Elemental and tight monogamy relations in nonsignaling theories

R. Augusiak,[1] M. Demianowicz,[1] M. Pawłowski,[2] J. Tura,[1] and A. Acín[1,3]
[1]*ICFO–Institut de Ciències Fotòniques, 08860 Castelldefels (Barcelona), Spain*
[2]*Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*
[3]*ICREA–Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain*
(Received 26 July 2013; revised manuscript received 17 October 2014; published 17 November 2014)

Physical principles constrain the way nonlocal correlations can be distributed among distant parties. These constraints are usually expressed by monogamy relations that bound the amount of Bell inequality violation observed among a set of parties by the violation observed by a different set of parties. We prove here that much stronger monogamy relations are possible for nonsignaling correlations by showing how nonlocal correlations among a set of parties limit *any* form of correlations, not necessarily nonlocal, shared among other parties. In particular, we provide tight bounds between the violation of a family of Bell inequalities among an arbitrary number of parties and the knowledge an external observer can gain about outcomes of *any single* measurement performed by the parties. Finally, we show how the obtained monogamy relations offer an improvement over the existing protocols for device-independent quantum key distribution and randomness amplification.

DOI: 10.1103/PhysRevA.90.052323 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

It is a well established fact that entanglement and nonlocal correlations (cf. Refs. [1,2]), i.e., correlations violating a Bell inequality [3], are fundamental resources of quantum information theory. It has been confirmed by many instances that, when distributed among spatially separated observers, they give an advantage over classical correlations at certain information-theoretic tasks, many of them being considered in the multipartite scenario. For instance, nonlocal correlations outperform their classical counterpart at communication complexity problems [4] and allow for security not achievable within classical theory [5,6].

Physical principles impose certain constraints on the way these resources can be distributed among separated parties; these are commonly referred to as monogamy relations. For instance, in any three-qubit pure state, one party cannot share a large amount of entanglement, as measured by concurrence, simultaneously with both remaining parties [7]. Analogous monogamy relations, both in qualitative [8–11] and quantitative [12,13] form, were demonstrated for nonlocal correlations, with the measure of nonlocality being the violation of specific Bell inequalities. In particular, Toner and Verstraete [12] and later Toner [13] showed that if three parties A, B, and C share, respectively, quantum and general nonsignaling correlations, then only a single pair can violate the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [14]. These findings were generalized to more complex scenarios [15,16] (see also Ref. [17]), and in particular, in Ref. [15] a general construction of monogamy relations for nonsignaling correlations from any bipartite Bell inequality was proposed.

In this work, we demonstrate that nonsignaling correlations are monogamous in a much stronger sense: the amount of nonlocality observed by a set of parties may imply severe limitations on any form of correlations with other parties. That is, instead of comparing nonlocality between distinct groups of parties, we rather relate it to the knowledge that external parties can gain on outcomes of any of the measurements performed by the parties (see Fig. 1). To be more illustrative, consider again parties A, B, and C performing a Bell experiment with M observables and d outcomes. We construct tight bounds between the violation of certain Bell inequalities [10] among any pair of parties, say A and B, and classical correlations that the third party C can establish with outcomes of any measurement performed by A or B. This means that the amount of *any* correlations—classical or nonlocal—that C could share with A or B is bounded by the strength of the Bell inequality violation between A and B. Our monogamies are further generalized to the scenario with an arbitrary number of parties N [(N,M,d) scenario], with nonlocality measured by the recent generalization of the Bell inequalities [10] presented in Ref. [11]. The obtained monogamy relations are logically independent from, and are in fact stronger than, the existing relations involving only nonlocal correlations, as a bound on nonlocal correlations does not necessarily imply any nontrivial constraint on the amount of classical correlations.

Our monogamy relations prove useful in device-independent protocols [6,18–21]. First, we show that they impose tight bounds on the guessing probability, the commonly used measure of randomness, that are significantly better than the existing ones [10,11]. We then argue that this translates into superior performance in protocols for device-independent quantum key distribution (DIQKD) [22] using measurements with more than two outputs. Finally, we show that they allow for a generalization of the results of [19] on randomness amplification to any number of parties and outcomes, demonstrating, in particular, that an arbitrary amount of arbitrarily good randomness can be amplified in a bipartite setup.

Before turning to the results, we provide some background. Consider N parties $A^{(1)},\ldots,A^{(N)}$ (for $N=3$ denoted by A,B,C), each measuring one of M possible observables $A^{(i)}_{x_i}$ ($x_i=1,\ldots,M$) with d outcomes (enumerated by $a_i=1,\ldots,d$) on their local physical systems. The produced correlations are described by a collection of probabilities $p(A^{(1)}_{x_1}=a_1,\ldots,A^{(N)}_{x_N}=a_N)\equiv p(a_1\ldots a_N|x_1\ldots x_N)\equiv p(\boldsymbol{a}|\boldsymbol{x})$ of obtaining results $\boldsymbol{a}\equiv a_1\ldots a_N$ upon measuring $\boldsymbol{x}\equiv x_1\ldots x_N$. One then says that the correlations $\{p(\boldsymbol{a}|\boldsymbol{x})\}$ are (i) nonsignaling (NC) if any of the marginals describing a subset of parties is independent of the measurement choices

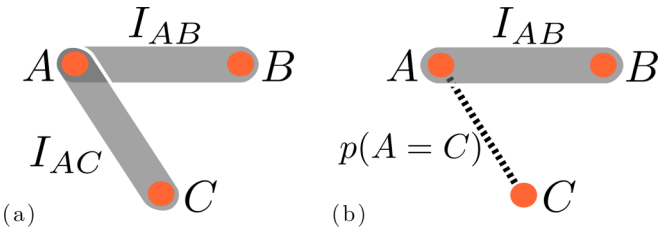

FIG. 1. (Color online) (a) The usual monogamies compare nonlocality (measured by the value of some Bell expression I) between different groups of parties (here between two pairs of parties AB and AC). Instead, (b) our monogamy relations compare nonlocality observed by a group of parties (here AB) to the knowledge, represented by the probability $p(A=C)$, the third party C can have about the outcomes observed by either of the parties. As such, they are qualitatively different, and in fact stronger than those of type (a).

made by the remaining parties and (ii) quantum (QC) if they arise by local measurements on quantum states (cf. [2]).

II. ELEMENTAL AND TIGHT MONOGAMIES FOR NONSIGNALING CORRELATIONS

We start with the derivation of our monogamy relations in the case of nonsignaling correlations. For clarity, we begin with the simplest tripartite scenario. We will use the Bell inequality introduced by Barrett, Kent, and Pironio (BKP) [10]. Denoting by $\langle\Omega\rangle$ the mean value of a random variable Ω, that is, $\langle\Omega\rangle = \sum_{i=1}^{d-1} i\,P(\Omega=i)$, it reads

$$I_{AB}^{2,M,d} := \sum_{\alpha=1}^{M}(\langle[A_\alpha - B_\alpha]\rangle + \langle[B_\alpha - A_{\alpha+1}]\rangle) \geqslant d-1, \quad (1)$$

with $[\Omega]$ being Ω modulo d, and $\Omega_{M+1} := [\Omega_1 + 1]$. For $d = 2$, inequality (1) reproduces the chained Bell inequalities [23], while for $M = 2$ the Collins-Gisin-Linden-Massar-Popescu (CGLMP) inequalities [24]. The maximal nonsignaling violation of (1) is $I_{AB}^{2,M,d} = 0$.

The only monogamy relations for (1) have been formulated in terms of its violations between Alice and M Bobs [15], which is a natural quantitative extension of the concept of M shareability [8]. In the following theorem we show that the BKP Bell inequalities allow one to introduce *elemental* monogamies obeyed by any NC.

Theorem 1. For any tripartite nonsignaling correlations $\{p(abc|xyz)\}$ with Md-outcome measurements, the inequality

$$I_{AB}^{2,M,d} + \langle[X_i - C_j]\rangle + \langle[C_j - X_i]\rangle \geqslant d-1 \quad (2)$$

holds for any pair $i,j = 1,\ldots,M$ and X denoting A or B.

Proof. Let us start with the case of $X = A$ and then notice that for a random variable Ω it holds that $\langle[\Omega]\rangle + \langle[-\Omega - 1]\rangle = d-1$ (see Appendix A). Consequently,

$$\sum_{\substack{\beta=1\\ \beta\neq i}}^{M}(\langle[C_j - A_\beta - 1]\rangle + \langle[A_\beta - C_j]\rangle) - (M-1)(d-1) \quad (3)$$

is equal to zero. The fact that for any β and j it holds that $\langle[C_j - A_\beta - 1]\rangle + \langle[A_\beta - C_j]\rangle = d-1 = \langle[A_\beta - C_j - 1]\rangle + \langle[C_j - A_\beta]\rangle$ allows us to rewrite (3) in the following way:

$$\begin{aligned}&\sum_{\beta=1}^{i-1}(\langle[C_j - A_\beta - 1]\rangle + \langle[A_{\beta+1} - C_j]\rangle)\\ &\quad + \sum_{\beta=i+1}^{M}(\langle[A_\beta - C_j - 1]\rangle\\ &\quad + \langle[C_j - A_\beta]\rangle) - (M-1)(d-1). \end{aligned} \quad (4)$$

Then, by adding $\langle[A_i - C_j]\rangle + \langle[C_j - A_i]\rangle$ to both sides of the above and rearranging some terms in the resulting expression, one obtains

$$\begin{aligned}&\langle[A_i - C_j]\rangle + \langle[C_j - A_i]\rangle\\ &= \sum_{\beta=1}^{i-1}(\langle[C_j - A_\beta - 1]\rangle + \langle[A_{\beta+1} - C_j]\rangle)\\ &\quad + \sum_{\beta=i}^{M-1}(\langle[A_{\beta+1} - C_j - 1]\rangle + \langle[C_j - A_\beta]\rangle)\\ &\quad + \langle[A_1 - C_j]\rangle + \langle[C_j - A_M]\rangle - (M-1)(d-1). \end{aligned} \quad (5)$$

In an analogous way, we may decompose $I_{AB}^{2,M,d}$:

$$\begin{aligned}I_{AB}^{2,M,d} &= \sum_{\alpha=1}^{i-1}(\langle[A_\alpha - B_\alpha]\rangle + \langle[B_\alpha - A_{\alpha+1}]\rangle)\\ &\quad + \sum_{\alpha=i}^{M-1}(\langle[A_\alpha - B_\alpha]\rangle + \langle[B_\alpha - A_{\alpha+1}]\rangle)\\ &\quad + \langle[A_M - B_M]\rangle + \langle[B_M - A_1 - 1]\rangle. \end{aligned} \quad (6)$$

In the last step of these manipulations, we add line by line Eqs. (5) and (6) in order to finally obtain

$$\begin{aligned}&I_{AB}^{2,M,d} + \langle[A_i - C_j]\rangle + \langle[C_j - A_i]\rangle\\ &= \sum_{\alpha=1}^{i-1}(\langle[C_j - A_\alpha - 1]\rangle + \langle[A_\alpha - B_\alpha]\rangle + \langle[B_\alpha - A_{\alpha+1}]\rangle\\ &\quad + \langle[A_{\alpha+1} - C_j]\rangle) + \sum_{\alpha=i}^{M-1}(\langle[C_j - A_\alpha]\rangle + \langle[A_\alpha - B_\alpha]\rangle\\ &\quad + \langle[B_\alpha - A_{\alpha+1}]\rangle + \langle[A_{\alpha+1} - C_j - 1]\rangle) + \langle[C_j - A_M]\rangle\\ &\quad + \langle[A_M - B_M]\rangle + \langle[B_M - A_1 - 1]\rangle\\ &\quad + \langle[A_1 - C_j]\rangle - (M-1)(d-1). \end{aligned} \quad (7)$$

What we have arrived at is basically the sum of M Bell expressions $I^{2,2,d}$ but "distributed" among three parties in such a way that Bob and Charlie measure only a single observable. It was shown in [15] that the minimal value such an expression can achieve over nonsignaling correlations is precisely its classical bound $d-1$. As a result, $I_{AB}^{2,M,d} + \langle[A_i - C_j]\rangle + \langle[C_j - A_i]\rangle \geqslant M(d-1) - (M-1)(d-1) = d-1$, finishing the proof for the case $X = A$.

If $X = B$ in inequality (2), then it suffices to rewrite the Bell expression from (1) as

$$I_{AB}^{2,M,d} = \sum_{\alpha=1}^{M} (\langle [B_\alpha - A_{\alpha+1}] \rangle + \langle [A_{\alpha+1} - B_{\alpha+1}] \rangle), \qquad (8)$$

add to it the zero expression (3) with A replaced by B, and repeat the above manipulations. This completes the proof. ■

Interestingly, all these inequalities are tight in the sense that for any values of $I_{AB}^{2,M,d}$ and $\langle [X_i - C_j] \rangle + \langle [C_j - X_i] \rangle$ saturating (2), one can find NC realizing these values. Take, for instance, a probability distribution $\{p(a,b,c|x,y,z) = p(a,b|x,y)p(c|z)\}$, with $\{p(a,b|x,y)\}$ being a mixture of a nonlocal model maximally violating (1) and a local deterministic model saturating it. Then, $\{p(c|z)\}$ is the same distribution as that used by A or B in the local model saturating (1).

The physical interpretation of our monogamies can be now concluded if we rewrite them in a bit different form. Using the fact that for any variable Ω, $\langle [\Omega] \rangle + \langle [-\Omega] \rangle = dP([\Omega] \neq 0) = d[1 - P([\Omega] = 0)]$ (see Appendix A), inequalities (2) transform to

$$I_{AB}^{2,M,d} + 1 \geqslant dp(X_i = C_j) \qquad (9)$$

for $X = A, B$, and any pair $i, j = 1, \ldots, M$. These relations hold if AB is replaced by any pair of parties and if any $m = 1, \ldots, d-1$ is added modulo d to the argument of probability. The meaning of the introduced monogamy relations is now transparent. The probability $p(X_i = C_j)$ that parties X and C obtain the same results upon measuring the ith and jth observables is a measure of how the outcomes of these measurements are classically correlated. Consequently, inequalities (2) establish tradeoffs between nonlocality, as measured by (1), that can be generated between any two parties and classical correlations that the third party can share with the results of any measurement performed by any of these two parties. Furthermore, they are tight. In fact, it is known that the maximal NC violation of (1), $I_{AB}^{2,M,d} = 0$, implies $p(X_i = C_j) = 1/d$ for any $i, j = 1, \ldots, M$, meaning that at the point of maximal violation C cannot share any correlations with any other party's measurement outcomes [10]. On the other hand, it is well known that at the point of no violation C can be arbitrarily correlated with A and B. For intermediate violations, the best one can hope for is a linear interpolation between these two extreme values, and this is precisely what our monogamy relations predict (see Fig. 2).

Let us now move to the general case of an arbitrary number of parties each having M d-outcome observables at their disposal. To this end, we will utilize the generalization of the Bell inequality (1) introduced in Ref. [11], which, most conveniently, can be stated in a recursive form as

$$I_{\mathsf{A}}^{N,M,d} = \frac{1}{M} \sum_{\alpha_{N-1}=1}^{M} I_{A^{(1)}\ldots A^{(N-1)}}^{N-1,M,d}(\alpha_{N-1}) \circ A_{\alpha_{N-1}}^{(N)} \geqslant d - 1, \qquad (10)$$

where $\mathsf{A} = A^{(1)} \ldots A^{(N)}$. The notation $\circ A_\gamma^{(i)}$ means insertion of $A_\gamma^{(i)}$ to the average $\langle \cdot \rangle$ with the opposite sign to the one of $A_\delta^{(i-1)}$ with any γ, δ, while $I_{A^{(1)}\ldots A^{(N-1)}}^{N-1,M,d}(\alpha_{N-1})$ is the same Bell expression as in (10), but for $N-1$ parties, and with observables of the last party relabeled as $\alpha_{N-2} \to \alpha_{N-2} + \alpha_{N-1} - 1$ with $\alpha_{N-1} = 1, \ldots, M$. The maximal nonsignalling violation of (10) is $I_{\mathsf{A}}^{N,M,d} = 0$. Then, the generalization of Theorem 1 to arbitrary N goes as follows:

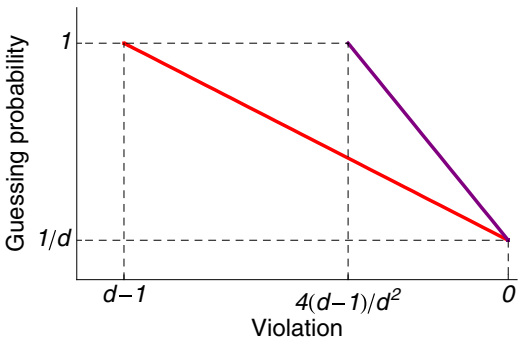

FIG. 2. (Color online) Comparison of the upper bounds on GP: present bound (32) (red line) and (33) (purple line). Our bound is tight—for any value $0 \leqslant I_{\mathsf{A}}^{N,M,d} \leqslant d-1$, it provides the maximum attainable value of GP. Instead, the bound (33) is nontrivial only in some restricted range of $I_{\mathsf{A}}^{N,M,d}$, namely, when $I_{\mathsf{A}}^{N,M,d} < 4(d-1)/d^2$, which tends to zero for $d \to \infty$.

Theorem 2. For any $(N+1)$–partite NC $\{p(\boldsymbol{a}|\boldsymbol{x})\}$ with M d-outcome measurements per site, the following inequality,

$$I_{\mathsf{A}}^{N,M,d} + \left\langle \left[A_{x_k}^{(k)} - A_{x_{N+1}}^{(N+1)} \right] \right\rangle + \left\langle \left[A_{x_{N+1}}^{(N+1)} - A_{x_k}^{(k)} \right] \right\rangle \geqslant d - 1, \qquad (11)$$

is satisfied for any $x_k, x_{N+1} = 1, \ldots, M$ and $k = 1, \ldots, N$.

Proof. The recursive formula in inequality (10), which for convenience we restate here

$$I_{\mathsf{A}}^{N,M,d} = \frac{1}{M} \sum_{\alpha_{N-1}=1}^{M} I_{A^{(1)}\ldots A^{(N-1)}}^{N-1,M,d}(\alpha_{N-1}) \circ A_{\alpha_{N-1}}^{(N)}, \qquad (12)$$

allows us to demonstrate the theorem inductively. The case of $N = 2$ has already been proved as Theorem 1, so we consider $N = 3$. Exploiting Eq. (12), one can express $I_{A^{(1)}A^{(2)}A^{(3)}}^{3,M,d}$ as

$$I_{A^{(1)}A^{(2)}A^{(3)}}^{3,M,d} = \frac{1}{M} \sum_{\alpha_2=1}^{M} I_{A^{(1)}A^{(2)}}^{2,M,d}(\alpha_2) \circ A_{\alpha_2}^{(3)}. \qquad (13)$$

It is clear that for every $\alpha_2 = 1, \ldots, M$,

$$I_{A^{(1)}A^{(2)}}^{2,M,d}(\alpha_2) = \sum_{\alpha_1=1}^{M} \left(\left\langle \left[A_{\alpha_1}^{(1)} - A_{\alpha_1+\alpha_2-1}^{(2)} \right] \right\rangle + \left\langle \left[A_{\alpha_1+\alpha_2-1}^{(2)} - A_{\alpha_1+1}^{(1)} \right] \right\rangle \right) \geqslant d - 1 \qquad (14)$$

is a Bell inequality equivalent to (1), in which the observables of the second party $A^{(2)}$ have been relabelled according to $\alpha_1 \to \alpha_1 + \alpha_2 - 1$. It must then fulfil the monogamy relations (2) (with $N = 2$) independently of the value of α_2. In order to see it in a more explicit way, let us consider the case $k = 1$, and in Eq. (7) just rename $A \to A^{(1)}$, $B \to A^{(2)}$, and $C \to A^{(3)}$, and also $\alpha \to \alpha_1$ for the first party, while $\alpha \to \alpha_1 + \alpha_2 - 1$ for the second one. Then, for those observables $A_{\alpha_1+\alpha_2-1}^{(2)}$ for which $\alpha_1 + \alpha_2 - 1 > M$ we use the rule $X_{i \times M + \gamma} = [X_\gamma + i]$ to get $[A_\gamma^{(2)} + i]$ with some γ and i, and later replace the latter by another variable $\widetilde{A}_\gamma^{(2)}$ (this is

just $A_\gamma^{(2)}$ with outcomes shifted by a constant). With the aid of formula (8), the same reasoning can be repeated for $k = 2$.

Now, we prove that each term in Eq. (13) fulfills (11) for $N = 3$, that is, that the inequalities

$$I^{2,M,d}_{A^{(1)}A^{(2)}}(\alpha_2) \circ A^{(3)}_{\alpha_2} + \langle [A^{(k)}_{x_k} - A^{(4)}_{x_4}] \rangle + \langle [A^{(4)}_{x_4} - A^{(k)}_{x_k}] \rangle \geqslant d - 1 \tag{15}$$

hold for any $\alpha_2 = 1, \ldots, M$, any pair $x_k, x_4 = 1, \ldots, M$, and any $k = 1,2,3$.

First assume $k = 1$. Let us write explicitly $I^{2,M,d}_{A^{(1)}A^{(2)}}(\alpha_2) \circ A^{(3)}_{\alpha_2}$ as

$$I^{2,M,d}_{A^{(1)}A^{(2)}}(\alpha_2) \circ A^{(3)}_{\alpha_2} = \sum_{\alpha_1=1}^{M} \big(\langle [A^{(1)}_{\alpha_1} - A^{(2)}_{\alpha_1+\alpha_2-1} + A^{(3)}_{\alpha_2}] \rangle + \langle [A^{(2)}_{\alpha_1+\alpha_2-1} - A^{(1)}_{\alpha_1+1} - A^{(3)}_{\alpha_2}] \rangle \big). \tag{16}$$

For any fixed α_2, the last party measures solely a single observable, and therefore we treat $A^{(2)}_{\alpha_1+\alpha_2-1} - A^{(3)}_{\alpha_2}$ as a single variable, or, in other words, for any $\alpha_2 = 1, \ldots, M$, $A^{(2)}_{\alpha_1+\alpha_2-1} - A^{(3)}_{\alpha_2}$ is a d-outcome observable [recall that in Eq. (16) all variables are modulo d]. Effectively, (15) is a three-partite inequality of the form (11) (with $N = 2$) that has just been proven. In the $k = 2$ case we insert the third party into the alternative expression (8) and further apply the same reasoning as above.

In order to show (11) for $k = 3$, we use the fact that the Bell inequality (10) for $N = 3$ is invariant under the exchange of the first and the third party [11], meaning that we can, analogously to Eq. (13), write it down as

$$I^{3,M,d}_{A^{(1)}A^{(2)}A^{(3)}} = \frac{1}{M} \sum_{\alpha_2=1}^{M} I^{2,M,d}_{A^{(3)}A^{(2)}}(\alpha_2) \circ A^{(1)}_{\alpha_2}. \tag{17}$$

Now, it is enough to repeat the above reasoning to complete the proof of the monogamy relations (11) for $N = 3$.

Having it proven for $N = 3$, let us now assume that the theorem is true for N parties (any N-partite nonsignaling probability distribution). In order to complete the proof, we again refer to the recursive formula (12). By grouping together the last two parties, each term in the sum in Eq. (12) is effectively an $(N-1)$-partite Bell expression for which we have just assumed (11) to hold for any x_k, x_N and $k = 1, \ldots, N$. Performing the summation over α_{N-1} and dividing further by M^{N-2}, we obtain (11) for any i, j and $k = 1, \ldots, N-1$. The case $k = N$ can be reached by using the fact that $I^{N,M,d}$ is invariant under exchange of the last and the $(N-2)$th party [11]. ■

All the properties of the three-partite monogamy relations persist for any N. In particular, all inequalities (11) are tight. Moreover, they can be rewritten as

$$I^{N,M,d}_{\mathsf{A}} + 1 \geqslant dp\big(A^{(k)}_{x_k} = [A^{(N+1)}_{x_{N+1}} + m]\big) \tag{18}$$

for any $x_k, x_{N+1} = 1, \ldots, M$, $k = 1, \ldots, N$, and $m = 0, \ldots, d-1$ and remain valid if the nonlocality is tested among any N-element subset of $N+1$ parties. Analogously to the three-partite case, inequalities (18) tightly relate the nonlocality observed by any N parties, as measured by $I^{N,M,d}_{\mathsf{A}}$, and correlations that $(N+1)$th party can share between measurement outcomes of any of these N parties. It is worth pointing out that for $d = 2$ it holds that $\langle [X - Y] \rangle = \langle [Y - X] \rangle$, and inequalities (11) simplify to $I^{N,M,2}_{\mathsf{A}} + 2\langle [A^{(k)}_{x_k} - A^{(N+1)}_{x_{N+1}}] \rangle \geqslant 1$, which can be rewritten in a more familiar form as $|\langle A^{(k)}_{x_k} A^{(N+1)}_{x_{N+1}} \rangle| \leqslant I^{N,M,2}_{\mathsf{A}}$, where $A^{(k)}_{x_k}$ stand now for dichotomic observables with outcomes ± 1, while $\langle XY \rangle = P(X = Y) - P(X \neq Y)$. Thus the strength of violation of (10) imposes tight bounds on a *single* mean value $\langle A^{(k)}_{x_k} A^{(N+1)}_{x_{N+1}} \rangle$ for any x_k, x_{N+1} and $k = 1, \ldots, N$, which is also a measure of how outcomes of a measurement performed by the external party $A^{(N+1)}$ are correlated to those of $A^{(k)}$ for any k. In particular, when $I^{N,M,2}_{\mathsf{A}} = 0$ (maximal nonsignaling violation), all these means are zero, while maximal correlations between a single pair of measurements, i.e., $\langle A^{(k)}_{x_k} A^{(N+1)}_{x_{N+1}} \rangle = \pm 1$ for some x_k, x_{N+1}, making the N parties unable to violate $I^{N,M,2}_{\mathsf{A}} \geqslant 1$.

III. ELEMENTAL MONOGAMIES FOR QUANTUM CORRELATIONS

One may further ask if it is possible to formulate analogous monogamy relations for QC. In general, the quantum case is much more difficult to handle and the only progress in this direction has been achieved for Bell inequalities with two dichotomic settings [12,16] (see also Ref. [17]). Here, we show that in the simplest (3,2,2) scenario, one can derive quantum analogs of the nonsignaling monogamies (2). To this end, we use a one-parameter modification of the CHSH Bell inequality [14], with the latter being a particular case of the Bell inequality (1) with $M = d = 2$. However, here we write it down in its "standard" form

$$\widetilde{I}^{\alpha}_{AB} = \alpha(\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle) + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle \leqslant 2\alpha \tag{19}$$

with $\alpha \geqslant 1$. Here A_i and B_i are local quantum observables with eigenvalues ± 1 and $\langle XY \rangle = \mathrm{Tr}[\rho(X \otimes Y)]$ for some quantum state ρ and local observables X, Y. Actually, one proves the following more general theorem, generalizing the result of Ref. [12] for the Bell inequality (19).

Theorem 3. Any three-partite quantum correlations with two dichotomic measurements per site must satisfy the following inequalities:

$$\alpha^2 \max\big\{(\widetilde{I}^{\alpha}_{AB})^2, (\widetilde{I}^{\alpha}_{AC})^2\big\} + \min\big\{(\widetilde{I}^{\alpha}_{AB})^2, (\widetilde{I}^{\alpha}_{AC})^2\big\} \leqslant 4\alpha^2(1 + \alpha^2) \tag{20}$$

and

$$(\widetilde{I}^{\alpha}_{AB})^2 + 4\langle A_i C_j \rangle^2 \leqslant 4(1 + \alpha^2) \tag{21}$$

for any $\alpha \geqslant 1$ and $i, j = 1,2$.

Proof. The proof is nothing more but a slight modification of the considerations of Ref. [12] (see also Ref. [25]). Nevertheless, we attach it here for completeness.

We start by noting that the monogamy regions, that is, the two-dimensional sets of allowed (realizable) within quantum theory pairs $\{\widetilde{I}^{\alpha}_{AB}, \widetilde{I}^{\alpha}_{AC}\}$ for inequality (20) and $\{\widetilde{I}^{\alpha}_{AB}, \langle A_i C_j \rangle\}$ with fixed i and j for inequality (21), must be convex. Therefore, as it is shown in Ref. [12] (see also Ref. [26]), every point of their boundaries can be realized with a real three-qubit pure state and real local one-qubit measurements.

Recall that the latter assume the form

$$X = \boldsymbol{x}\cdot\boldsymbol{\sigma}, \tag{22}$$

with $\boldsymbol{x}\in\mathbb{R}^2$ being a unit vector and $\boldsymbol{\sigma}=[\sigma_x,\sigma_z]$ denoting a vector consisting of the standard Pauli matrices σ_x and σ_z.

Then, it follows from a series of papers [12,25,27] that for a given two-qubit state ρ_{AB}, the maximal value of $\widetilde{I}^{\alpha}_{AB}$ over local, real, and traceless observables [i.e., those of the form (22)] measured by Alice A_i and Bob B_i amounts to

$$\max_{A_i,B_j}\left(\widetilde{I}^{\alpha}_{AB}\right)=2\sqrt{\alpha^2\lambda_1+\lambda_2}. \tag{23}$$

Here, λ_i $(i=1,2)$ denotes the eigenvalues of $T_{AB}T_{AB}^T$ put in a decreasing order, i.e., $\lambda_1\geqslant\lambda_2$, and T_{AB} is the following reduced correlation matrix:

$$T_{AB}=\begin{pmatrix}\langle\sigma_x\otimes\sigma_x\rangle_{AB} & \langle\sigma_x\otimes\sigma_z\rangle_{AB}\\ \langle\sigma_z\otimes\sigma_x\rangle_{AB} & \langle\sigma_z\otimes\sigma_z\rangle_{AB}\end{pmatrix}. \tag{24}$$

We added the subscript AB in (24) to indicate that the mean values are taken in the state ρ_{AB}. In particular, one can similarly compute the maximal value of a single average $\langle AB\rangle$ in the state ρ_{AB} over local observables A and B of the form (22) to be

$$\max_{A,B}\langle AB\rangle=\lambda_1. \tag{25}$$

Equipped with these facts, we can now turn to the proof of the inequalities (20) and (21). We start from the first one and note that it suffices to demonstrate it in the case of $\widetilde{I}^{\alpha}_{AB}\geqslant\widetilde{I}^{\alpha}_{AC}$, in which it becomes

$$\alpha^2\left(\widetilde{I}^{\alpha}_{AB}\right)^2+\left(\widetilde{I}^{\alpha}_{AC}\right)^2\leqslant 4\alpha^2. \tag{26}$$

The opposite case will follow immediately by exchanging $B\leftrightarrow C$.

Then let $|\psi_{ABC}\rangle$ be a pure real three-qubit state. By ρ_{AB} and ρ_{AC} we denote its subsystems arising by tracing out the third and the second party, respectively, and by T_{AB} and T_{AC} the corresponding correlation matrices [cf. Eq. (24)]. Finally, let λ_i and $\widetilde{\lambda}_i$ $(i=1,2)$ be eigenvalues of $T_{AB}T_{AB}^T$ and $T_{AC}T_{AC}^T$, respectively, where we keep the convention that $\lambda_1\geqslant\lambda_2$ and $\widetilde{\lambda}_1\geqslant\widetilde{\lambda}_2$. It was pointed out in Ref. [12] that the latter matrices are diagonal in the same basis, which allows one to simultaneously maximize both $\widetilde{I}^{\alpha}_{AB}$ and $\widetilde{I}^{\alpha}_{AC}$ with the same observables on Alice site. This, together with Eq. (23), means that

$$\begin{aligned}\max_{\substack{A_i,B_j,\\ C_k}}\left[\alpha^2\left(\widetilde{I}^{\alpha}_{AB}\right)^2+\left(\widetilde{I}^{\alpha}_{AC}\right)^2\right]&=4[\alpha^2(\alpha^2\lambda_1+\lambda_2)+\alpha^2\widetilde{\lambda}_1+\widetilde{\lambda}_2]\\ &=4[\alpha^4\lambda_1+\alpha^2(\lambda_2+\widetilde{\lambda}_1)+\widetilde{\lambda}_2].\end{aligned} \tag{27}$$

In order to complete the proof, we make use of the Toner-Verstraete monogamy relation for the CHSH Bell inequality [12], which we state here in terms of λ_i and $\widetilde{\lambda}_i$ as

$$\lambda_2+\widetilde{\lambda}_1\leqslant 2-\lambda_1-\widetilde{\lambda}_2. \tag{28}$$

When applied to (27), it leads us to

$$\begin{aligned}\max_{\substack{A_i,B_j,\\ C_k}}\left[\alpha^2\left(\widetilde{I}^{\alpha}_{AB}\right)^2+\left(\widetilde{I}^{\alpha}_{AC}\right)^2\right]&\leqslant 4[(\alpha^2-1)(\alpha^2\lambda_1-\widetilde{\lambda}_2)+2\alpha^2]\\ &=4[\alpha^2(\alpha^2-1)+2\alpha^2]\\ &=4\alpha^2(1+\alpha^2),\end{aligned} \tag{29}$$

where the second line follows form the facts that $\lambda_1\leqslant 1$, $\widetilde{\lambda}_2\geqslant 0$, and $\alpha\geqslant 1$.

To prove inequality (21), we follow the above reasoning to obtain

$$\begin{aligned}\max_{A_i,B_j,C_l}\left[\left(\widetilde{I}^{\alpha}_{AB}\right)^2+4\langle A_kC_l\rangle^2\right]&=4(\alpha^2\lambda_1+\lambda_2)+4\widetilde{\lambda}_1\\ &=4\alpha^2\lambda_1+4(\lambda_2+\widetilde{\lambda}_1)\end{aligned} \tag{30}$$

for $k=1,2$. Subsequent application of (28) to the term in parentheses in the second line of the above directly gives inequality (21), completing the proof. ■

For $i=1$ and $j=1,2$, the relations (21) are tight since any pair of values of $\widetilde{I}^{\alpha}_{AB}$ and $\langle A_1C_j\rangle$ saturating them can be realized with the state $(\beta_+|01\rangle+\beta_-|10\rangle)|0\rangle$, where $\beta_\pm=(1/2)(1\pm\sqrt{2}\sin\theta)^{1/2}$ and $\theta\in[0,\pi/4]$. It is, however, no longer true for $i=2$. In this case we numerically found tight monogamy relations for particular values of α (see Fig. 3).

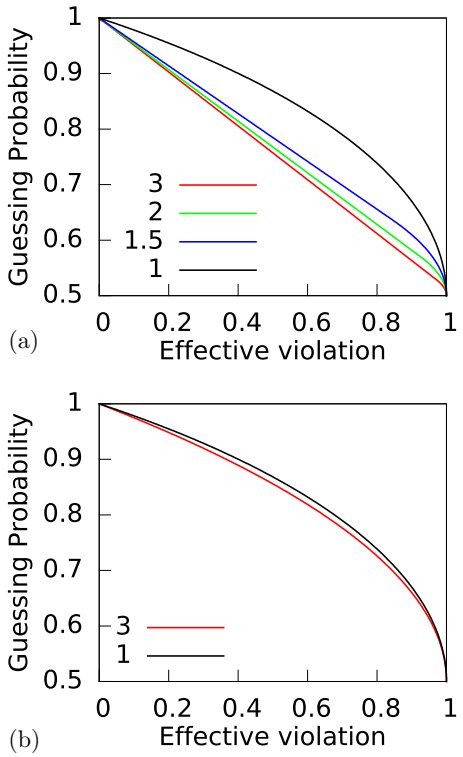

FIG. 3. (Color online) (a) Guessing probability (and simultaneously the tight analogs of monogamies in Theorem 3) for $i=2$ as a function of $(\widetilde{I}^{\alpha}_{AB}-2\alpha)/2(\sqrt{1+\alpha^2}-\alpha)$ for various values of α. All curves were found using two methods. First, we maximized the guessing probability for a given value of $\widetilde{I}^{\alpha}_{AB}$ over two-ququart states and one-ququart dichotomic measurements. Then, we used the hierarchy of Ref. [29] and with its third level we arrived at curves that coincide with those obtained with the first method with precision 10^{-7}. For comparison, (b) presents the corresponding nontight monogamies proven in theorem 3 ($i=2$) for $\alpha=1,3$ (the curves for $\alpha=1.5,2$ fall in between these two). The black curve is the same on both plots.

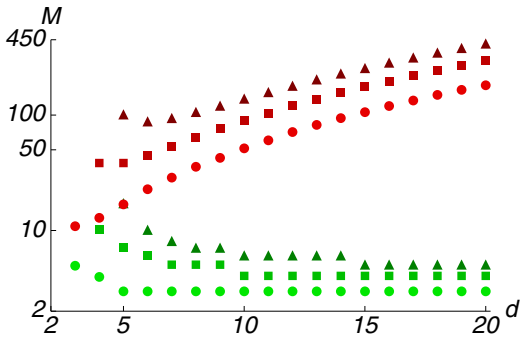

FIG. 4. (Color online) Minimal number of measurements M on a maximally entangled state of local dimension d necessary for the secret-key rate R secure against nonsignaling eavesdroppers to be at least one (dots), $\log_2 3$ (squares), and two (triangles) bits, when (32) (green) and (33) (red) are used to bound R. Using our bound the parties need to use many fewer measurements to reach the same key rate. Moreover, contrary to what is predicted by the previously known bound, the number of measurements decreases with the dimension.

IV. BOUNDS ON RANDOMNESS

Our monogamies are of particular importance for device-independent applications, since they imply upper bounds on the guessing probability (GP) of the outcomes of any measurement performed by any of the N parties by the additional party, here called E. Recall that one defines the guessing probability of an outcome of the measurement x_k performed by the kth party as

$$P_g(x_k) := \max_{a_k} p(A^{(k)}_{x_k} = a_k) = \max_{a_k} p(a_k|x_k). \tag{31}$$

Now, in order to derive bounds on $P_g(x_k)$, assume that E has full knowledge about all parties devices and their measurement choices and wishes to guess the outcomes of, say $A^{(k)}_{x_k}$. The best E can do for this purpose is to simply measure one of its observables, say the zth one, and, irrespectively of the obtained result, deliver the most probable outcome of $A^{(k)}_{x_k}$. Then, $\max_{a_k} p(A^{(k)}_{x_k} = a_k) = p(E_z = A^{(k)}_{x_k})$, and inequalities (18) imply that for any x_k and k, GP is bounded as

$$\max_{a_k} p(a_k|x_k) \equiv \max_{a_k} p\big(A^{(k)}_{x_k} = a_k\big) \leqslant \frac{1}{d}\big(1 + I_{\mathsf{A}}^{N,M,d}\big). \tag{32}$$

These bounds are tight and significantly stronger than the previously existing one,

$$\max_{a_k} p(a_k|x_k) \leqslant \frac{1}{d}\left[1 + \frac{d^N}{4}(N-1) I_{\mathsf{A}}^{N,M,d}\right], \tag{33}$$

derived in Refs. [10] and [11] (see Fig. 2).

Finally, let us notice that the quantum monogamies (21) impose the following upper bounds on the guessing probability:

$$\max_{j} p(X_i = j) \leqslant \tfrac{1}{2}\big\{1 + \big[1 + \alpha^2 - \big(\widetilde{I}^{\alpha}_{AB}/2\big)^2\big]^{1/2}\big\}, \tag{34}$$

with $X = A, B$, $i = 1,2$, and $\alpha \geqslant 1$. This bound was already derived in Ref. [27], and, as already said, it is tight only for $i = 1$. In the case $i = 2$, we determined the tight bounds numerically for a few values of α and present them in Fig. 3.

V. APPLICATIONS

Here we show how our bounds on the guessing probability (32) apply in device-independent tasks such as quantum key distribution and randomness amplification.

A. Quantum key distribution

Let us now discuss how the bound (32) performs in comparison to (33) in security proofs of DIQKD against no-signaling eavesdroppers. At the moment, a general security proof in this scenario is missing and the strongest proof requires the assumption that the eavesdropper E is not only limited by the no-signaling principle but also lacks a long-term quantum memory (the so-called bounded-storage model) [22]. Assume that Alice and Bob share a two-qudit maximally entangled state and they use it to maximally violate (1) by performing the optimal measurements for this setup (see, e.g., [10]). To generate the secure key, Bob performs one more measurement that is perfectly correlated to one of Alice's measurements. The key rate of this protocol is lower bounded as $R \geqslant -\log_2[\tau(I_{AB}^{2,M,d})] - H(A|B)$ [22], where τ is any upper bound on GP for nonsignaling correlations, and $H(A|B)$ is the conditional Shannon entropy between Alice and Bob for the measurements used to generate the secret key. As the state is maximally entangled, this term is equal to zero. Figure 4 compares bounds on the secret key obtained by using our bound (32) and the previous bound (33) in this protocol. We fix the key rate and compute the minimal number of measurements needed to attain this rate using these bounds as a function of the number of outputs. As shown in Fig. 4, the number of measurements when using our bound is much smaller and, in particular, decreases with the number of outputs.

B. Randomness amplification

Let us finally show the usefulness of our monogamy relations in randomness amplification. Assume that each party is given a sequence of bits produced by the Santha-Vazirani (SV) source (or the ε-source). Its working is defined as follows: it produces a sequence $y_1, y_2, \ldots, y_n$ of bits according to

$$\tfrac{1}{2} - \varepsilon \leqslant p(y_k|w) \leqslant \tfrac{1}{2} + \varepsilon, \quad k = 1, \ldots, n, \tag{35}$$

where w denotes any space-time variable that could be the cause of y_k. Thus the bits are possibly correlated with each other, retaining, however, some intrinsic randomness—we say that they are ε-free. The goal is now to obtain a perfectly random bit (or more generally $d$it) from an arbitrarily long sequence of ε-free bits by using quantum correlations that violate the Bell inequality (10). This procedure is called randomness amplification (RA).

It is useful to recast this task in the adversarial picture [19], in which one assumes that an adversary E, using the ε-sources, wants to simulate the quantum violation of (10) by NC, in particular, the local ones. The random variable W is now held by E, who uses it to control both the ε-sources and the physical devices possessed by the parties. That is, for every value w of W, the former provides settings $\boldsymbol{x}$ with probabilities obeying (35), while these devices generate the N-partite probability distribution $\{p(\boldsymbol{a}|\boldsymbol{x}, w)\}_{\boldsymbol{a},\boldsymbol{x}}$. Let us then denote by $\{p(a_k, w|\boldsymbol{x})\}_{a_k,w}$ correlations between outcomes

obtained by party k and the random variable W for a particular choice of measurement settings $\boldsymbol{x}$. Also, let $\{\widetilde{p}(a)\}$ be the one-party uniform probability distribution, i.e., $\widetilde{p}(a)=1/d$ for any a. Introducing then the variational distance

$$D(\{p(x)\},\{q(x)\})=\frac{1}{2}\sum_{x}|p(x)-q(x)| \tag{36}$$

between two probability distributions $\{p(x)\}$ and $\{q(x)\}$, we can now restate and generalize Lemma 1 of [19] (see also Appendix B for an alternative proof).

Theorem 4. Let for any w, $\{p(\boldsymbol{a}|\boldsymbol{x},w)\}_{\boldsymbol{a},\boldsymbol{x}}$ be an N-partite nonsignaling probability distribution. Then for any $k=1,\ldots,N$ and any choice of measurement settings $\boldsymbol{x}$:

$$\begin{aligned}&D(\{p(a_k,w|\boldsymbol{x})\}_{a_k,w},\{\widetilde{p}(a_k)p(w|\boldsymbol{x})\}_{a_k,w})\\&=\frac{1}{2}\sum_{a_k,w}|p(a_k,w|\boldsymbol{x})-\widetilde{p}(a_k)p(w|\boldsymbol{x})|\\&\leqslant\frac{(d-1)^2+1}{2d}\,Q_M(\boldsymbol{x})I_{\mathsf{A}}^{N,M,d},\end{aligned} \tag{37}$$

where $I_{\mathsf{A}}^{N,M,d}$ is taken in the probability distribution observed by the parties $\{p(\boldsymbol{a}|\boldsymbol{x})\}$. Then

$$Q_M(\boldsymbol{x})=\max_{w}\left[\frac{p(w|\boldsymbol{x})}{p_{\min}(w)}\right], \tag{38}$$

where $p_{\min}(w)=\min_{\boldsymbol{x}}\{p(w|\boldsymbol{x})\}$ with the minimum taken over all measurement settings $\boldsymbol{x}$ appearing in the Bell inequality (10).

Proof. For simplicity, but without any loss of generality, we prove this theorem for the bipartite case. The generalization to the multipartite case is straightforward.

As before, we denote the parties by A and B, while the adversary is denoted by E. Then, the corresponding inputs and outputs are denoted by x, y, z, and a, b, and e, respectively.

Let us start by noting that for any probability distribution $\{p(a,b|x,y,w)\}_{a,b,x,y}$, the maximal probability of local outcomes obtained by any of the parties, say, for simplicity, Alice, must obey the inequalities on the guessing probability [see inequality (7) in the main text]. That is,

$$\max_{a}p(a|x,w)\leqslant\frac{1}{d}\left(1+I_w^{2,M,d}\right) \tag{39}$$

for any $x=1,\ldots,M$, where by $I_w^{2,M,d}$ we have denoted the value of the Bell expression (1) computed for the probability distribution $\{p(a,b|x,y,w)\}_{a,b,x,y}$. Clearly, this bound holds also for any $p(a|x,w)$, which together with the normalization

$$p(a|x,w)=1-\sum_{\alpha\neq a}p(\alpha|x,w), \tag{40}$$

means that $p(a|x,w)\geqslant(1/d)[1-(d-1)I_w^{2,M,d}]$, and therefore the inequality

$$\left|p(a|x,w)-\frac{1}{d}\right|\leqslant\frac{d-1}{d}I_w^{2,M,d} \tag{41}$$

holds for any a and x. Using then the inequality (39) for $\max_a p(a|x,w)$ and (41) for the rest of $p(a|x,w)$, we obtain that for any strategy w and a measurement setting x,

$$\begin{aligned}D(\{p(a|x,w)\}_a,\{\widetilde{p}(a)\})&=\frac{1}{2}\sum_{a}|p(a|x,w)-\widetilde{p}(a)|\\&\leqslant\frac{(d-1)^2+1}{2d}I_w^{2,M,d}.\end{aligned} \tag{42}$$

The remainder of the proof goes along exactly the same lines as in Ref. [19]; however, for completeness, we will recall it here.

Due to the fact that the observers do not have access to the variable W, one has to average inequality (42) over the probability distribution $\{p(w|x,y)\}_w$ for a particular choice of measurements x and y. Together with the facts that $p(a|x,w)=p(a|x,y,w)$ (no-signaling) and $p(w|x,y)p(a|x,y,w)=p(a,w|x,y)$, this allows one to write

$$\begin{aligned}&D(\{p(a,w|x,y)\}_{a,w},\{\widetilde{p}(a)p(w|x,y)\}_{a,w})\\&=\frac{1}{2}\sum_{a,w}|p(a,w|x,y)-\widetilde{p}(a)p(w|x,y)|\\&\leqslant\frac{(d-1)^2+1}{2d}\sum_{w}p(w|x,y)I_w^{2,M,d}.\end{aligned} \tag{43}$$

Let us now concentrate on the right-hand side of inequality (43). By using Eq. (1), we can bound it from above in the following way:

$$\begin{aligned}&\sum_{w}p(w|x,y)I_w^{2,M,d}\\&=\sum_{w,\alpha}p(w|x,y)(\langle[A_\alpha-B_\alpha]\rangle_w+\langle[B_\alpha-A_{\alpha+1}]\rangle_w)\\&=\sum_{w,\alpha}\left(p(w|\alpha,\alpha)\frac{p(w|x,y)}{p(w|\alpha,\alpha)}\langle[A_\alpha-B_\alpha]\rangle_w\right.\\&\quad\left.+\,p(w|\alpha+1,\alpha)\frac{p(w|x,y)}{p(w|\alpha+1,\alpha)}\langle[B_\alpha-A_{\alpha+1}]\rangle_w\right)\\&\leqslant Q_M(x,y)\sum_{w,\alpha}[p(w|\alpha,\alpha)\langle[A_\alpha-B_\alpha]\rangle_w\\&\quad+\,p(w|\alpha+1,\alpha)\langle[B_\alpha-A_{\alpha+1}]\rangle_w]\\&=Q_M(x,y)\sum_{\alpha}(\langle[A_\alpha-B_\alpha]\rangle+\langle[B_\alpha-A_{\alpha+1}]\rangle)\\&=Q_M(x,y)I_{AB}^{2,M,d},\end{aligned} \tag{44}$$

where the subscript w in the expectation values $\langle[A_\alpha-B_\alpha]\rangle_w$ and $\langle[B_\alpha-A_{\alpha+1}]\rangle_w$ means that they are computed for the probability distribution $\{p(a,b|x,y,w)\}_{a,b,x,y}$, and also the convention $p(M+1,M|w)\equiv p(1,M|w)$ is used. Then, $I_{AB}^{2,M,d}$ is computed for the probability distribution $\{p(a,b|x,y)\}$ observed by A and B.

By substituting inequality (44) into inequality (43), one finally obtains inequality (37), completing the proof. ■

It then follows that if correlations $\{p(\boldsymbol{a}|\boldsymbol{x})\}$ violate maximally the Bell inequality (10), then the *dits* observed by the parties are perfectly random and uncorrelated from W [19].

Let us now show that one can amplify partially random input bits to almost perfectly random *dits* by using QC that produce an arbitrarily high violation of $I_{\mathsf{A}}^{N,M,d}$. To generate

one of the M measurement settings, each party uses its SV source $r = \lceil \log_2 M \rceil$ times. Hence for any $\boldsymbol{x}$,

$$Q_r(\boldsymbol{x}) \leqslant \left(\frac{1+2\varepsilon}{1-2\varepsilon}\right)^{Nr} \tag{45}$$

(cf. Ref. [19]). Then, there is a state and measurement settings [10,11] such that for large M,

$$I_{\mathsf{A}}^{N,M,d} \approx \lambda(d)/M \leqslant \lambda(d)/2^{r-1}, \tag{46}$$

where $\lambda(d)$ is a function of d. After plugging everything into (37), one checks that its right-hand side tends to zero for $M \to \infty$ if and only if

$$\varepsilon < \varepsilon_N := \frac{1}{2}\frac{2^{1/N}-1}{2^{1/N}+1}. \tag{47}$$

As a result, QC violating (46) can be used to amplify randomness of any ε-source provided $\varepsilon < \varepsilon_N$. In particular, for $N = 2$, the above reproduces the value $\varepsilon_2 = (\sqrt{2}-1)^2/2$ found in [19], and, because ε_N is a strictly decreasing function of N, the larger the value of N, the lower the critical epsilon ε_N for this method to work. Notice, however, that ε_N is independent of d, so almost perfectly random *dits* are obtained from partially random bits. This means that by using the setup from Ref. [19] we can in fact achieve both amplification and expansion of randomness simultaneously.

Recently, with the same Bell inequality but for $N = d = 2$, the critical ε was shifted from $\varepsilon_2 \approx 0.086$ to $\varepsilon_2' \approx 0.096\,1$ [20]. We will now show that by using a slightly different approach the critical epsilon can be almost doubled. To this end, we exploit the fact that only $2M^{N-1}$ measurement settings out of all possible M^N appear in $I_{\mathsf{A}}^{N,M,d}$. However, to generate them a *common* source has to be used. Assuming then that this is the case, $R = \log_2(2M^{N-1}) = 1 + (N-1)r$ (instead of Nr) uses of the SV source are enough to generate all measurement settings in $I_{\mathsf{A}}^{N,M,d}$. Thus

$$Q_r(\boldsymbol{x}) \leqslant \left(\frac{1+2\varepsilon}{1-2\varepsilon}\right)^{1+(N-1)r}, \tag{48}$$

which together with (46) implies that the right-hand side of (37) vanishes for $M \to \infty$ if and only if

$$\varepsilon < \varepsilon_N'' = \frac{1}{2}\frac{2^{1/(N-1)}-1}{2^{1/(N-1)}+1}, \tag{49}$$

and, in particular, $\varepsilon_2'' = 1/6 > \varepsilon_2'$.

VI. CONCLUSIONS

We have introduced a class of monogamy relations obeyed by any nonsignaling physical theory. They tightly relate the amount of nonlocality, as quantified by the violation of Bell inequalities [10,11], that N parties have generated in an experiment to the classical correlations an external party can share with outcomes of any measurement performed by the parties. Such tradeoffs find natural applications in device-independent protocols, and here we have discussed how they apply in quantum key distribution (cf. also Ref. [28]) and generation and amplification of randomness. We have finally shown that bipartite quantum correlations allow one to amplify ε-free *dits* for any $\varepsilon < 1/6$.

Our results provoke further questions. First, it is natural to ask if analogous monogamies hold for quantum correlations, and, in fact, such elemental monogamies can be derived in the simplest (3,2,2) scenario. From a more fundamental perspective, it is of interest to understand what is the (minimal) set of of monogamy relations generating the same set of multipartite correlations as the no-signaling principle.

ACKNOWLEDGMENTS

Discussions with Gonzalo De La Torre are gratefully acknowledged. This work is supported by NCN Grant No. 2013/08/M/ST2/00626, FNP TEAM, ERC Grants QITBOX, QOLAPS, and QUAGATUA, and the Spanish project Chist-Era DIQIP. This publication was made possible through the support of a grant from the John Templeton Foundation. R.A. also acknowledges the Spanish MINECO for support through the Juan de la Cierva Program.

APPENDIX A: A SIMPLE FACT

Here we prove a simple fact. Recall for this purpose that $\langle\Omega\rangle$ is the standard mean value of a random variable Ω, that is, $\langle\Omega\rangle = \sum_{i=1}^{d-1} i\,P(\Omega = i)$ and $[\Omega]$ stands for Ω modulo d.

Fact 1. It holds that for any random variable Ω,

$$\text{(a)} \quad \langle[\Omega]\rangle + \langle[-\Omega-1]\rangle = d-1, \tag{A1}$$

$$\text{(b)} \quad \langle[\Omega]\rangle + \langle[-\Omega]\rangle = d[1-p([\Omega]=0)]. \tag{A2}$$

Proof. Both equations follow from the very definition of $\langle[\cdot]\rangle$. To prove (a) we notice that $[-\Omega-1]+[\Omega] = d-1$, and hence

$$\begin{aligned}
\langle[-\Omega-1]\rangle &= \sum_{i=1}^{d-1} i p([\Omega] = d-i-1) \\
&= \sum_{i=0}^{d-2} (d-i-1) p([\Omega] = i) \\
&= (d-1)\sum_{i=0}^{d-2} p([\Omega]=i) - \sum_{i=0}^{d-2} i\,P([\Omega]=i) \\
&= (d-1)\sum_{i=0}^{d-1} p([\Omega]=i) - \langle[\Omega]\rangle \\
&= (d-1) - \langle[\Omega]\rangle,
\end{aligned} \tag{A3}$$

where the second equality is a consequence of the changing of the summation index, the fourth one stems from the definition of $\langle[\Omega]\rangle$ and rearranging terms, and the last equality follows from normalization.

To prove (b), we write

$$\begin{aligned}
\langle[\Omega]\rangle + \langle[-\Omega]\rangle &= \sum_{i=1}^{d-1} i[p([\Omega]=i) + p([-\Omega]=i)] \\
&= \sum_{i=1}^{d-1} i[p([\Omega]=i) + p([\Omega]=d-i)]
\end{aligned}$$

$$= \sum_{i=1}^{d-1} i\,p([\Omega]=i) + \sum_{i=1}^{d-1}(d-i)\,p([\Omega]=i)$$
$$= d\sum_{i=1}^{d-1} p([\Omega]=i)$$
$$= d[1-p([\Omega]=0)], \tag{A4}$$

where the second equality is a consequence of the fact that $[\Omega]+[-\Omega]=d$, while the third equality follows from the shifting of the summation index in the second sum. ■

APPENDIX B: ALTERNATIVE PROOF OF THEOREM 4

Let us also notice that one can derive inequality (37) using a slightly different approach, which, for completeness, we present below.

Theorem 5. Let $\{p(\boldsymbol{a}|\boldsymbol{x},w)\}_{\boldsymbol{a},\boldsymbol{x}}$ be a nonsignaling probability distribution for any w and let the probabilities $p(\boldsymbol{x})$ be all equal. Then for any $k=1,\ldots,N$ and any choice of measurement settings $\boldsymbol{x}$,

$$D(\{p(a_k,w|\boldsymbol{x})\}_{a_k,w},\{\widetilde{p}(a_k)p(w|\boldsymbol{x})\}_{a_k,w})$$
$$= \frac{1}{2}\sum_{a_k,w}|p(a_k,w|\boldsymbol{x})-\widetilde{p}(a_k)p(w|\boldsymbol{x})|$$
$$\leqslant \frac{(d-1)^2+1}{2d}\,\widetilde{Q}_M(\boldsymbol{x})I_{\mathsf{A}}^{N,M,d}, \tag{B1}$$

where $I_{\mathsf{A}}^{N,M,d}$ is taken in the probability distribution observed by the parties $\{p(\boldsymbol{a}|\boldsymbol{x})\}$ and

$$\widetilde{Q}_M(\boldsymbol{x}) = \max_w\left[\frac{p(\boldsymbol{x}|w)}{\widetilde{p}_{\min}(w)}\right], \tag{B2}$$

where $\widetilde{p}_{\min}(w)=\min_{\boldsymbol{x}}\{p(\boldsymbol{x}|w)\}$ with the minimum taken over all measurement settings $\boldsymbol{x}$ appearing in the Bell inequality (10).

Proof. For simplicity but without any loss of generality, we prove this theorem for the bipartite case. The generalization to the multipartite case is straightforward.

As before, we denote the parties by A and B, while the adversary is denoted by E. Then, the corresponding inputs and outputs are denoted by x, y, z, and a, b, and e, respectively.

Let us start by noting that, by analogy to the case considered in the main text [see inequality (6) there], for any w, the probability distribution $\{p(a,b|x,y,w)\}_{a,b,x,y}$ satisfies the following monogamy relations:

$$\frac{I_w^{2,M,d}}{\widetilde{p}_{\min}(w)}+1 \geqslant d\,p(X_i=E_j|w) \quad (X=A,B) \tag{B3}$$

for any pair $\{i,j\}$ $(i,j=1,\ldots,M)$. In the above,

$$I_w^{2,M,d} = \sum_{\alpha=1}^{M}[p(\alpha,\alpha|w)\langle[A_\alpha-B_\alpha]\rangle_w + p(\alpha+1,\alpha|w)\langle[B_\alpha-A_{\alpha+1}]\rangle_w] \tag{B4}$$

is a modified BKP Bell expression, taking into account that the inputs x,y are generated with the biased probabilities $p(x,y|w)$, all correlators $\langle[A_\alpha-B_\alpha]\rangle_w$ and $\langle[B_\alpha-A_{\alpha+1}]\rangle_w$ are computed for the distribution $\{p(a,b|x,y,w)\}_{a,b,x,y}$, and now

$$\widetilde{p}_{\min}(w) = \min_{\alpha=1,\ldots,M}\{p(\alpha,\alpha|w),p(\alpha+1,\alpha|w)\}, \tag{B5}$$

where the convention $p(M+1,M|w)\equiv p(1,M|w)$ is used.

The monogamy relations (B3) imply (see the main text for the argument in favor of this fact) the bound on the probability of the adversary when using the strategy w to guess the outcomes of any of the measurements performed by one of the parties, say, for concreteness, Alice (but the same bound holds for outcomes of party B):

$$\max_a p(a|x,w) \leqslant \frac{1}{d}\left(1+\frac{I_w^{2,M,d}}{\widetilde{p}_{\min}(w)}\right) \quad (x=1,\ldots,M). \tag{B6}$$

Clearly, this bound holds also for any $p(a|x,w)$, which together with the normalization

$$p(a|x,w) = 1-\sum_{\alpha\neq a}p(\alpha|x,w), \tag{B7}$$

means that $p(a|x,w)\geqslant(1/d)-(d-1)[I_w^{2,M,d}/d\,\widetilde{p}_{\min}(w)]$, and therefore the inequality

$$\left|p(a|x,w)-\frac{1}{d}\right| \leqslant \frac{d-1}{d}\frac{I_w^{2,M,d}}{\widetilde{p}_{\min}(w)} \tag{B8}$$

holds for any a and x. Using then the inequality (B6) for $\max_a p(a|x,w)$ and (B8) for the rest of $p(a|x,w)$, we obtain that for any strategy w,

$$D(\{p(a|x,w)\}_a,\{\widetilde{p}(a)\}) = \frac{1}{2}\sum_a|p(a|x,w)-\widetilde{p}(a)| \leqslant \frac{(d-1)^2+1}{2d}\frac{I_w^{2,M,d}}{\widetilde{p}_{\min}(w)}. \tag{B9}$$

Now, since the parties do not have access to W, one needs further to average inequality (B9) over the probability distribution $\{p(w|x,y)\}_w$ for a particular choice of measurements x and y. This, together with the facts that $p(a|x,w)=p(a|x,y,w)$ (nosignaling) and $p(w|x,y)=p(x,y|w)p(w)/p(x,y)$, implying that $p(w|x,y)p(a|x,y,w)=p(a,w|x,y)$, allows one to write

$$D(\{p(a,w|x,y)\}_{a,w},\{\widetilde{p}(a)p(w|x,y)\}_{a,w})$$
$$= \frac{1}{2}\sum_{a,w}|p(a,w|x,y)-\widetilde{p}(a)p(w|x,y)|$$
$$\leqslant \frac{(d-1)^2+1}{2d}\sum_w\frac{p(x,y|w)}{\widetilde{p}_{\min}(w)}\frac{p(w)}{p(x,y)}I_w^{2,M,d}$$
$$\leqslant \frac{(d-1)^2+1}{2d}\,\widetilde{Q}_M(x,y)\sum_w\frac{p(w)}{p(x,y)}I_w^{2,M,d}, \tag{B10}$$

with $\widetilde{Q}_M(x,y)=\max_w[p(x,y|w)/\widetilde{p}_{\min}(w)]$. In order to obtain inequality (B1) from inequality (B10), it is enough to

notice that

$$p(a,b|x,y) = \sum_w p(w|x,y)p(a,b|x,y,w), \tag{B11}$$

which, with the aid of the assumption that all the probabilities $p(x,y)$ are equal, further translates to

$$I_{AB}^{2,M,d} = \sum_w \frac{p(w)}{p(x,y)} I_w^{2,M,d}, \tag{B12}$$

where $I_{AB}^{2,M,d}$ is computed for the observed probability distribution $\{p(a,b|x,y)\}$ and the probabilities $p(x,y) = \sum_w p(w)p(x,y|w)$ are assumed to be equal for all x,y. This completes the proof. ■

Let us finally notice that under the assumption, which we make above, that all $p(x,y)$ are equal, it holds that $Q_M(\boldsymbol{x}) = \widetilde{Q}_M(\boldsymbol{x})$.

[1] R. Horodecki, M. Horodecki, P. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[2] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[3] J. S. Bell, Physics **1**, 195 (1964).
[4] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).
[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); J. Barrett, L. Hardy, and A. Kent, *ibid.* **95**, 010503 (2005).
[6] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[7] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
[8] Ll. Masanes, A. Acín, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).
[9] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).
[10] J. Barrett, A. Kent, and S. Pironio, Phys. Rev. Lett. **97**, 170409 (2006).
[11] L. Aolita, R. Gallego, A. Cabello, and A. Acín, Phys. Rev. Lett. **108**, 100401 (2012).
[12] B. Toner and F. Verstraete, arXiv:quant-ph/0611001.
[13] B. Toner, Proc. R. Soc. London, Ser. A **465**, 59 (2009).
[14] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[15] M. Pawłowski and Č. Brukner, Phys. Rev. Lett. **102**, 030403 (2009).
[16] P. Kurzyński, T. Paterek, R. Ramanathan, W. Laskowski, and D. Kaszlikowski, Phys. Rev. Lett. **106**, 180402 (2011).
[17] T. R. de Oliveira, A. Saguia, and M. S. Sarandy, Europhys. Lett. **100**, 60004 (2012).
[18] S. Pironio *et al.*, Nature (London) **464**, 1021 (2010).
[19] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).
[20] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan, Phys. Rev. A **90**, 032322 (2014).
[21] R. Gallego, Ll. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acín, Nat. Commun. **4**, 2654 (2013).
[22] S. Pironio, Ll. Masanes, A. Leverrier, and A. Acín, Phys. Rev. X **3**, 031007 (2013).
[23] S. L. Braunstein and C. Caves, Ann. Phys. **202**, 22 (1990).
[24] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).
[25] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **200**, 340 (1995).
[26] Ll. Masanes, arXiv:quant-ph/0512100.
[27] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).
[28] M. Pawłowski, Phys. Rev. A **82**, 032313 (2010).
[29] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007).