conjugation (see [19] for a discussion of this point).

Let us now determine the action of the POVM B_7. For simplicity of notation, let us denote it $\tilde{R}$ and the corresponding outcome operators $\tilde{R}_b$. The correlations between the outcomes of this POVM and Alice's observables should equal those of the ideal setup defined earlier, as expressed in Eq. (1). This means that $\langle\Psi_{ABE}|A_\mu \otimes \tilde{R}_b \otimes I|\Psi_{ABE}\rangle = \langle\phi^+|\sigma_\mu \otimes R_b|\phi^+\rangle$, where A_0 denotes the identity operator.

Let us now note that the ideal POVM elements R_b used in the definition of P can be written as $R_b = \sum_\mu r_b^\mu \sigma_\mu$ where $\{\sigma_\mu : \mu = 0,1,2,3\}$ is the basis of the four Pauli operators and r_b^μ are complex coefficients defining the POVM. We then have $\langle\phi^+|\sigma_\mu \otimes R_b|\phi^+\rangle = r_b^\mu$, hence $\langle\Psi_{ABE}|A_\mu \otimes \tilde{R}_b \otimes I|\Psi_{ABE}\rangle = r_b^\mu$.

On the other hand, since $\tilde{R}_B$ acts jointly on systems BB', without loss of generality we can decompose its operators as $\tilde{R}_b = \sum_\mu \sigma_\mu \otimes \tilde{R}_b^\mu$, where $\{\sigma_\mu : \mu = 0,1,2,3\}$ is the basis of the four Pauli operators on B and $\tilde{R}_b^\mu$ are arbitrary Hermitian operators on B'. Inserting these expressions for $\tilde{R}_b$ and using the specific form of $|\Psi_{ABE}\rangle$ and A_1,A_2,A_3 enforced by the CHSH constraints, we find $\langle\psi_{A'B'E}|I \otimes \tilde{R}_b^\mu \otimes I|\psi_{A'B'E}\rangle = r_b^\mu$ in the case $\mu \neq 2$ and $\langle\psi_{A'B'E}|M_{A'} \otimes \tilde{R}_b^\mu \otimes I|\psi_{A'B'E}\rangle = r_b^\mu$ when $\mu = 2$.

Introduce the normalized states $|\varphi_{B'}^{\pm,e}\rangle = (M_{A'}^{\pm} \otimes I \otimes Z_e)|\psi_{A'B'E}\rangle/\sqrt{q_{\pm,e}}$, where $M_{A'}^{\pm}$ is the projector on the $\pm$ eigenspace of $M_{A'}$ and Z_e is the projector corresponding to Eve's outcome e (without generality we can assume Eve's measurement Z to be projective). We can then write

$$\begin{aligned} r_b^\mu &= \sum_{\pm,e} q_{\pm,e}\langle\varphi^{\pm,e}|I \otimes \tilde{R}_b^\mu \otimes I|\varphi^{\pm,e}\rangle \\ &= \sum_e \left[q_{+,e}\,\tilde{r}_b^{\mu;+,e} + q_{-,e}\,\tilde{r}_b^{\mu;-,e}\right] \end{aligned} \tag{4}$$

for $\mu = 0,1,3$ and

$$\begin{aligned} r_b^\mu &= \sum_{\pm,e} q_{\pm,e}\langle\varphi^{\pm,e}|M_{A'} \otimes \tilde{R}_b^\mu \otimes I|\varphi^{\pm,e}\rangle \\ &= \sum_e \left[q_{+,e}\,\tilde{r}_b^{\mu;+,e} - q_{-,e}\tilde{r}_b^{\mu;-,e}\right] \end{aligned} \tag{5}$$

for $\mu = 2$, where we have defined the coefficients $\tilde{r}_b^{\mu;\pm,e} = \langle\varphi^{\pm,e}|I \otimes R_b^\mu \otimes I|\varphi^{\pm,e}\rangle$. Note that these coefficients define a family of valid qubit POVMs $\tilde{R}^{\pm,e}$ with operators $\tilde{R}_b^{\pm,e} = \sum_\mu \tilde{r}_b^{\mu;\pm,e}\sigma_\mu$. These POVMs simply correspond to preparing an ancilla system B' in the state $|\varphi_{B'}^{\pm,e}\rangle$ and performing the POVM $\tilde{R}$ on the joint system BB'.

Now redefine $\tilde{r}_b^{\mu;-,e}$ as above but with the sign of $\tilde{r}_b^{2;-,e}$ changed. Then this also defines valid POVMs, which are just the complex conjugates of $\tilde{R}^{\pm,e}$. With this redefinition, we can now write Eqs. (4) and (5) as

$$r_b^\mu = \sum_{\pm,e} q_{\pm,e}\,\tilde{r}_b^{\mu;\pm,e} \tag{6}$$

for $\mu = 0,1,2,3$. We can interpret this as providing a convex decomposition for the ideal POVM R in terms of the POVMs $\tilde{R}^{\pm,e}$ with respective weights $q_{\pm,e}$. But since this POVM is extremal, we must have $\tilde{r}_b^{\mu;\pm,e} = r_b^\mu$ for all $\pm,e$. In particular, $\tilde{r}_b^{0;\pm,e} = r_b^0 = 1/4$ for all $\pm,e$.

Finally, let us now rewrite the guessing probability for the input $y = 7$ with these notations. We have

$$\begin{aligned} G(y=7,P) &= \sum_{b=0}^{3}\langle\Psi_{ABE}|I \otimes \tilde{R}_b \otimes Z_b|\Psi_{ABE}\rangle \\ &= \sum_{b=0}^{3}\langle\psi_{A'B'E}|I \otimes \tilde{R}_b^0 \otimes Z_b|\psi_{A'B'E}\rangle \\ &= \sum_{b=0}^{3} q_{\pm,b}\,\tilde{r}_b^{0;\pm,b} = 1/4, \end{aligned}$$

which provide the two announced random bits.

Second optimal construction. Our second construction to generate two random bits from a qubit is slightly simpler but the certification of randomness makes use of the numerical SDP techniques introduced in Ref. [4] based on the NPA hierarchy for quantum correlations [13].

The construction is based on the elegant Bell inequality introduced in [11]. It is defined in a scenario involving three measurements on Alice's side and four on Bob's. All measurements have two outputs and the inequality reads

$$\begin{aligned} \beta_{\text{el}} = E_{11} + E_{12} - E_{13} - E_{14} + E_{21} - E_{22} + E_{23} - E_{24} \\ + E_{31} - E_{32} - E_{33} + E_{34} \leqslant 6. \end{aligned} \tag{7}$$

The maximal known quantum violation of the inequality is equal to $4\sqrt{3}$ and is obtained with a maximally entangled state, projective measurements $A_1 = \sigma_x$, $A_2 = \sigma_y$, $A_3 = \sigma_z$ on Alice, while Bob's projective measurements are defined by the four vectors of a tetrahedron. In the Supplemental Material [20], we show that this known quantum violation is in fact optimal, which gives a new Tsirelson-type bound for quantum correlations.

We introduce a four-outcome measurement R, but now on Alice's side. As above, this measurement will be used to generate the two random bits. Given this configuration of measurements, we define the modified elegant Bell inequality

$$\beta'_{\text{el}} = \beta_{\text{el}} - k \sum_{i=1}^{4} P(a = i, b = +1 | x = 4, y = i) \leqslant 6, \quad (8)$$

where k is an arbitrary strictly positive constant. As the last term in the inequality is always negative, the bound follows from the bound on β_{el}. The same argument implies that the quantum violation cannot be larger than $4\sqrt{3}$. If we use the known optimal qubit settings, given above, the only way of getting this maximal violation is if the POVM elements of measurement R are antialigned with the four projective measurements on Bob's side, so that all probabilities $P(a = i, b = +1 | x = 4, y = i)$ are zero. But then, the corresponding measurement, when acting on half of a maximally entangled state, define two random bits on Alice's side. The intuition, then, is that the maximal violation of the modified elegant Bell inequality should certify the generation of two random bits for measurement R.

We used the numerical techniques in [4] to bound the randomness present in the correlations maximally violating (8). Recall that these techniques are based on SDP and, therefore, one has control over the precision of the numerical result. Using these techniques at level $2 + AAB + ABB$ of the NPA hierarchy with an arbitrary-precision solver [21,22], we can show that the generated randomness by measurement R in the previous setup is larger than 1.999 999 894 747 02 bits.

Noise robustness. The numerical approach of [4] also allows one to study the robustness of the previous constructions against noise. A typical noise model consists of mixing, with weights v and $1 - v$, with $0 \leqslant v \leqslant 1$, the ideal quantum correlations with uncorrelated noise in which all outputs have the same probability. By decreasing v, often known as visibility, the amount of certified randomness decreases. In Fig. 1 we plot a lower bound on the generated randomness as a function of the visibility for the two previous constructions. It can be seen that the gain provided by the POVM is fragile, in the sense that a small fraction of noise, of the order of 0.01, makes the obtained randomness smaller than one bit, which is the randomness provided by projective measurements. These considerations are relevant, for instance, when thinking of a possible experiment showing the advantage of using POVM's for randomness certification. A natural open question opened by our work is thus to identify robust setups for randomness generation using POVMs.

Global randomness. Before concluding, we would like to briefly discuss the problem of global randomness. The question is whether it is possible to find Bell setups involving a pair of maximally entangled qubits allowing the generation of four bits of randomness. We mainly leave this question for future work. Nevertheless, we made some preliminary numerical searches, using slightly more complex variations of the previous construction based on the elegant Bell inequality. These constructions are described in the Supplemental Material. As shown there, they can be used to certify the generation of 2.8997 bits, which is both higher than the global randomness that can be certified with projective measurements and the local randomness that can be certified with general measurements.

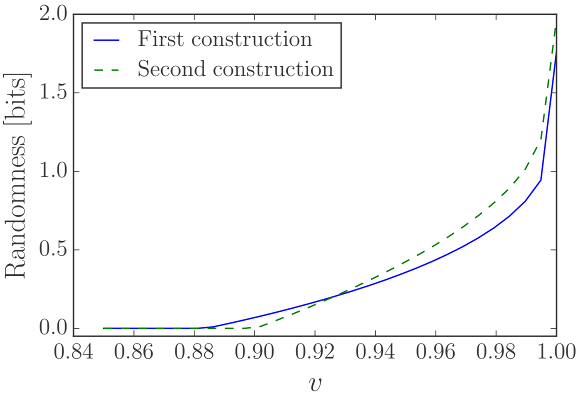

FIG. 1. Lower bound on the randomness ($-\log_2$ of the guessing probability) as a function of the visibility v ranging from 0.85 to 1.0. The correlations are of the form $v\mathbf{q} + (1 - v)\mathbf{r}$, where $\mathbf{q}$ are the quantum correlations yielding the maximum violation of the respective inequalities, and $\mathbf{r}$ denotes the completely unbiased correlations that assign the same probability to each measurement outcome. The figure was obtained using level 2 of the NPA hierarchy and thus only represents a lower bound on the maximal randomness (note, for instance, that we do not recover the optimal values of two bits for $v = 1$). Better noise resistance than the one provided by these curves may thus be obtained by performing a more complex analysis.

Conclusions. We have shown that an ebit can certify the presence of more than one bit of randomness locally and more than two bits globally. This result can only be achieved by making use of general measurements, proving thus that these measurements provide an advantage for randomness certification. This should also be contrasted with certain non-device-independent scenarios for randomness certification where the use of general measurements has been shown to be pointless [15]. For the case of local randomness, we have found two constructions that can certify two bits of randomness, the maximal possible value. Both constructions involve a maximally entangled state and the three Pauli measurements on Alice's side. In the first construction, the violation of three CHSH inequalities are used to self-test the maximally entangled state and these three Pauli measurements on Alice's side. This in turn allows one to self-test a four-outcome extremal POVM on Bob's, which generates the two bits of local randomness. We believe this construction is interesting per se and may find applications in other problems of certification and self-testing of quantum devices. Our second construction is instead based on a single inequality—the elegant inequality introduced in [11]. In this case, we had to resort to SDP techniques to put a bound on the local randomness. A possible way to prove this bound analytically, would be to first prove that the elegant Bell inequality also provides a self-test for the maximally entangled state and the three Pauli measurements on Alice's side. It would then be possible to add the four-outcome measurement on Bob's side and use the same proof in our first construction to conclude that it generates two random bits.

Both constructions are quite sensitive to noise, as a fraction of noise of the order of 0.01 makes the obtained randomness smaller than one bit, which can already be obtained with more robust constructions based on projective measurements. A natural open question is thus to identify robust and optimal setups for randomness certification using POVMs.

Finally, we also found a construction based on POVMs which yields more than two bits of global randomness, the best that can be obtained with projective measurements, but less than the theoretical maximum of four bits. It remains an open question whether this maximum can actually be attained.

Acknowledgments. We acknowledge financial support from the EU projects QALGO and SIQS, the ERC CoG QITBOX, the F.R.S.-FNRS under the project DIQIP, the Brussels-Capital Region through a BB2B grant, the Spanish project FOQUS, the Generalitat de Catalunya (SGR875), the Hungarian National Research Fund OTKA (K111734), the János Bolyai Programme of the Hungarian Academy of Sciences, and the John Templeton Foundation. S.P. is supported by the FRS-FNRS as a Research Associate.

[1] J. Bell, Physics **1**, 195 (1964).

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

[3] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).

[4] O. Nieto-Silleras, S. Pironio, and J. Silman, New J. Phys. **16**, 013035 (2014).

[5] J.-D. Bancal, L. Sheridan, and V. Scarani, New J. Phys. **16**, 033011 (2014).

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

[7] U. Vazirani and T. Vidick, arXiv:1111.6054.

[8] C. A. Miller and Y. Shi, arXiv:1411.6608.

[9] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).

[10] G. de la Torre, M. J. Hoban, C. Dhara, G. Prettico, and A. Acín, Phys. Rev. Lett. **114**, 160502 (2015).

[11] N. Gisin, arXiv:quant-ph/0702021v2.

[12] T. Vértesi and E. Bene, Phys. Rev. A **82**, 062115 (2010).

[13] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007); New J. Phys. **10**, 073013 (2008).

[14] C. Dhara, G. Prettico, and A. Acín, Phys. Rev. A **88**, 052116 (2013).

[15] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, J. Phys. A: Math. Theor. **47**, 424028 (2014).

[16] G. M. D'Ariano, P. Lo Presti, and P. Perinotti, J. Phys. A: Math. Gen. **38**, 5979 (2005).

[17] J. F. Clauser *et al.*, Phys. Rev. Lett. **23**, 880 (1969).

[18] M. McKague, arXiv:1006.2352.

[19] M. McKague and M. Mosca, arXiv:1006.0150.

[20] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.93.040102 for a proof on the optimal quantum violation of the elegant Bell inequality and for a detailed description of the construction to generate global randomness exceeding 2 bits.

[21] P. Wittek, ACM Trans. Math. Software **41**, 21 (2015).

[22] M. Nakata, in *Proceedings of the IEEE International Symposium on Computer-Aided Control System Design* (IEEE, 2010), pp. 29–34.