Bell Inequalities Tailored to Maximally Entangled States

Alexia Salavrakos,[1] Remigiusz Augusiak,[2] Jordi Tura,[1,3] Peter Wittek,[1,4] Antonio Acín,[1,5] and Stefano Pironio[6]
[1]ICFO-Institut de Ciencies Fotoniques, Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain
[2]Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland
[3]Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, 85748 Garching, Germany
[4]University of Borås, Allegatan 1, 50190 Borås, Sweden
[5]ICREA—Institucio Catalana de Recerca i Estudis Avancats, E-08010 Barcelona, Spain
[6]Laboratoire d'Information Quantique, CP 224, Université libre de Bruxelles (ULB), 1050 Bruxelles, Belgium
(Received 20 September 2016; revised manuscript received 16 May 2017; published 26 July 2017)

Bell inequalities have traditionally been used to demonstrate that quantum theory is nonlocal, in the sense that there exist correlations generated from composite quantum states that cannot be explained by means of local hidden variables. With the advent of device-independent quantum information protocols, Bell inequalities have gained an additional role as certificates of relevant quantum properties. In this work, we consider the problem of designing Bell inequalities that are tailored to detect maximally entangled states. We introduce a class of Bell inequalities valid for an arbitrary number of measurements and results, derive analytically their tight classical, nonsignaling, and quantum bounds and prove that the latter is attained by maximally entangled states. Our inequalities can therefore find an application in device-independent protocols requiring maximally entangled states.

DOI: 10.1103/PhysRevLett.119.040402

Introduction.—Measurements on separated subsystems in a joint entangled state may display correlations that cannot be mimicked by local hidden variable (LHV) models. These correlations are termed nonlocal and are detected by violating Bell inequalities [1,2]. In recent years, it has become clear that nonlocality is interesting not only for fundamental reasons, but also as a resource for device-independent (DI) quantum information tasks [2] such as quantum key distribution [3,4] or random number generation [5,6]. Thus, violations of Bell inequalities are not only indicators of nonlocality, but can also be used to make qualitative and quantitative statements about operationally relevant quantum properties.

Traditionally, the problem of constructing Bell inequalities has been addressed from the point of view of deriving constraints satisfied by LHV models. Following this standard approach, the inequalities are derived using well-known techniques in convex geometry. Indeed, the set of correlations admitting LHV models defines a polytope [2], i.e., a bounded convex set with a finite number of vertices. These vertices correspond to local deterministic assignments, while the facets are the desired Bell inequalities. Facet (or tight) Bell inequalities provide necessary and sufficient criteria to detect the nonlocality of given correlations. Clauser-Horne-Shimony-Holt (CHSH) [7] and Collins-Gisin-Linden-Massar-Popescu (CGLMP) [8] Bell inequalities are examples thereof.

Although such facet Bell inequalities are optimal detectors of nonlocality, they are not necessarily optimal for inferring specific quantum properties in the DI setting. For instance, in a scenario where two binary measurements are performed on two entangled subsystems, it is well known that the violation of the CHSH inequality [7] is a necessary and sufficient condition for nonlocality. But certain "nonfacet" Bell inequalities are better certificates of randomness than the CHSH one when the two quantum systems are partially entangled [9].

The main aim of this work is to introduce Bell inequalities valid for an arbitrary number of measurements and outcomes whose maximal quantum violation, usually referred to as the *Tsirelson bound* [10], is attained by maximally entangled states

$$|\psi_d^+\rangle = (1/\sqrt{d}) \sum_{i=0}^{d-1} |ii\rangle. \tag{1}$$

This is a desirable property since these states have particular features such as perfect correlations between outcomes of local measurements in the same bases, and therefore many quantum information protocols rely on them. In the particular case of two measurements, CHSH is the simplest example of a Bell inequality with the above property, but others are known [11–13] (see also results for many settings [14–16]). Our construction works, however, for arbitrary numbers of measurements and outcomes, and, crucially, the Tsirelson bound of the resulting Bell inequalities can be computed *analytically.*

In the case where only two measurements are made on each subsystem, all facet Bell inequalities are known for a small number of outputs, and they are of the CGLMP form [8]. However, they are not maximally violated by the maximally entangled states of two qudits (except in the case $d = 2$ corresponding to the CHSH inequality) [17–19]. Thus, we should not expect our Bell inequalities to be tight, and indeed they are not.

This implies that we cannot use standard tools from convex geometry to construct them. In fact, no quantum

property is used for the construction of tight Bell inequalities like the CGLMP one and, in this sense, it is not surprising that their maximal violation does not require maximal entanglement. Our approach is completely different: it starts from quantum theory and exploits the symmetries and perfect correlations of maximally entangled states to derive a Bell inequality (cf. Ref. [16] for a similar method). It exploits sum of squares decompositions of Bell operators, which is used to determine their Tsirelson bound. Thus, contrary to any previous derivation of Bell inequalities, quantum theory becomes a key ingredient of our method.

Our results provide new insight into the structure of the boundary of the set of quantum correlations (see discussion in the Supplemental Material [20]). In addition, our Bell inequalities have the potential to be used in DI quantum information protocols such as random number generation, quantum key distribution, or to self-testing [21] (see more detailed discussion below).

Preliminaries.—We consider a Bell scenario with two distant parties A and B performing one of m measurements A_x and B_y with d outcomes on their share of some physical system. We label the measurements and outcomes as $x, y \in \{1, \ldots, m\}$ and $a, b \in \{0, \ldots, d-1\}$. The correlations obtained in this experiment are described by $(md)^2$ joint probabilities $P(A_x = a, B_y = b)$ that A and B obtain a and b upon performing the xth and yth measurement, respectively. These probabilities are ordered into a vector $\vec{p} := \{P(A_x = a, B_y = b)\}_{a,b,x,y} \in \mathbb{R}^{(md)^2}$.

Importantly, the set of allowed vectors $\vec{p}$ varies depending on the physical principle they obey. If the measurements define spacelike separated events, the observed correlations should obey the *no-signaling principle*, which prevents any faster-than-light communication among the parties. These correlations form a convex polytope denoted $\mathcal{N}$. Contained in this set is the set of quantum correlations $\mathcal{Q}$, which is formed by those $\vec{p}$ whose components can be written as $P(A_x = a, B_y = b) = \langle\psi| P_a^{(x)} \otimes P_b^{(y)} |\psi\rangle$, where $|\psi\rangle$ is some state in a product Hilbert space $H_A \otimes H_B$ of unconstrained dimension, and $\{P_a^{(x)}\}$ and $\{P_b^{(y)}\}$ are projection operators defining, respectively, Alice's and Bob's measurements. Finally, the set of correlations admitting LHV models, denoted $\mathcal{L}$, contains those $\vec{p}$ that can be written as a convex sum of product deterministic correlations $P(A_x = a, B_y = b) = P(A_x = a)P(B_y = b)$ with $P(A_x = a), P(B_y = b) = 0, 1$ for all x, y [22].

Bell was the first to prove that not all quantum correlations admit an LHV model [1]. To this end, he used the concept of a Bell inequality $I \leq C_b$, where I is the so-called Bell expression that is a linear combination of the $(md)^2$ joint probabilities of the form

$$I := \sum_{abxy} I_{abxy} P(A_x = a, B_y = b), \tag{2}$$

and $C_b = \max_{\vec{p}\in\mathcal{L}} I$ is its classical bound. The quantum or Tsirelson bound of I is the maximum value $Q_b = \max_{\vec{p}\in\mathcal{Q}} I$ that it can achieve for quantum correlations. A Bell expression I gives rise to a proper Bell inequality—one that is violated by quantum theory—if $C_b < Q_b$. If $\vec{p}$ violates a Bell inequality, the correlations described by $\vec{p}$ are termed nonlocal. Finally, one defines $NS_b = \max_{\vec{p}\in\mathcal{N}} I$ as the maximum value of I over no-signaling correlations. For most of the known Bell inequalities, $NS_b > Q_b > C_b$ [1,23,24].

Let us stress that although $\mathcal{Q}$ is convex, it is not a polytope. More importantly, the boundary of $\mathcal{Q}$ remains unknown despite several attempts to characterize it analytically [25–28] (see, nevertheless, [29]). This clearly makes the derivation of Tsirelson bounds a hard task. Given a Bell inequality, there is no procedure that guarantees finding its quantum bound, and it was achieved analytically only in a handful of cases. There is, however, a practical approximation scheme based on semidefinite programming, which consists in a hierarchy of sets $\mathcal{Q}_1 \supseteq \mathcal{Q}_2 \supseteq \ldots \supseteq \mathcal{Q}_k \supseteq \ldots$ converging to $\mathcal{Q}$ as $k \to \infty$, and allows one to bound Q_b from above [19] (see also [11]). Although for small Bell scenarios, this method yields good numerical bounds (often tight), it becomes computationally expensive for scenarios involving a large number of measurements or outcomes.

Class of Bell expressions.—Our aim now is to introduce a family of Bell expressions, whose maximal quantum value is attained by the *two-qudit* maximally entangled state $|\psi_d^+\rangle$. To derive them, we start from the premise that their maximal quantum values are obtained when Alice and Bob perform the optimal CGLMP measurements introduced in [8,30,31] (cf. [20]). This choice stems from the fact that these measurements generalize the CHSH measurements ($d = 2$) to arbitrary dimensions, and they lead to nonlocal correlations that are most robust to noise [30] or for $m = 2$, give a stronger statistical test [32].

The probabilities $P(A_x = a, B_y = b)$ obtained when using the optimal CGLMP measurements on $|\psi_d^+\rangle$ have several symmetries. For instance, they only depend on the difference $a - b = k \bmod d$. If we impose that our Bell expressions respect this symmetry, the probabilities $P(A_x = j + k \bmod d, B_y = j)$ should be treated equally for all j; i.e., the Bell expressions should be linear combinations of $P(A_x = B_y + k) := \sum_{j=0}^{d-1} P(A_x = j + k \bmod d, B_y = j)$. Taking into account all symmetries, a generic form for our Bell expressions is

$$I_{d,m} := \sum_{k=0}^{\lfloor d/2 \rfloor - 1} (\alpha_k \mathbb{P}_k - \beta_k \mathbb{Q}_k), \tag{3}$$

where $\mathbb{P}_k := \sum_{i=1}^{m} [P(A_i = B_i + k) + P(B_i = A_{i+1} + k)]$, $\mathbb{Q}_k := \sum_{i=1}^{m} [P(A_i = B_i - k - 1) + P(B_i = A_{i+1} - k - 1)]$ with $A_{m+1} := A_1 + 1$. The parameters α_k and β_k are our

degrees of freedom. Taking, e.g., $\alpha_k = \beta_k = 1-2k/(d-1)$ for $m = 2$, one recovers the CGLMP Bell inequalities.

To exploit the symmetries inherent in Bell inequalities, we often write them in terms of correlators instead of probabilities. As we consider an arbitrary number of outcomes, we appeal to the notion of generalized correlators (see, e.g., Refs. [15,33] for other options). These are complex numbers that are defined through the two-dimensional Fourier transform of the probabilities $P(A_x = a, B_y = b)$,

$$\langle A_x^k B_y^l \rangle = \sum_{a,b=0}^{d-1} \omega^{ak+bl} P(A_x = a, B_y = b), \tag{4}$$

where $\omega = \exp(2\pi i/d)$, $k,\ l \in \{0, \ldots, d-1\}$, and $\{A_x^k\}_k$ and $\{B_y^l\}_l$ can be thought of as measurements with outcomes labeled by roots of unity ω^i $(i = 0, \ldots, d-1)$. For quantum correlations $\vec{p}$, the correlators $\langle A_x^k B_y^l \rangle$ are average values of the tensor product of the operators $A_x^k = \sum_{a=0}^{d-1} \omega^{ak} P_a^{(x)}$ and $B_y^l = \sum_{b=0}^{d-1} \omega^{bl} P_b^{(y)}$ in the state $|\psi\rangle$. Note that they are unitary, their eigenvalues are the roots of unity, and they satisfy $(A_x^k)^\dagger = A_x^{d-k}$ and $(B_y^l)^\dagger = B_y^{d-l}$ for any k, l.

Now, exploiting (4), expression (3) can be rewritten as

$$\tilde{I}_{d,m} = \sum_{i=1}^{m} \sum_{l=1}^{d-1} \langle A_i^l \bar{B}_i^l \rangle, \tag{5}$$

where, for clarity, the change of variables $\bar{B}_i^l = a_l B_i^{d-l} + a_l^* B_{i-1}^{d-l}$ with $a_l = \sum_{k=0}^{\lfloor d/2 \rfloor - 1} (\alpha_k \omega^{-kl} - \beta_k \omega^{(k+1)l})$ was introduced on Bob's side. Because of the convention $A_{m+1} = A_1 + 1$, the term $\bar{B}_1^l$ is defined as $\bar{B}_1^l = a_l B_1^{d-l} + a_l^* \omega^l B_m^{d-l}$. For simplicity, in (5), we ignored the irrelevant scalar term corresponding to $l = 0$ and rescaled the expression. Below we denote the classical, quantum and no-signaling bound of $\tilde{I}_{d,m}$ by $\tilde{C}_b$, $\tilde{Q}_b$, and $\widetilde{NS}_b$, respectively.

Our aim now is to fix the free parameters α_k and β_k according to the quantum property we need: maximal violation by the maximally entangled state $|\psi_d^+\rangle$. At this point, it is instructive to look at the specific example of the CHSH Bell expression ($m = 2$, $d = 2$). In the notation (5), the CHSH Bell expression $\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle$ reads $\tilde{I}_{2,2} = \langle A_1 \bar{B}_1 \rangle + \langle A_2 \bar{B}_2 \rangle$, where $\bar{B}_1 = (B_1 + B_2)/\sqrt{2}$, $\bar{B}_2 = (B_1 - B_2)/\sqrt{2}$. Then, for the optimal measurements leading to the Tsirelson bound of $\tilde{I}_{2,2}$, we have $\bar{B}_1 = A_1^*$ and $\bar{B}_2 = A_2^*$. This reflects the property that for the maximally entangled state

$$M \otimes N |\psi_d^+\rangle = \mathbb{1} \otimes N M^T |\psi_d^+\rangle, \quad \forall\ M, N. \tag{6}$$

This condition implies that a measurement by Alice is perfectly correlated with its complex conjugate by Bob. Our intuition to derive Bell inequalities detecting maximal entanglement is to impose this property for any m and d: we choose the parameters α_k and β_k such that

$$\bar{B}_i^l = (A_i^l)^* \tag{7}$$

hold for $l = 1, \ldots, d-1$ and $i = 1, \ldots, m$ with the initial operators $\{P_a^{(x)}\}$ and $\{P_b^{(y)}\}$ being the optimal CGLMP operators. Conditions (7) give rise to a set of linear equations for α_k and β_k which yields (see [20] for details)

$$\alpha_k = \frac{1}{2d} \tan\left(\frac{\pi}{2m}\right) \left[g(k) - g\left(\left\lfloor \frac{d}{2} \right\rfloor\right) \right], \tag{8}$$

$$\beta_k = \frac{1}{2d} \tan\left(\frac{\pi}{2m}\right) \left[g\left(k + 1 - \frac{1}{m}\right) + g\left(\left\lfloor \frac{d}{2} \right\rfloor\right) \right] \tag{9}$$

with $g(x) := \cot(\pi(x + 1/2m)/d)$.

To sum up, our class of Bell expressions is given by $I_{d,m}$ (3) or equivalently by $\tilde{I}_{d,m}$ (5), with coefficients (8) and (9). We arrived at it by writing the most general Bell expression satisfying the symmetry of CGLMP correlations, rewriting these Bell expressions in the simple form (5) through a change of variable on Bob's side, and then imposing the conditions (7) that take into account the symmetries of the maximally entangled state, as CHSH does for two binary measurements.

Properties of the novel Bell expressions.—We now analyze the main properties of our Bell expressions: we compute all the relevant bounds $\tilde{C}_b$, $\tilde{Q}_b$, $\widetilde{NS}_b$, and show that $\tilde{C}_b < \tilde{Q}_b < \widetilde{NS}_b$ for any d and m. For clarity, we only include sketches of proofs (see [20] for details).

Let us begin with the classical bound.

Theorem 1. The classical bound of $\tilde{I}_{d,m}$ is given by $\tilde{C}_b = (1/2)\tan(\pi/2m)\{(2m-1)g(0) - g(1-1/m)\} - m$.

Proof.—We start with the expression $I_{d,m}$. Since we can restrict the problem to local deterministic strategies, finding $\tilde{C}_b$ becomes a question of distributing 0s and 1s over all the terms $P(A_x = B_y + z)$. It turns out that the optimal strategy is to set $2m-1$ of the terms multiplied by α_0, and a single term multiplied by β_0 to one, and the remaining terms to zero.□

Importantly, the resulting Bell inequality $\tilde{I}_{d,m} \leq \tilde{C}_b$ is violated by quantum theory; one can reach the value $\tilde{I}_{d,m} = m(d-1)$ by applying the CGLMP measurements on $|\psi_d^+\rangle$. This is seen by using Eq. (7), the unitarity of A_i^k, and the symmetries of the maximally entangled states (6). Then, all the correlators in (5) equal one, yielding the quantum violation of $m(d-1)$. This violation is optimal and defines the tight Tsirelson bound of $\tilde{I}_{d,m}$.

Theorem 2. The Tsirelson bound of $\tilde{I}_{d,m}$ is given by $\tilde{Q}_b = m(d-1)$.

Proof.—We construct a sum-of-squares (SOS) decomposition of the shifted Bell operator $\tilde{\mathcal{B}} := \tilde{Q}_b \mathbb{1} - \mathcal{B}$, where $\mathbb{1}$ is the identity operator and $\mathcal{B}$ the Bell operator corresponding to expression (5) (see, e.g., [34,35]). For any positive semidefinite operator $\mathcal{P}$, an SOS decomposition is a collection of operators P_λ such that $\mathcal{P} = \sum_\lambda P_\lambda^\dagger P_\lambda$. If $\tilde{\mathcal{B}}$ admits the latter form, it must be positive semidefinite, implying that $\tilde{Q}_b$ upper bounds our Bell expression, i.e., $\langle \psi | \mathcal{B} | \psi \rangle \leq \tilde{Q}_b$ for any $|\psi\rangle$.

To show that $\tilde{Q}_b = m(d-1)$ is indeed the Tsirelson bound of $\tilde{I}_{d,m}$, we prove that $\tilde{Q}_b\mathbb{1} - \mathcal{B}$ decomposes as

$$\tilde{Q}_b\mathbb{1} - \mathcal{B} = \frac{1}{2}\sum_{i=1}^{m}\sum_{k=1}^{d-1} P_{ik}^{\dagger}P_{ik} + \frac{1}{2}\sum_{i=1}^{m-2}\sum_{k=1}^{d-1} T_{ik}^{\dagger}T_{ik}, \quad (10)$$

where $P_{ik} = \mathbb{1}\otimes\bar{B}_i^k - (A_i^k)^{\dagger}\otimes\mathbb{1}$, and $T_{ik} = (\mu_{i,k}B_2^{d-k} + \nu_{i,k}B_{i+2}^{d-k} + \tau_{i,k}B_{i+3}^{d-k})$ with $\mu_{i,k}$, $\nu_{i,k}$, $\tau_{i,k}\in\mathbb{R}$. The Bell operator reads $\mathcal{B} = \sum_{i=1}^{m}\sum_{l=1}^{d-1} A_i^k\otimes\bar{B}_i^k$, and the decomposition is independent of the choice of A_i^k and B_i^k. The exact values of the coefficients along with details on the SOS decomposition can be found in [20]. Notice that (10) generalizes the SOS derived for the chained Bell inequalities in [36] to any number of outcomes. □

A few remarks are in order. First, it is not difficult to see that $\tilde{Q}_b > \tilde{C}_b$ for any m, $d \geq 2$, meaning that all our Bell inequalities are nontrivial (cf. [20]). Second, let us elaborate on how the SOS works in the case of two measurements, $m = 2$, which justifies the choice of conditions (7). For $m = 2$, the second part of the SOS decomposition (10) vanishes. For the optimal CGLMP measurements, both sides of (10) must yield zero when applied to $|\psi_d^+\rangle$, which stems from conditions (6) and (7). This allows one to grasp the intuition behind conditions (7); i.e., they allow one to construct in a quite direct way an SOS decomposition (10), in which all operators P_{ik} are polynomials of the measurement operators A_i^k and B_i^k of order one, significantly facilitating the computation of the Tsirelson bound. For the CHSH Bell inequality, one observes the same effect, as these same properties of the optimal state and measurements allow the Bell operator $\mathcal{B}_{\mathrm{CHSH}} = A_1\otimes B_1 + A_1\otimes B_2 + A_2\otimes B_1 - A_2\otimes B_2$ to have the decomposition: $2\sqrt{2}\mathbb{1} - \mathcal{B}_{\mathrm{CHSH}} = (P_1^{\dagger}P_1 + P_2^{\dagger}P_2)/\sqrt{2}$, with $P_1 = (1/\sqrt{2})\mathbb{1}\otimes(B_1 + B_2) - A_1\otimes\mathbb{1}$, and $P_2 = (1/\sqrt{2})\mathbb{1}\otimes(B_1 - B_2) - A_2\otimes\mathbb{1}$. Thus, our construction generalizes this quantum aspect of the CHSH Bell operator. For a larger number of measurements, $m > 2$, the first part of the SOS decomposition is not enough, and one has to add "by hand" the extra term in which all T_{ik}'s are also of order one in B_i^k.

Note that for two measurements, our Bell expressions coincide with those introduced in [12] and then rederived in [11] using a different approach. Moreover, the Tsirelson bounds of these Bell inequalities was computed in Refs. [11,13] exploiting other techniques, and it was proven in [13] that they are not tight. On the other hand, for $d = 2$ and any m, our class recovers the well-known chained Bell inequalities [37]. We finally notice that the alternative generalization of the CHSH Bell inequality to three measurements and outcomes given in [38] was also found to be maximally violated by $|\psi_3^+\rangle$ [15].

Let us eventually compute the no-signaling bound of our Bell expressions.

Theorem 3. The no-signaling bound of $\tilde{I}_{d,m}$ is given by $\widetilde{NS}_b = m\tan(\pi/2m)g(0) - m$.

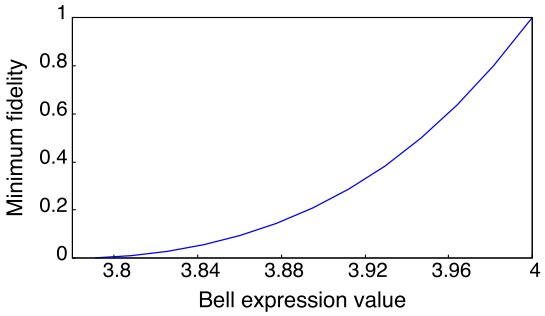

FIG. 1. Minimum fidelity of the state in the black box to the maximally entangled state of two qutrits, as a function of the violation of $\tilde{I}_{3,2}$. At the maximal violation 4, the fidelity is equal to 1, meaning that the quantum state used in the Bell experiment must be maximally entangled. The numerical method that we used does not yield a positive lower bound on the fidelity below $\tilde{I}_{3,2} \approx 3.79$ (for comparison, the classical bound is $\tilde{I}_{3,2} \leq (1+3\sqrt{3})/2 \approx 3.01$).

Proof.—We provide no-signaling correlations $\vec{p}$ and show that they attain the algebraic bound of $I_{d,m}$. They correspond to having all the probabilities which are multiplied by α_0 in $I_{d,m}$ equal to one, and all the others equal to zero (see [20]). □

Again, it is not difficult to see that $\widetilde{NS}_b > \tilde{Q}_b$ for any m, $d \geq 2$ (see [20] for the proof and scalings of $\tilde{C}_b$, $\tilde{Q}_b$, and $\widetilde{NS}_b$ with m and d).

Applications to device-independent protocols.—A natural application for our Bell inequalities is self-testing—a DI protocol in which a state and measurements performed on it are certified up to local isometries, based on the nonlocal correlations they produce. To perform self-testing, the correlations $\vec{p}$ maximally violating the given Bell inequality must be unique, i.e., attained, up to local isometries, by certain state and measurements. This is generally hard to prove. There exists, however, a numerical method for self-testing [39]. We applied it to the simplest case $m = 2$ and $d = 3$, and the results are plotted in Fig. 1. It shows that one can self-test the maximally entangled state of two qutrits $|\psi_3^+\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$ with our inequalities.

An open question is whether one can generalize this result to any dimension. Our inequalities could then be applied in DI random number generation protocols [5,6,40]. Indeed, if $\vec{p}$ maximally violating $\tilde{I}_{d,m}$ is unique, one can apply the method of [41] and use the symmetries of the Bell expressions to guarantee a dit of perfect randomness. This, by increasing the dimension d, would result in unbounded randomness expansion.

Our inequalities could also find applications in DI quantum key distribution. An advantage that our inequalities have over CGLMP in that scenario [42] is that, as said before, the maximal violation is obtained for the maximally entangled state. This state can produce perfect correlations between the users, which reduces the error-correcting phase of the protocol and can lead to better key generation rates. We study this question in the Supplemental Material [20]. Numerically, we find that for $m = 2$ and $d = 3$, our

inequalities lead to higher key rates than CGLMP for levels of white noise up to 4.2%. While this advantage is not very large, we believe it grows with the dimension of the systems, at least in the noiseless case [18]. Moreover, it is known that maximally entangled states are much simpler to prepare experimentally than fine-tuned partially entangled states. It would be interesting to confirm these conjectures in a future work focused on DIQKD.

Conclusions.—In this work, we introduced a new technique allowing one to construct Bell inequalities with arbitrary numbers of measurements and outcomes that are maximally violated by the maximally entangled states. It exploits the SOS decompositions of Bell operators and, crucially, allows one to compute analytically their Tsirelson bounds. Our results are general as, unlike previous works, we do not consider a particular Bell scenario, but allow for arbitrary number of measurements m and outcomes d. Our inequalities can be seen as the "quantum" or the DI-oriented generalization of CHSH Bell inequality, in the same spirit as the CGLMP inequality generalizes the CHSH one classically.

We wish to thank Y.-C. Liang, M. Navascués, T. Vértesi, and J. Kaniewski for fruitful discussions, and especially, J.-D. Bancal for sharing with us his code. This work was supported ERC CoG QITBOX and AdG OSYRIS, the AXA Chair in Quantum Information Science, Spanish MINECO (Grants No. FOQUS FIS2013-46768-P, No. SEV-2015-0522, No. QIBEQI FIS2016-80773-P, and No. FISICATEAMO FIS2016-79508-P), Fundació Privada Cellex, the Generalitat de Catalunya (Grants No. SGR 874, No. SGR 875 and the CERCA programme), the EU projects QALGO and SIQS, and the John Templeton Foundation. This project has received funding from the European Unions Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grants No. 705109 and No. 748549. We acknowledge financial support from the Fondation Wiener-Anspach and the Interuniversity Attraction Poles program of the Belgian Science Policy Office under the grant IAP P7-35 photonics@be. J. T. acknowledges the CELLEX-ICFO-MPQ programme. S. P. is a Research Associate of the Fonds de la Recherche Scientifique F.R.S.-FNRS (Belgium).

[1] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[2] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[3] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, in *Proceedings of 39th Annual Symposium (FOCS)* (1998), 503.
[4] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[5] R. Colbeck, Ph.D. thesis, University of Cambridge, 2006; R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011).
[6] S. Pironio *et al.*, Nature (London) **464**, 1021 (2010).
[7] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[8] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).
[9] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).
[10] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).
[11] J. I. de Vicente, Phys. Rev. A **92**, 032103 (2015).
[12] W. Son, J. Lee, and M. S. Kim, Phys. Rev. Lett. **96**, 060406 (2006).
[13] S.-W. Lee, Y. W. Cheong, and J. Lee, Phys. Rev. A **76**, 032108 (2007).
[14] S.-W. Ji, J. Lee, J. Lim, K. Nagata, and H.-W. Lee, Phys. Rev. A **78**, 052103 (2008).
[15] Y.-C. Liang, C.-W. Lim, and D.-L. Deng, Phys. Rev. A **80**, 052116 (2009).
[16] J. Lim, J. Ryu, S. Yoo, C. Lee, J. Bang, and J. Lee, New J. Phys. **12**, 103012 (2010).
[17] A. Acín, T. Durt, N. Gisin, and J. I. Latorre, Phys. Rev. A **65**, 052325 (2002).
[18] S. Zohren and R. D. Gill, Phys. Rev. Lett. **100**, 120406 (2008).
[19] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007); New J. Phys. **10**, 073013 (2008).
[20] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.119.040402 for details on the derivation of our Bell inequalities, proofs of the classical, quantum and no-signaling bounds, a study of the scaling of these bounds, and discussions on the use of our Bell inequalities for DIQKD and on the structure of the quantum set.
[21] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A **45**, 455304 (2012).
[22] A. Fine, Phys. Rev. Lett. **48**, 291 (1982).
[23] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[24] R. Ramanathan, J. Tuziemski, M. Horodecki, and P. Horodecki, Phys. Rev. Lett. **117**, 050401 (2016).
[25] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature (London) **461**, 1101 (2009).
[26] M. Navascués and H. Wunderlich, Proc. R. Soc. A **466**, 881 (2010).
[27] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín, Nat. Commun. **4**, 2263 (2013).
[28] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín, Nat. Commun. **6**, 6288 (2015).
[29] Ll. Masanes, Necessary and Sufficient Condition for Quantum-Generated Correlations, arXiv:quant-ph/0309137.
[30] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).
[31] J. Barrett, A. Kent, and S. Pironio, Phys. Rev. Lett. **97**, 170409 (2006).
[32] A. Acín, R. Gill, and N. Gisin, Phys. Rev. Lett. **95**, 210402 (2005).
[33] J.-D. Bancal, C. Branciard, N. Brunner, N. Gisin, and Y.-C. Liang, J. Phys. A **45**, 125301 (2012).
[34] C. Bamps and S. Pironio, Phys. Rev. A **91**, 052111 (2015).
[35] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner, The quantum moment problem and bounds on entangled multi-prover games, in *Proceedings of IEEE Conference on Computational Complexity* (2008), 199.
[36] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, New J. Phys. **18**, 035013 (2016).

[37] P. A. Pearle, Phys. Rev. D **2**, 1418 (1970); S. L. Braunstein and C. Caves, Ann. Phys. (N.Y.) **202**, 22 (1990).
[38] H. Buhrman and S. Massar, Phys. Rev. A **72**, 052103 (2005).
[39] T. H. Yang, and T. Vértesi, J-D. Bancal, V. Scarani, and M. Navascués, Phys. Rev. Lett. **113**, 040401 (2014).
[40] S. Pironio and S. Massar, Phys. Rev. A **87**, 012336 (2013).
[41] C. Dhara, G. Prettico, and A. Acín, Phys. Rev. A **88**, 052116 (2013).
[42] M. Huber and M. Pawłowski, Phys. Rev. A **88**, 032309 (2013).