Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems

Jędrzej Kaniewski[1,2], Ivan Šupić[3], Jordi Tura[4], Flavio Baccari[3], Alexia Salavrakos[3], and Remigiusz Augusiak[1]

[1]Center for Theoretical Physics, Polish Academy of Sciences, Al. Lotników 32/46, 02-668 Warsaw, Poland
[2]QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark
[3]ICFO-Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
[4]Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, 85748 Garching, Germany

Bell inequalities are an important tool in device-independent quantum information processing because their violation can serve as a certificate of relevant quantum properties. Probably the best known example of a Bell inequality is due to Clauser, Horne, Shimony and Holt (CHSH), which is defined in the simplest scenario involving two dichotomic measurements and whose all key properties are well understood. There have been many attempts to generalise the CHSH Bell inequality to higher-dimensional quantum systems, however, for most of them the maximal quantum violation—the key quantity for most device-independent applications—remains unknown. On the other hand, the constructions for which the maximal quantum violation can be computed, do not preserve the natural property of the CHSH inequality, namely, that the maximal quantum violation is achieved by the maximally entangled state and measurements corresponding to mutually unbiased bases. In this work we propose a novel family of Bell inequalities which exhibit precisely these properties, and whose maximal quantum violation can be computed analytically. In the simplest scenario it recovers the CHSH Bell inequality. These inequalities involve d measurements settings, each having d outcomes for an arbitrary prime number $d \geq 3$. We then show that in the three-outcome case our Bell inequality can be used to self-test the maximally entangled state of two-qutrits and three mutually unbiased bases at each site. Yet, we demonstrate that in the case of more outcomes, their maximal violation does not allow for self-testing in the standard sense, which motivates the definition of a new weak form of self-testing. The ability to certify high-dimensional MUBs makes these inequalities attractive from the device-independent cryptography point of view.

1 Introduction

Nonlocality of quantum mechanics, in the sense first described by Einstein, Podolsky and Rosen [EPR35] and later formalised by Bell [Bel64], is arguably one of its most counterintuitive features. While the original motivation for studying Bell inequalities was to rule out a classical (local-realistic) description of the system under study, we now understand that Bell nonlocality can also be used in a constructive manner. If we assume that our system is governed by quantum mechanics, we can use Bell violations to certify specific quantum properties. One can, for instance, certify the dimension [BPA+08], the amount of entanglement present in the state [MBL+13], or the degree of incompatibility of the measurements [CS16, CBLC16]. Bell violations are also used to certify randomness produced in the experiment, which is often applied to *device-independent cryptography*, e.g. randomness generation/expansion [Col06, PAM+10, CK11, VV12, MS16, BPPP14], quantum key distribution [BHK05, AGM06, ABG+07, RUV13, VV14, MS16, AFDF+18] or multi-party cryptography [SCA+11, KW16, RTK+18, RMW16, RMW18]. In some cases the observed nonlocal correlations give us a full description of the system under study (up to well-understood equivalences). This constitutes the most complete variant of device-independent certification and goes under the name of *self-testing* [MY98, MY04]. Most self-testing schemes allow us to certify states which are locally qubits [BLM+09, McK14, MYS12, YN13, BP15, WWS16, ŠASA16]. These results were combined to give certification schemes for higher-dimensional systems [YN13, CGS17, ŠCAA18]. However, they are still based on the violation of many two-outcome Bell inequalities; in particular, the observables they use are constructed out of single-qubit measurements. It remains a highly nontrivial and interesting problem to propose certification schemes for quantum states of higher local dimension based on a single d-outcome Bell inequality and exploiting genuine d-outcome measurements such as higher-dimensional mutually unbiased bases. The main aim of our work is to fill this gap.

The certification aspect adds a new layer of complexity to nonlocality. Given a Bell inequality it is no longer sufficient to find the local and quantum values, but one should go one step further to investigate whether the observed violation can be used for certification of quantum resources. Numerous Bell inequalities have been proposed in the last 25 years (see Ref. [BCP+14] for a comprehensive review), but their certification properties are in most cases poorly understood.

The simplest and most-studied Bell inequality is due to Clauser, Horne, Shimony and Holt (CHSH) [CHSH69]. In the CHSH scenario there are two devices which have two settings and two outcomes each. It is well known that this inequality can be maximally violated by performing maximally incompatible qubit measurements on the maximally entangled state of two qubits. In fact, this is essentially the only manner of achieving the maximal violation [Tsi87, SW87, PR92, Tsi93]. Several generalisations of the CHSH inequality to Bell scenarios involving d-outcome measurements have been proposed. However, for most of them the maximal quantum value is not known [CGL+02, BM05, BKP06, SLK06]. For those for which the maximal quantum value can be computed, the maximal quantum violation is achieved by the maximally entangled state, but the optimal measurements do not correspond to mutually unbiased bases [dV15, SAT+17, Col18].

In this work we introduce a generalisation of the CHSH Bell inequality which fills this gap. To this aim we consider the Bell functional due to Buhrman and Massar (BM) [BM05] in which the settings and outcomes instead of being bits come from the set $\{0, 1, \ldots, d-1\}$ for some integer d and the winning condition is interpreted modulo d. While this functional seems to be quite a natural generalisation of the CHSH one, it turns out to be surprisingly hard to analyse. In particular, the quantum value is only known for $d = 3$ (and the proof is numerical). Here we define a modification of the BM inequality for d being an odd prime and show that it has several desirable features. Most importantly, we can compute the quantum value by first exhibiting a sum-of-squares (SOS) decomposition of the Bell operator and then giving an explicit quantum realisation which saturates this bound. This quantum realisation uses the maximally entangled state of local dimension d and rank-1 projective measurements which are pairwise mutually unbiased. On the other hand, finding the classical value of our Bell expressions turns out to be a difficult problem and we compute it only for $d = 3, 5, 7$. Nevertheless, we conjecture that the classical and quantum values differ for any prime d.

Importantly, the SOS decomposition allows us to derive explicit algebraic relations that the optimal observables must satisfy. For $d = 3$ we are able to completely solve these relations, i.e. for this inequality we obtain a complete self-testing statement. To the best of our knowledge this is the first analytical self-testing statement, which does not rely on self-testing results for two-dimensional systems (except for Ref. [CS17] which relates the self-testing problem to representations of a certain group). Note that a partial self-testing statement for the maximally entangled state of two qutrits has recently been proven numerically for a different Bell inequality [SAT+17]. For $d = 5$ and $d = 7$, on the other hand, the situation becomes more complicated: we show that the maximal violation can be achieved by quantum realisations which are not equivalent according to the standard definition of self-testing.

The paper is organised as follows. In Section 2 we establish notation, whereas in Section 3 we explicitly state the modified BM inequality and compute its quantum value. In Section 4 we provide a partial characterisation of the quantum realisations saturating the quantum bound and derive a self-testing statement for $d = 3$. We summarise our findings and discuss some resulting open questions in Section 5.

2 Preliminaries

This section sets up the scenario and introduces the relevant notation and terminology from the area of Bell nonlocality.

2.1 Measurements and observables

Throughout this work we assume all the systems to be finite-dimensional. A measurement with d outcomes is a collection of positive semidefinite operators $\{F_a\}_{a=0}^{d-1}$ satisfying $\sum_{a=0}^{d-1} F_a = \mathbb{1}$. Given a measurement and an integer $n \in \mathbb{Z}$ we define

$$A^{(n)} := \sum_{a=0}^{d-1} \omega^{an} F_a,$$

where $\omega := \exp(2\pi \mathrm{i}/d)$. Clearly, the operator corresponding to $n = 0$ is fixed by the normalisation condition: $A^{(0)} = \mathbb{1}$. Since this is a discrete Fourier transform, the inverse transformation is given by

$$F_a = \frac{1}{d} \sum_{n=0}^{d-1} \omega^{-an} A^{(n)}.$$

Therefore, we may think of the operators $A^{(1)}, \ldots, A^{(d-1)}$ as an alternative description of the measurement. This representation turns out to be convenient for our purposes.

Since all computations in this work are performed at the level of operators $A^{(n)}$, let us state some of their properties (see Appendix A for proofs). For arbitrary n we have

$$\left[A^{(n)}\right]^\dagger = A^{(-n)} \quad \text{and} \quad \left[A^{(n)}\right]^\dagger A^{(n)} \leq \mathbb{1}.$$

Moreover, it is clear that $A^{(n)} = A^{(n+d)} = A^{(n-d)}$, i.e. there are at most $d-1$ distinct operators (because $A^{(0)} = \mathbb{1}$). This description becomes particularly simple when the original measurement is projective, i.e. the measurement operators satisfy $F_a F_b = \delta_{ab} F_a$ with δ_{ab} being the Kronecker delta. Then, the entire measurement can be encoded into a single operator: it is easy to verify that $A^{(n)} = A^n$ for $A := A^{(1)}$. In such a case we will refer to the unitary operator A as the *observable* and one can check that its spectrum is contained in $\{1, \omega, \omega^2, \ldots, \omega^{d-1}\}$. To ensure that an unknown measurement is projective, it suffices to check that the operator $A^{(1)}$ is unitary, i.e. $\left[A^{(1)}\right]^\dagger A^{(1)} = \mathbb{1}$.

2.2 Bell scenario and Bell inequalities

In this work we consider a bipartite Bell scenario in which two parties, traditionally named Alice and Bob, share some bipartite physical system, and each of them performs a number of measurements on their share of this system. We assume that both parties perform d measurements and each measurement has exactly d outcomes. The measurement choices of Alice and Bob are labelled by j and k, whereas the outcomes by a and b, respectively, and we use the convention that $a, b, j, k \in \{0, 1, \ldots, d-1\}$. Denoting the probability of observing outcomes a and b given settings j and k by $P(ab|jk)$, the above experiment, termed also Bell experiment, is described by a set of probability distributions $\{P(ab|jk)\}$.

It is natural to assume that any correlations observed in such a Bell experiment satisfy the no-signalling principle, meaning that the outcomes of one of the parties cannot depend on the measurement choice made by the other party. Mathematically, this is expressed as a set linear constraints of the form

$$\sum_a P(ab|jk) = \sum_a P(ab|j'k) \tag{1}$$

for all b, k and $j \neq j'$, and

$$\sum_b P(ab|jk) = \sum_a P(ab|jk') \tag{2}$$

for all a, j and $k \neq k'$. By the very definition, correlations obeying the no-signalling principle form a convex polytope that for further purposes we denote $\mathcal{N}_d$.

Imagine now that Alice and Bob share a quantum system represented by a bipartite density matrix ρ_{AB} and perform quantum measurements on it. Then, the conditional probabilities are given by the following well-known formula

$$P(ab|jk) = \mathrm{tr}\left[(F_a^j \otimes G_b^k)\rho_{AB}\right], \tag{3}$$

where $\{F_a^j\}, \{G_b^k\}$ represent the measurements of Alice and Bob, respectively. Let us notice that all such quantum correlations, that is, correlations obtained from quantum states (if we do not constrain their local dimension) form a convex set, denoted $\mathcal{Q}_d$, whose structure is in general unknown and difficult to characterise [Slo17].

The last set of correlations we need to introduce here is that of correlations admiting the local-realistic description, that is, those for which $P(ab|jk)$ can be represented as

$$P(ab|jk) = \sum_\lambda P(\lambda) D_A(a|x,\lambda) D_B(b|y,\lambda), \tag{4}$$

where λ are the hidden variables, while $D_A(a|x,\lambda)$ (and similarly $D_B(b|y,\lambda)$) is a deterministic function that for a given x and λ returns a fixed outcome with probability one. Correlations admitting such description are usually referred to as local or classical, and, similarly to the no-signalling correlations, they form a convex set that is a polytope, denoted $\mathcal{P}_d$.

For a given scenario it holds that $\mathcal{P}_d \subsetneq \mathcal{Q}_d \subsetneq \mathcal{N}_d$. In particular, a natural way to show that $\mathcal{P}_d \subsetneq \mathcal{Q}_d$ is to use Bell inequalities. To define them explicitly let us consider a Bell functional

$$\beta := \sum_{abjk} c_{abjk} P(ab|jk), \tag{5}$$

where c_{abjk} are some real coefficients. Computing then the maximal value of β over the local set $\mathcal{P}_d$, that is, $\beta_C := \max_{\mathcal{P}_d} \beta$, one arrives at a Bell inequality

$$\sum_{abjk} c_{abjk} P(ab|jk) \leq \beta_C \tag{6}$$

whose violation indicates nonlocality. Let us also denote by β_Q and β_{NS} the maximal values of β over the quantum and no-signalling sets, that is,

$$\beta_Q := \sup_{\mathcal{Q}_d} \beta, \qquad \beta_{NS} := \max_{\mathcal{N}_d} \beta. \tag{7}$$

2.3 Bell operators and sum of squares decompositions

Let us now consider a Bell experiment performed on a quantum state ρ_{AB} with measurements $\{F_a^j\}$ and $\{G_b^k\}$. Due to Born's formula (3) the value of a Bell functional β corresponding to a Bell inequality (5) can be computed as $\beta = \mathrm{tr}(W\rho_{AB})$, where

$$W := \sum_{abjk} c_{abjk} F_a^j \otimes G_b^k \tag{8}$$

is the Bell operator constructed from the measurements $\{F_a^j\}$ and $\{G_b^k\}$.

It will be highly beneficial for us to reformulate the Bell operator in terms of quantum observables instead of positive semi-definite measurements operators, in particular it will facilitate devising a sum of squares decomposition for our Bell inequality. To be more precise, let us denote the Fourier transforms of the measurements $\{F_a^j\}$ and $\{G_b^k\}$ by $\{A_j^{(n)}\}$ and $\{B_k^{(n)}\}$ (see Sec. 2.1), respectively. This allows us to rewrite the Bell operator (8) in the following form

$$W = \frac{1}{d^2} \sum_{abjk} \sum_{n_1 n_2} c_{abjk} \omega^{-an_1 - bn_2} A_j^{(n_1)} \otimes B_k^{(n_2)},$$

where as before the summations go over $\{0, 1, \ldots, d-1\}$. The coefficients

$$u_{n_1,n_2,j,k} := \frac{1}{d^2} \sum_{ab} c_{abjk} \omega^{-an_1 - bn_2}$$

correspond to the 2-dimensional discrete Fourier transform of the Bell coefficients (c_{abjk}). Since (c_{abjk}) are real, the Fourier coefficients satisfy

$$u_{n_1,n_2,j,k} = u^*_{d-n_1,d-n_2,j,k}. \tag{9}$$

We will later use the fact that this condition is also sufficient for the Bell coefficients to be real.

Analytic bounds on the quantum value of a Bell operator can be obtained by constructing an SOS decomposition. More specifically, suppose that we can show that

for all valid measurements of Alice and Bob we have

$$W \leq c\,\mathbb{1} - \sum_{j=1}^{t} L_j^\dagger L_j,$$

where $c \in \mathbb{R}$ is a constant and $(L_j)_{j=1}^t$ is a collection of bipartite operators constructed from the measurement operators of Alice and Bob. This immediately implies that for any state ρ_{AB} we have $\mathrm{tr}(W\rho_{AB}) \leq c$. Moreover, if the SOS decomposition is tight, i.e. $\beta_Q = c$, it yields explicit restrictions on the optimal realisation: any quantum realisation that achieves $\mathrm{tr}(W\rho_{AB}) = \beta_Q$ must satisfy

$$\mathrm{tr}(L_j^\dagger L_j \rho_{AB}) = 0 \tag{10}$$

for all $j \in \{1, 2, \ldots, t\}$. Note that $\mathrm{tr}(L_j^\dagger L_j \rho_{AB}) = \left\| L_j \rho_{AB}^{1/2} \right\|_F^2$, where $\|\cdot\|_F$ is the Frobenius norm. Therefore, Eq. (10) is equivalent to $L_j \rho_{AB}^{1/2} = 0$ and immediately implies $L_j \rho_{AB} = 0$.

2.4 Two approaches to self-testing

Self-testing constitutes the most complete form of device-independent certification in which the quantum realisation is determined up to local unitaries and extra degrees of freedom. These two ambiguities cannot be resolved in a device-independent scenario and it is implicitly understood that in the task of self-testing we identify the quantum realisation up to these two equivalences. For brevity we will refer to them as the *standard equivalences*. While for many scenarios these equivalences are sufficient, in some cases there is an extra equivalence resulting from the fact that the quantum realisation can be transposed to obtain an inequivalent realisation [MM11, Kan17, ABB+17]. Since the transpose is as well-understood and unavoidable as the other two equivalences, we believe it is justified to also refer to this phenomenon as self-testing.

If we want to base a self-testing statement on the observed Bell violation, there are two approaches we can choose from. The starting point of a self-testing argument are algebraic relations satisfied by the optimal observables. Typically, in order to derive such relations from the observed Bell value, we examine the SOS decomposition (although in some cases one can also look at the square of the Bell operator [Kan17]). In the first approach we use the knowledge of the ideal observables to propose a swap unitary. This unitary acts jointly on one part of the unknown state and a fresh register and attempts to swap out the relevant part of the state into the new register. Such a unitary is applied on both sides and we then use the algebraic relations to show that at the end the new registers hold the desired ideal state.

In this work, however, we use a different method proposed originally by Popescu and Rohrlich [PR92]. We use the previously deduced algebraic relations to derive relations which contain observables of a single party only. Since properties of observables can only be determined on the support of the reduced states ρ_A and ρ_B, it is convenient to assume that the reduced states are full-rank (this assumption does not affect the conclusions, but it significantly simplifies the mathematical description of the problem). These single-party algebraic relations allow us to deduce the exact form of the local observables for each party up to local unitaries and extra degrees of freedom. Once the local observables have been characterised, we can simply construct the Bell operator and diagonalise it. The state shared by the players is now determined by the eigenspace corresponding to the largest eigenvalue.

3 The modified Buhrman-Massar functional

We are now ready to present our main result. We begin with a new generalisation of the CHSH Bell inequality to d-outcome Bell scenarios.

In the CHSH scenario the settings j, k and the outcomes a, b are bits and the Bell functional is given by

$$c_{abjk} := \begin{cases} 1/4 & \text{if} \quad a \oplus b \oplus jk = 0, \\ 0 & \text{otherwise.} \end{cases}$$

It is well known that $\beta_L = 3/4$, $\beta_Q = 1/2 + 1/(2\sqrt{2})$ and $\beta_{NS} = 1$. Buhrman and Massar proposed a natural generalisation of the CHSH functional by extending the input and output alphabet to $\{0, 1, \ldots, d-1\}$ and replacing the XOR operation by addition modulo d [BM05]. The BM functional is defined as

$$c_{abjk} := \begin{cases} 1/d^2 & \text{if} \quad a + b + jk \equiv 0 \mod d, \\ 0 & \text{otherwise.} \end{cases}$$

The no-signalling value of this functional equals $\beta_{NS} = 1$ for all d [BM05] and is achieved by a straightforward generalisation of the Popescu-Rohrlich box [PR94]. The quantum value is in general not known and the only analytic bound states that whenever d is prime we have [BS15]

$$\beta_Q \leq \frac{1}{d} + \frac{d-1}{d\sqrt{d}}. \tag{11}$$

For small values of d upper and lower bounds have been computed numerically by Liang et al. [LLD09]. The only case in which the two bounds coincide corresponds to $d = 3$ and the resulting value is in excellent agreement with the analytic expression

$$\beta_Q = \frac{1}{3} + \frac{2\cos(\pi/18)}{3\sqrt{3}}$$

given in Ref. [JLL+08]. The local value has been explicitly computed for prime d up to $d = 13$ [LLD09], but no analytic formula is known.

Although the BM functional is clearly a natural generalisation of the CHSH functional, its quantum value seems hard to determine. To avoid this problem, we propose a modification of the BM functional for which the quantum value can be computed analytically. Writing the BM operator in terms of operators $A_j^{(n)}$ and $B_k^{(n)}$ yields

$$\frac{1}{d^3} \sum_{n=0}^{d-1} \sum_{jk} \omega^{njk} A_j^{(n)} \otimes B_k^{(n)}.$$

We consider a generalisation of this Bell operator given by

$$W_d := \frac{1}{d^3} \sum_{n=0}^{d-1} \lambda_n \sum_{jk} \omega^{njk} A_j^{(n)} \otimes B_k^{(n)}, \tag{12}$$

where λ_n are complex numbers of unit modulus. To ensure that condition (9) is satisfied, we must choose λ_0 to be real, i.e. $\lambda_0 = 1$, and $\lambda_n = \lambda_{d-n}^*$ for $n \in \{1, 2, \ldots, d-1\}$.

In the remainder of this section we show that for every prime dimension $d \geq 3$ there exists a valid choice of phases λ_n for which the quantum value can be computed analytically. In the first step we show that regardless of the choice of λ_n we have

$$W_d \leq \left(\frac{1}{d} + \frac{d-1}{d\sqrt{d}} \right) \mathbb{1}, \tag{13}$$

which means that the upper bound given in Eq. (11) holds for arbitrary phase factors. In the second step we specify the phases and give a quantum realisation which saturates this bound.

To prove the generic upper bound given in Eq. (13) we construct a SOS decomposition. For an integer n satisfying $|n| \leq d-1$ define

$$C_j^{(n)} := \frac{\lambda_n}{\sqrt{d}} \sum_k \omega^{njk} B_k^{(n)}, \tag{14}$$

where $\lambda_{-n} := \lambda_{d-n}$. It is easy to check that $\left[C_j^{(n)}\right]^\dagger = C_j^{(-n)}$, which allows us to write the Bell operator as

$$W_d = \frac{1}{d^2\sqrt{d}} \sum_{n=0}^{d-1} \sum_j A_j^{(n)} \otimes C_j^{(n)}.$$

The term corresponding to $n = 0$ is proportional to identity, whereas terms n and $d-n$ are conjugate to each other. Therefore, it is convenient to write the Bell operator as

$$W_d = \frac{\mathbb{1}}{d} + \frac{1}{d^2\sqrt{d}} \sum_{n=1}^{(d-1)/2} T_n \tag{15}$$

for

$$T_n := \sum_j A_j^{(n)} \otimes C_j^{(n)} + \sum_j A_j^{(-n)} \otimes C_j^{(-n)}.$$

(Note that since d is odd, $(d-1)/2$ is an integer.) This expression can be rewritten as

$$\begin{aligned} T_n = &\sum_j A_j^{(n)} A_j^{(-n)} \otimes \mathbb{1} + \mathbb{1} \otimes \sum_k B_k^{(-n)} B_k^{(n)} \\ &- \sum_j \left[L_j^{(n)}\right]^\dagger L_j^{(n)} \end{aligned} \tag{16}$$

for $L_j^{(n)} := A_j^{(-n)} \otimes \mathbb{1} - \mathbb{1} \otimes C_j^{(n)}$. Since $A_j^{(n)} A_j^{(-n)} \leq \mathbb{1}$ and $B_k^{(-n)} B_k^{(n)} \leq \mathbb{1}$, we conclude that

$$T_n \leq 2d\,\mathbb{1}, \tag{17}$$

which gives the desired operator bound.

Before proceeding to the second step, let us make two comments about this SOS decomposition. First note that so far we have only used the fact that d is odd. However, the decomposition easily generalises to the case of even d (the only difference being that the operator T_n corresponding to $n = d/2$ is a single sum of Hermitian operators). This shows that the upper bound given in Eq. (11) holds for all dimensions d (not necessarily prime). Moreover, note that the SOS decomposition can be straightforwardly generalised to the case where the coefficients λ_n are arbitrary complex numbers satisfying $\lambda_n = \lambda_{d-n}^*$.

To show that the upper bound given in Eq. (13) can be saturated, we specify the phases and give an explicit quantum realisation. For an odd prime d the phases are chosen as (see Appendix D for details)

$$\lambda_n := \left[\varepsilon_d \left(\frac{n}{d}\right)\right]^{-1} \omega^{-g(n,d)/48} \tag{18}$$

where

$$\varepsilon_d := \begin{cases} 1 & \text{if} \quad d \equiv 1 \mod 4, \\ i & \text{if} \quad d \equiv 3 \mod 4, \end{cases} \tag{19}$$

$\left(\frac{n}{d}\right)$ is the Legendre symbol[1] and

$$g(n,d) := \begin{cases} n\left[n^2 - d(d+6) + 3\right] & \text{if} \quad n \equiv 0 \mod 2 \quad \text{and} \quad (n+d+1)/2 \equiv 0 \mod 2, \\ n\left[n^2 - d(d-6) + 3\right] & \text{if} \quad n \equiv 0 \mod 2 \quad \text{and} \quad (n+d+1)/2 \equiv 1 \mod 2, \\ n(n^2+3) + 2d^2(-5n+3) & \text{if} \quad n \equiv 1 \mod 4, \\ n(n^2+3) + 2d^2(n+3) & \text{if} \quad n \equiv 3 \mod 4. \end{cases} \tag{20}$$

The optimal quantum realisation is inspired by that of Ji et al. [JLL+08]: Alice and Bob share a maximally entangled state of local dimension d,

$$|\Phi\rangle_{AB} := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A |j\rangle_B, \tag{21}$$

and perform rank-1 projective measurements which are (pairwise) mutually unbiased. Since the measurements are projective, they are fully determined by a single unitary operator: the observable. These are conveniently expressed in terms of the Heisenberg-Weyl operators:

$$X := \sum_j |j+1\rangle\langle j| \quad \text{and} \quad Z := \sum_j \omega^j |j\rangle\langle j|,$$

where the summation goes over $j \in \{0, 1, \ldots, d-1\}$ and $|d\rangle \equiv |0\rangle$. The observable corresponding to the k-th mea-

[1] Recall that the Legendre symbol $\left(\frac{n}{d}\right)$ equals $+1$ if n is a quadratic residue modulo d and -1 otherwise.

surement of Bob is given by

$$B_k := \omega^{k(k+1)} X Z^k. \tag{22}$$

It is straightforward to check that these are valid observables (they are clearly unitary, while the correctness of the spectrum can be verified by showing that $B_k^d = \mathbb{1}$), and therefore $B_k^{(n)} = B_k^n$. To see that these observables correspond to mutually unbiased bases note that if we disregard the multiplicative factor $\omega^{k(k+1)}$, which corresponds to a cyclic shift of the outcomes, we obtain one of the standard constructions of a complete set of mutually unbiased bases in prime dimension [BBRV02].

Before defining the observables of Alice, it is convenient to explore some properties of the observables of Bob. If we compute the corresponding operator $C_j^{(1)}$ (as defined in Eq. (14)), we find that $C_j^{(1)}$ itself is a valid observable (i.e. it is unitary and has the correct spectrum). Moreover, the higher-order operators satisfy

$$C_j^{(n)} = \left[C_j^{(1)}\right]^n \tag{23}$$

for $n \in \{2, 3, \ldots, d-1\}$ (see Appendix D for details). The first observation enables us to define the observables of Alice as

$$A_j := \left[C_j^{(1)}\right]^* = \frac{\lambda_1^*}{\sqrt{d}} \sum_k \omega^{-jk-k(k+1)} X Z^{-k},$$

where * denotes the complex conjugation in the standard basis (which does not affect the spectrum of the operator). The power relation given in Eq. (23) allows us to evaluate all the terms appearing in the Bell functional:

$$\begin{aligned}\langle \Phi_{AB} | A_j^{(n)} \otimes C_j^{(n)} | \Phi_{AB} \rangle &= \langle \Phi_{AB} | A_j^n \otimes \left[C_j^{(1)}\right]^n | \Phi_{AB} \rangle \\ &= \langle \Phi_{AB} | A_j^n \otimes \left[A_j^*\right]^n | \Phi_{AB} \rangle = \frac{1}{d} \operatorname{tr}\left(A_j^n \left[A_j^\dagger\right]^n\right) = 1.\end{aligned}$$

This immediately implies that

$$\langle \Phi_{AB} | W_d | \Phi_{AB} \rangle = \frac{1}{d} + \frac{d-1}{d\sqrt{d}},$$

which saturates the upper bound given in Eq. (13).

Since this quantum realisation saturates the Bell expression term-by-term, it is clear that the same will be true if we rescale terms corresponding to distinct n by arbitrary non-negative numbers (the scaling must preserve the condition (9)). In other words, we have obtained a whole family of Bell inequalities saturated by precisely the same set of probability points. For certification purposes in the exact case, i.e. when the violation is maximal, all these inequalities are equivalent. In the presence of noise they will not be the same, but it is not clear what the optimal choice of weights is.

Having presented the quantum realisation saturating the upper bound, it is easy to see how the phases λ_n were computed. We started from the observables of Bob given in Eq. (22) and looked for phases which would give the resulting operators $C_j^{(n)}$ the desired properties (unitarity and correct spectrum of $C_j^{(1)}$ and the power relation specified in Eq. (23)). Clearly, for a generic choice of observables of Bob this would not be possible. This shows that the measurements proposed by Ji et al. [JLL+08], which combine the standard MUB construction with carefully chosen prefactors, constitute a rather special choice.

We have shown how to achieve the quantum value using quantum systems of local dimension d, but it is not a priori clear that one cannot achieve it using quantum systems of lower dimension. To gain some intuition we have performed numerical search over quantum strategies of local dimension $r < d$ for $d = 3, 5$. We have used the standard see-saw procedure in which we pick a random quantum realisation (states and measurements) on $\mathbb{C}^r \otimes \mathbb{C}^r$ and optimise until we reach a local maximum. This procedure is not guaranteed to converge to the global maximum, but given a sufficient number of repetitions one can hope to explore the entire landscape of realisations in a fixed dimension. Let β_Q^r be the largest value achievable using quantum systems of local dimension r. Clearly $\beta_Q^1 = \beta_L$, whereas for our inequalities $\beta_Q^d = \beta_Q$, therefore, we only consider $r \in \{2, 3, \ldots, d-1\}$. For completeness for $d = 3, 5, 7$ we have also computed the classical value (by enumerating all deterministic strategies).

For $d = 3$ we have

$$\beta_L = \frac{1}{3} + \frac{2\cos(\pi/9)}{3\sqrt{3}} \approx 0.6950, \quad \beta_Q = \frac{1}{3} + \frac{2}{3\sqrt{3}} \approx 0.7182.$$

The numerical search over two-qubit strategies did not yield a single instance exceeding the classical value. Therefore, we conjecture that one cannot violate the $d = 3$ inequality using qubits (similar to the inequality proposed in Ref. [LRY+10]).

For $d = 5$ we have

$$\beta_L = \frac{9}{25} + \frac{8}{25\sqrt{5}} \approx 0.5031, \quad \beta_Q = \frac{1}{5} + \frac{4}{5\sqrt{5}} \approx 0.5578.$$

The numerical search suggests that

$$\beta_Q^2 = 0.5100, \quad \beta_Q^3 = \beta_Q^4 = 0.5373.$$

Interestingly enough, setting $r = 4$ always leads to a solution where the state is of Schmidt-rank 3.

For $d = 7$ we have[2]

$$\beta_L \approx 0.4001, \quad \beta_Q = \frac{1}{7} + \frac{6}{7\sqrt{7}} \approx 0.4668.$$

One might ask whether these Bell inequalities correspond to facets of the local set, but we believe that this is not the case. For $d = 3$ and $d = 5$ we have found all the deterministic points saturating the local bound (9 and 125 points, respectively) and these did not correspond to a facet. We conjecture that the inequalities for larger values of d behave in analogous manner.

4 Quantum realisations which achieve the maximal violation

In the previous section we have proposed a new Bell functional and shown that the quantum value can be achieved

[2]The analytic expression for β_L is quite complicated, so we only give an approximate value.

by performing mutually unbiased measurements on the maximally entangled state of dimension d. A natural follow-up question is whether this Bell functional is a self-test, i.e. whether this is the only manner of achieving the quantum value (up to the standard equivalences).

In this section we show that the optimal observables are fully characterised by simple algebraic relations. For $d = 3$ these conditions are sufficient to explicitly derive the form of the observables, which leads to a complete self-testing statement (although the extra freedom coming from the transposition map must be included). On the other hand, for $d = 5$ and $d = 7$ we have found additional, inequivalent quantum realisations, which implies that the introduced Bell functionals are not self-tests.

4.1 Necessary and sufficient algebraic conditions

As explained in Section 2.2 a tight SOS decomposition leads to explicit algebraic conditions that every optimal realisation must satisfy. To achieve the quantum value every term in Eq. (15) must be saturated, i.e. $\mathrm{tr}(T_n \rho_{AB}) = 2d$ for all $n \in \{1, 2, \ldots, (d-1)/2\}$. By the SOS decomposition given in Eq. (16) this implies that

$$\mathrm{tr}\left[A_j^{(n)} A_j^{(-n)} \rho_A\right] = 1, \tag{24}$$

$$\mathrm{tr}\left[B_k^{(-n)} B_k^{(n)} \rho_B\right] = 1, \tag{25}$$

$$L_j^{(n)} \rho_{AB} = 0. \tag{26}$$

for all $j, k \in \{0, 1, \ldots, d-1\}$ and $n \in \{1, 2, \ldots, d-1\}$. It is easy to see that swapping the roles of $L_j^{(n)}$ and $\left[L_j^{(n)}\right]^\dagger$ leads to an analogous SOS decomposition, which implies

$$\left[L_j^{(n)}\right]^\dagger \rho_{AB} = 0. \tag{27}$$

Conditions (24) and (25) simply require that the observables of Alice and Bob correspond to measurements which are projective on the (local) support of the state. Under the assumption that the reduced states are full-rank, we deduce that all the measurements are projective. As explained in Section 2.1 this allows us to write $A_j^{(n)} = A_j^n$ for $A_j := A_j^{(1)}$, where A_j is a unitary satisfying $A_j^d = \mathbb{1}$. Similarly $B_k^{(n)} = B_k^n$ for $B_k := B_k^{(1)}$, which is unitary and satisfies $B_k^d = \mathbb{1}$.

Conditions (26) and (27), on the other hand, imply some relations between the observables of Alice and Bob, namely:

$$(A_j^{-n} \otimes \mathbb{1})\rho_{AB} = (\mathbb{1} \otimes C_j^{(n)})\rho_{AB}, \tag{28}$$

$$(A_j^{n} \otimes \mathbb{1})\rho_{AB} = (\mathbb{1} \otimes C_j^{(-n)})\rho_{AB}. \tag{29}$$

for $n \in \{1, 2, \ldots, d-1\}$. Our goal now is to infer what impact these two relations have on the form of the operators $C_j^{(n)}$. Let us start with $n = 1$. The fact that the observables of Alice are unitary implies that

$$\begin{aligned}\rho_{AB} &= (A_j A_j^{-1} \otimes \mathbb{1})\rho_{AB} = (A_j \otimes C_j^{(1)})\rho_{AB} \\ &= (\mathbb{1} \otimes C_j^{(1)} C_j^{(-1)})\rho_{AB}.\end{aligned}$$

Tracing out the subsystem of Alice and using the fact that ρ_B is full-rank gives $C_j^{(1)} C_j^{(-1)} = \mathbb{1}$. Since $C_j^{(-1)} = \left[C_j^{(1)}\right]^\dagger$, this implies that for all $j \in \{0, 1, \ldots, d-1\}$ the operators $C_j^{(1)}$ are unitary. Moreover, since $A_j^{-d} = \mathbb{1}$, we have

$$\rho_{AB} = (A_j^{-d} \otimes \mathbb{1})\rho_{AB} = \left(\mathbb{1} \otimes \left[C_j^{(1)}\right]^d\right)\rho_{AB}$$

and we conclude that $\left[C_j^{(1)}\right]^d = \mathbb{1}$, i.e. it has the correct spectrum. Moreover, for an arbitrary integer $t \in \{1, 2, \ldots, d-1\}$ we can write

$$(\mathbb{1} \otimes C_j^{(t)})\rho_{AB} = (A_j^{-t} \otimes \mathbb{1})\rho_{AB} = (\mathbb{1} \otimes \left[C_j^{(1)}\right]^t)\rho_{AB},$$

where we have used the relation (28) twice: for $n = t$ and $n = 1$. This immediately implies that

$$C_j^{(t)} = \left[C_j^{(1)}\right]^t \tag{30}$$

for all $t \in \{1, 2, \ldots, n-1\}$.

In the previous paragraph we have established that the maximal violation requires the operators $C_j^{(n)}$ to be unitary, have the correct spectrum and satisfy the power relation (30). Since the operators $C_j^{(n)}$ are constructed out of the observables of Bob, these conditions are restrictions on the observables B_k. However, it follows immediately from the calculations presented in Section 3 that any observables satisfying these conditions can be used to construct the entire quantum realisation: we simply take the maximally entangled state and define the observables of Alice as $A_j := \left[C_j^{(1)}\right]^*$. This shows that this characterisation is tight: a set of observables of Bob is capable of producing the maximal violation (on a state that is locally full rank) if and only if the resulting operators $C_j^{(n)}$ are unitary, have the correct spectrum and satisfy the power relation.

4.2 A complete self-testing statement for $d = 3$

For $d = 3$ the algebraic characterisation is sufficient to derive the explicit form of the observables. In this case the condition $\left[C_j^{(1)}\right]^3 = \mathbb{1}$ is equivalent to

$$\left[C_j^{(1)}\right]^\dagger = \left[C_j^{(1)}\right]^2,$$

which can be rewritten as

$$\frac{\lambda_1^*}{\sqrt{3}} \sum_k \omega^{-jk} B_k^\dagger = \frac{\lambda_1^2}{3} \sum_{kk'} \omega^{j(k+k')} B_k B_{k'}$$

for $\omega = \exp(2\pi\mathrm{i}/3)$ and $\lambda_1 = e^{-\mathrm{i}\pi/18}$. Since the observables of Bob are projective, we have $B_j^2 = B_j^\dagger$, which leads to

$$-\omega^2 \sum_k \omega^{-jk} B_k^\dagger = \sum_{k \neq k'} \omega^{j(k+k')} B_k B_{k'}, \tag{31}$$

where we have used the fact that

$$\frac{\lambda_1^* \sqrt{3}}{\lambda_1^2} - 1 = -\omega^2.$$

By taking suitable linear combinations of Eq. (31) corresponding to distinct values of $j \in \{0,1,2\}$ we arrive at

$$B_0^\dagger = -\omega\{B_1, B_2\},$$
$$B_2^\dagger = -\omega\{B_0, B_1\},$$
$$B_1^\dagger = -\omega\{B_2, B_0\}$$

and these relations turn out to be sufficient to reconstruct the observables of Bob.

As explained in Section 2.4 sometimes the standard equivalences must be supplemented by the freedom resulting from the transposition map and this is precisely what happens in this case. In Appendix B we show that projectivity and the commutation relations above imply that the Hilbert space of Bob $\mathcal{H}_B$ contains a qutrit, i.e. $\mathcal{H}_B \equiv \mathcal{H}_{B'} \otimes \mathcal{H}_{B''}$ for $\mathcal{H}_{B'} \equiv \mathbb{C}^3$. Moreover, one can find a unitary $U_B : \mathcal{H}_B \to \mathcal{H}_{B'} \otimes \mathcal{H}_{B''}$ such that

$$U_B B_k U_B^\dagger = O_k^{(1)} \otimes Q_1 + O_k^{(2)} \otimes Q_2,$$

where the *canonical observables* are given by

$$O_0^{(1)} = X, \qquad O_1^{(1)} = X^2 Z, \qquad O_2^{(1)} = Z^2,$$
$$O_0^{(2)} = X, \qquad O_1^{(2)} = Z^2, \qquad O_2^{(2)} = X^2 Z$$

and Q_1, Q_2 are orthogonal projectors satisfying $Q_1 + Q_2 = \mathbb{1}_{B''}$. These two projectors identify the orthogonal subspaces corresponding to the two inequivalent solutions. Since the Bell functional is symmetric, we obtain analogous relations for the observables of Alice: we conclude that $\mathcal{H}_A \equiv \mathcal{H}_{A'} \otimes \mathcal{H}_{A''}$ for $\mathcal{H}_{A'} \equiv \mathbb{C}^3$ and that one can find a unitary $U_A : \mathcal{H}_A \to \mathcal{H}_{A'} \otimes \mathcal{H}_{A''}$ such that

$$U_A A_j U_A^\dagger = O_j^{(1)} \otimes P_1 + O_j^{(2)} \otimes P_2,$$

where P_1, P_2 are orthogonal projectors satisfying $P_1 + P_2 = \mathbb{1}_{A''}$. This characterisation allows us to write down the Bell operator as

$$U W_3 U^\dagger = \sum_{xy} W_{xy} \otimes P_x \otimes Q_y, \tag{32}$$

where $U := U_A \otimes U_B$, the summation goes over $x, y \in \{0,1\}$ and W_{xy} is the two-qutrit Bell operator corresponding to the canonical observables $A_j = O_j^{(x)}$ and $B_k = O_k^{(y)}$. The two-qutrit Bell operators can be diagonalised explicitly and we find that only W_{01} and W_{10} contain $\mu = \frac{1}{3} + \frac{2}{3\sqrt{3}}$ as an eigenvalue. In both cases the corresponding eigenspace is 1-dimensional and the eigenvector is simply the maximally entangled state of two qutrits: $|\Phi\rangle := (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$. It follows that any state that achieves the maximal violation must be of the form

$$U \rho_{AB} U^\dagger = \Phi_{A'B'} \otimes \sigma_{A''B''}, \tag{33}$$

where $\sigma_{A''B''}$ is an arbitrary state satisfying

$$\mathrm{tr}\left[(P_0 \otimes Q_1 + P_1 \otimes Q_0)\sigma_{A''B''}\right] = 1. \tag{34}$$

Condition (33) implies that the maximal violation certifies the maximally entangled state of two qutrits, which can be extracted by tracing out the auxiliary registers A'' and B''. Condition (34) shows that the maximal violation is only possible when the observables of Alice and Bob belong to the two inequivalent classes.

This self-testing result has a couple of immediate consequences. First of all, the maximal violation is achieved by a single probability point in the quantum set of correlations, which implies that this is an exposed[3] point of the quantum set. Moreover, the marginal distributions of outcomes are uniform and it is easy to see that they remain uniform even for an eavesdropper who holds a purification. Intuitively speaking, this comes from the fact that the randomness is produced from the pure entangled state $\Phi_{A'B'}$, whereas the adversary can only hold the purification of $\sigma_{A''B''}$. The maximal violation certifies $\log 3$ bits of local randomness (for each input of Alice or Bob) against an external adversary, which makes this Bell inequality a good candidate for cryptographic tasks like generation of certified randomness or secret key.

4.3 Inequivalent quantum realisations for $d = 5$ and $d = 7$

Having fully solved the $d = 3$ case one might expect to obtain similar results for higher dimensions. Perhaps surprisingly, this turns out not to be the case: we have found that in dimensions $d = 5$ and $d = 7$ there exist additional, inequivalent choices of local observables which give rise to the maximal violation. The construction is a simple generalisation of the original observables given in Eq. (22). It is easy to check that for arbitrary $q \in \{1, 2, \ldots, d-1\}$ and arbitrary function $h : \{0, 1, \ldots, d-1\} \to \{0, 1, \ldots, d-1\}$ the operators

$$B_k := \omega^{h(k)} X Z^{qk}. \tag{35}$$

constitute a valid set of observables. We have found that for $d = 5, 7$ for every $q = \{1, 2, \ldots, d-1\}$ there exists a function h which ensures that these observables of Bob give rise to valid operators $C_j^{(n)}$. To see that these are not equivalent to the original observables, it suffices to look at commutation relations: the observables defined above satisfy

$$\omega^q B_0 B_1 = B_1 B_0.$$

On the other hand, the original observables from Eq. (22) satisfy

$$\omega B_0 B_1 = B_1 B_0,$$

whereas their transposes satisfy

$$\omega^{d-1} B_0^{\mathrm{T}} B_1^{\mathrm{T}} = B_1^{\mathrm{T}} B_0^{\mathrm{T}}.$$

Clearly, whenever $d \geq 5$ choosing $q = 2$ in Eq. (35) gives rise to a solution which is neither unitarily equivalent to the original realisation nor to its transpose. Nevertheless, all these realisations use the maximally entangled state

[3] A point in the quantum set of correlations is called *exposed* if it is the unique maximiser of some Bell functional. Note, however, that although every exposed point is extremal, the converse does not hold (see Ref. [GKW+18] for an example of an extremal but not exposed point of the quantum set).

of local dimension d. Therefore, it is possible that the maximal violation certifies the state, but not the measurements. Finally, let us point out that these distinct quantum realisations lead to the same probability point. Therefore, one might conjecture that despite the ambiguity at the level of quantum realisations, the Bell functional is maximised by a single probability point.

5 Conclusions

The Buhrman-Massar generalisation of the CHSH inequality, despite its apparent simplicity, turns out to be hard to analyse. In particular, despite both analytical and numerical studies the behaviour of its quantum value is not known. In this work we propose a simple modification which allows us to analyse the resulting functional. More specifically, we propose a family of Bell functionals labelled by prime $d \geq 3$, whose quantum value can be determined analytically. For every such d we give an explicit realisation which achieves the quantum value in which Alice and Bob share the maximally entangled state of local dimension d and perform local rank-1 projective measurements which are pairwise mutually unbiased. We thus generalise the CHSH Bell inequality to d-outcome Bell scenarios, preserving at the same time the most relevant of its properties: (i) analytical computability of its maximal quantum value and (ii) achievability of the maximal quantum violation by the maximally entangled state and mutually unbiased bases.

Once we know the quantum value and we have a particular quantum realisation of it, one might ask whether this realisation is unique (up to some well-understood equivalences). The SOS decomposition yields explicit algebraic relations that the local measurements must satisfy. For $d = 3$ these can be fully resolved: the quantum realisation is unique up to extra degrees of freedom, local unitaries and transposition. Unfortunately, the situation becomes more complicated for higher d. For $d = 5$ and $d = 7$ we have found alternative realisations which despite apparent similarity (they also employ the maximally entangled state and mutually unbiased bases) are not equivalent according to the definition of self-testing (even if we allow for the extra freedom coming from the transposition map).

The first follow-up question that arises from our work is whether the new Bell functional is a self-test in some weaker sense. We conjecture that the maximal violation requires maximal entanglement and mutually unbiased bases, but providing a mathematical formulation of this conjecture is not trivial: for instance, it is clear that not all possible combinations of mutually unbiased bases will give rise to the maximal violation.

Another interesting direction would be to investigate whether the new Bell functionals can be modified to be maximally violated by other entangled states, keeping at the same time their attractive features, i.e. analytically computable quantum value and an explicit quantum realisation achieving it. Similarly to how adding a marginal term to the CHSH inequality yields the tilted CHSH inequality [AMP12], which has found numerous applications, one might add an analogous local term to the new Bell operator and investigate the consequences. On one hand, one might expect such an inequality to be maximally violated by a non-maximally entangled state of dimension d. On the other hand, given the recent non-closure results [Slo17, DPP17, CS18], it is not even guaranteed that the maximal violation can be achieved by finite-dimensional states. Therefore, adding the marginal term could have much more dramatic consequences that in the case of binary outcomes, which makes the problem even more interesting to study.

Acknowledgements

We would like to thank Antonio Acín, Joseph Bowles, Roberto Ferrara, Jinhyoung Lee, Giacomo De Palma and Wonmin Son for fruitful discussions. R. A. acknowledges the support from the Foundation for Polish Science through the First Team project (First TEAM/2017-4/31) co-financed by the European Union under the European Regional Development Fund. J. K. acknowledges support from the POLONEZ programme which has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant (grant no. 665778), the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Action ROSETTA (grant no. 749316), the European Research Council (grant no. 337603) and VILLUM FONDEN via the QMATH Centre of Excellence (grant no. 10059). This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie-Skłodowska-Curie grant agreement No 748549. J. T. acknowledges support from the Alexander von Humboldt Foundation. I. Š., F. B. and A. S. acknowledge the support from Spanish MINECO (QIBEQI FIS2016-80773-P, Severo Ochoa SEV-2015-0522 and a Severo Ochoa PhD fellowship), Fundacio Cellex, Generalitat de Catalunya (SGR875 and CERCA Program), ERC CoG QITBOX and AXA Chair in Quantum Information Science.

A Measurements and observables

In this appendix we prove some properties stated in Section 2.1 and let us start with the following proposition.

Proposition A.1. *Let $\{F_a\}_a$ be a collection of positive semidefinite operators acting on a finite-dimensional Hilbert*

space satisfying $\sum_a F_a = \mathbb{1}$*. Then, for arbitrary phases* $\phi_a \in [0, 2\pi)$ *the operator*

$$A := \sum_a e^{\mathbb{i}\phi_a} F_a$$

satisfies $A^\dagger A \leq \mathbb{1}$*. Moreover, if the phases are distinct* ($\phi_a = \phi_b \iff a = b$)*, the operator equality* $A^\dagger A = \mathbb{1}$ *holds iff the operators are orthogonal projectors, i.e.* $F_a F_b = \delta_{ab} F_a$ *with* δ_{ab} *being the standard Kronecker's delta.*

Proof. Define

$$V := \sum_a \sqrt{F_a} \otimes |a\rangle,$$
$$U := \mathbb{1} \otimes \sum_a e^{\mathbb{i}\phi_a} |a\rangle\langle a|$$

and note that $A = V^\dagger U V$. The operator V is an isometry ($V^\dagger V = \mathbb{1}$), which implies that $VV^\dagger = \Pi$ for some projector Π and in particular $VV^\dagger \leq \mathbb{1}$. Combining this with the fact that U is a unitary immediately implies

$$A^\dagger A = V^\dagger U^\dagger V V^\dagger U V \leq V^\dagger U^\dagger \cdot \mathbb{1} \cdot U V = V^\dagger U^\dagger U V = V^\dagger V = \mathbb{1}.$$

To prove the second part note that

$$A^\dagger A = \sum_a F_a^2 + \sum_{a \neq b} e^{\mathbb{i}(\phi_a - \phi_b)} F_b F_a + e^{-\mathbb{i}(\phi_a - \phi_b)} F_a F_b.$$

The "if" part is clear, so let us focus on the "only if" statement. The trace of $A^\dagger A$ satisfies

$$\begin{aligned} \operatorname{tr}\left(A^\dagger A\right) &= \sum_a \operatorname{tr}\left(F_a^2\right) + 2 \sum_{a \neq b} \cos(\phi_a - \phi_b) \operatorname{tr}(F_a F_b) \\ &\leq \sum_a \operatorname{tr}\left(F_a^2\right) + 2 \sum_{a \neq b} \operatorname{tr}(F_a F_b) = \operatorname{tr}\left[\Big(\sum_a F_a\Big)^2\right] = \operatorname{tr} \mathbb{1}. \end{aligned}$$

If $A^\dagger A = \mathbb{1}$, this inequality is tight, which means that for all $a \neq b$ we have

$$\cos(\phi_a - \phi_b) \operatorname{tr}(F_a F_b) = \operatorname{tr}(F_a F_b).$$

Since the phases are distinct, we deduce that $\operatorname{tr}(F_a F_b) = 0$, which for positive semidefinite operators implies orthogonality, i.e. $F_a F_b = 0$ for $a \neq b$. The fact that the upper bound

$$A^\dagger A = \sum_a F_a^2 \leq \sum_a F_a = \mathbb{1}$$

is tight implies that $F_a^2 = F_a$ for all a. □

Let us now apply these results to the operators $A^{(n)}$. Recall that for a d-outcome measurement given by $\{F_a\}_{a=0}^{d-1}$ the operator $A^{(n)}$ is defined as

$$A^{(n)} := \sum_{a=0}^{d-1} \omega^{an} F_a$$

for $\omega := \exp(2\pi\mathbb{i}/d)$. The first part of Proposition A.1 immediately implies that $[A^{(n)}]^\dagger A^{(n)} \leq \mathbb{1}$ for all n. If the original measurement is projective, i.e. the measurement operators are orthogonal projectors $F_a F_b = \delta_{ab} F_a$, the measurement can be encoded in an observable $A := A^{(1)}$ (it is easy to verify that $A^{(n)} = A^n$). This observable is unitary $A^\dagger A = A A^\dagger = \mathbb{1}$ and satisfies $A^d = \mathbb{1}$. The second part of Proposition A.1 allows us to deduce that the measurement is projective by looking only at the $A^{(n)}$ operators: the operator $A^{(1)}$ satisfies the condition of the proposition, so if $[A^{(1)}]^\dagger A^{(1)} = \mathbb{1}$, then the measurement is projective. In fact, the same argument works for $A^{(k)}$ for any integer k which is coprime to d.

B Optimal observables for $d = 3$

In this appendix we show that the commutation relations derived in Sec. 4.2 allow us to reconstruct the optimal observables. Let us start with two technical propositions.

Proposition B.1. *Let d be an arbitrary integer and let X and Z be the corresponding Heisenberg-Weyl operators*

$$X := \sum_{j=0}^{d-1} |j+1\rangle\langle j| \quad \textit{and} \quad Z := \sum_{j=0}^{d-1} \omega^j |j\rangle\langle j|,$$

where $|d\rangle \equiv |0\rangle$. Let B_0, B_1 be unitaries acting on a finite-dimensional Hilbert space $\mathcal{H}$ satisfying $B_0^d = B_1^d = \mathbb{1}$. Suppose B_0 and B_1 satisfy the commutation relation

$$B_0 B_1 = \omega^q B_1 B_0,$$

where q and d are coprime. Then, $\dim(\mathcal{H}) = d \cdot t$ for some integer $t \geq 1$ and there exists a unitary $U : \mathcal{H} \to \mathbb{C}^d \otimes \mathbb{C}^t$ such that

$$UB_0U^\dagger = Z^q \otimes \mathbb{1} \quad \textit{and} \quad UB_1U^\dagger = X \otimes \mathbb{1}. \tag{36}$$

Proof. Let $t \in \mathbb{N}$ be the multiplicity of the $\lambda = 1$ eigenvalue of B_0 and let $\{|e_j^{(0)}\rangle\}_{j=0}^{t-1}$ be an orthonormal basis of the corresponding eigenspace. For $k = 1, 2, \ldots, d-1$ define

$$|e_j^{(k)}\rangle := B_1^k |e_j^{(0)}\rangle.$$

The commutation relation implies that for any $k \in \mathbb{N}$

$$B_0 B_1^k = \omega^{qk} B_1^k B_0$$

and therefore

$$B_0 |e_j^{(k)}\rangle = \omega^{qk} |e_j^{(k)}\rangle.$$

It is also clear that the vectors $\{|e_j^{(k)}\rangle\}_{j=0}^{t-1}$ span the eigenspace of B_0 corresponding to the eigenvalue ω^{qk}. Since q and d are coprime, going over $k = 1, 2, \ldots, d-1$ recovers all the eigenspaces of B_0. This allows us to deduce that $\dim(\mathcal{H}) = d \cdot t$ and that the set $\{|e_j^{(k)}\rangle\}$ for $j = 0, 1, \ldots, t-1$ and $k = 0, 1, \ldots, d-1$ constitutes an orthonormal basis for $\mathcal{H}$. Writing the two observables in this basis gives

$$B_0 = \sum_{j=0}^{t-1} \sum_{k=0}^{d-1} \omega^{qk} |e_j^{(k)}\rangle\langle e_j^{(k)}|,$$
$$B_1 = \sum_{j=0}^{t-1} \sum_{k=0}^{d-1} |e_j^{(k+1)}\rangle\langle e_j^{(k)}|,$$

where $|e_j^{(d)}\rangle \equiv |e_j^{(0)}\rangle$. The desired unitary $U : \mathcal{H} \to \mathbb{C}^d \otimes \mathbb{C}^t$ is given by

$$U|e_j^{(k)}\rangle = |k\rangle|g_j\rangle,$$

where $\{|k\rangle\}_{k=0}^{d-1}$ is the standard basis on $\mathbb{C}^d$ and $\{|g_j\rangle\}_{j=0}^{t-1}$ is an arbitrary basis on $\mathbb{C}^t$. □

In Eq. (36) we have chosen the canonical observables to be Z^q and X, but clearly we can replace them with any observables satisfying the right commutation relation (this is precisely what Prop. B.1). For our purposes it is better to make a different choice. For $d = 3$ and $q = 1$ we choose the unitary U such that

$$UB_0U^\dagger = X \otimes \mathbb{1} \quad \text{and} \quad UB_1U^\dagger = X^2 Z \otimes \mathbb{1}, \tag{37}$$

whereas for $d = 3$ and $q = 2$ we choose

$$UB_0U^\dagger = X \otimes \mathbb{1} \quad \text{and} \quad UB_1U^\dagger = Z^2 \otimes \mathbb{1}. \tag{38}$$

Let us also mention that this argument could be generalised to infinite-dimensional Hilbert spaces to yield a unitary $U : \mathcal{H} \to \mathbb{C}^d \otimes \mathcal{H}'$, where both $\mathcal{H}$ and $\mathcal{H}'$ are infinite-dimensional.

Proposition B.2. *Let $B_0, B_1 \in \mathcal{L}(\mathcal{H}_B)$ be unitary operators satisfying $B_0^3 = B_1^3 = \mathbb{1}$. If the anticommutator $\{B_0, B_1\}$ is unitary, then $\mathcal{H}_B \equiv \mathcal{H}_{B'} \otimes \mathcal{H}_{B''}$ for $\mathcal{H}_{B'} \equiv \mathbb{C}^3$ and there exists a unitary $U : \mathcal{H}_B \to \mathcal{H}_{B'} \otimes \mathcal{H}_{B''}$ such that*

$$UB_0U^\dagger = X \otimes Q_1 + X \otimes Q_2,$$
$$UB_1U^\dagger = X^2 Z \otimes Q_1 + Z^2 \otimes Q_2,$$

where Q_1 and Q_2 are orthogonal projectors satisfying $Q_1 + Q_2 = \mathbb{1}_{B''}$.

Proof. The unitarity of the anticommutator reads

$$\{B_0^\dagger, B_1^\dagger\}\{B_0, B_1\} = \mathbb{1}$$

and is equivalent to

$$T + T^\dagger + \mathbb{1} = 0,$$

where $T = B_0^\dagger B_1^\dagger B_0 B_1$. This implies that the eigenvalues of T satisfy $\lambda + \lambda^* + 1 = 0$ and since T is unitary, the only possibilities are $\lambda = \omega$ and $\lambda = \omega^2$. Let us now show that the unitaries B_0 and B_1 respect the block structure of T. We choose a basis in which T reads

$$T = \begin{pmatrix} \omega\mathbb{1} & \\ & \omega^2\mathbb{1} \end{pmatrix}$$

and write B_0 in the same basis

$$B_0 = \begin{pmatrix} E_0 & F_0 \\ F_1 & E_1 \end{pmatrix}.$$

The requirement $B_0^\dagger = B_0^2$ implies

$$\begin{pmatrix} E_0^\dagger & F_1^\dagger \\ F_0^\dagger & E_1^\dagger \end{pmatrix} = \begin{pmatrix} E_0^2 + F_0F_1 & E_0F_0 + F_0E_1 \\ F_1E_0 + E_1F_1 & F_1F_0 + E_1^2 \end{pmatrix}. \tag{39}$$

Let

$$R := B_0T = \begin{pmatrix} \omega E_0 & \omega^2 F_0 \\ \omega F_1 & \omega^2 E_1 \end{pmatrix}. \tag{40}$$

Since $R = B_1^\dagger B_0 B_1$, we also have $R^\dagger = R^2$, which in the block form reads

$$\begin{pmatrix} \omega^2 E_0^\dagger & \omega^2 F_1^\dagger \\ \omega F_0^\dagger & \omega E_1^\dagger \end{pmatrix} = \begin{pmatrix} \omega^2 E_0^2 + F_0F_1 & E_0F_0 + \omega F_0E_1 \\ \omega^2 F_1E_0 + E_1F_1 & F_1F_0 + \omega E_1^2 \end{pmatrix}. \tag{41}$$

The top-left entries of Eqs. (39) and (41), i.e.

$$\begin{aligned} E_0^\dagger &= E_0^2 + F_0F_1, \\ \omega^2 E_0^\dagger &= \omega^2 E_0^2 + F_0F_1 \end{aligned}$$

immediately imply that $F_0F_1 = 0$. Similarly, the bottom-right entries imply $F_1F_0 = 0$. The bottom-left entries read

$$\begin{aligned} F_0^\dagger &= F_1E_0 + E_1F_1, \\ \omega F_0^\dagger &= \omega^2 F_1E_0 + E_1F_1. \end{aligned}$$

Right-multiplying both equations by F_0 yields

$$\begin{aligned} F_0^\dagger F_0 &= F_1E_0F_0, \\ \omega F_0^\dagger F_0 &= \omega^2 F_1E_0F_0, \end{aligned}$$

which immediately implies that $F_0^\dagger F_0 = 0$ and, therefore, $F_0 = 0$. Similarly, by looking at the top-right entry we deduce that $F_1 = 0$. Therefore, B_0 respects the block structure of T. Since the same argument applies to B_1, when solving the equation $T = B_0^\dagger B_1^\dagger B_0 B_1$ it suffices to solve the two blocks separately. Fortunately, on each block the unitaries B_0 and B_1 satisfy a commutation relation covered by Proposition B.1, so we already have the solution. In particular, if we use the canonical observables specified in Eqs. (37) and (38) the unitaries B_0 and B_1 in the block form are given by

$$B_0 = \begin{pmatrix} X \otimes \mathbb{1} & \\ & X \otimes \mathbb{1} \end{pmatrix} \quad \text{and} \quad B_1 = \begin{pmatrix} X^2Z \otimes \mathbb{1} & \\ & Z^2 \otimes \mathbb{1} \end{pmatrix}.$$

The final step is to incorporate the block structure into the tensor product according to the equivalence

$$(\mathbb{C}^3 \otimes \mathbb{C}^{t_1}) \oplus (\mathbb{C}^3 \otimes \mathbb{C}^{t_2}) \equiv \mathbb{C}^3 \otimes (\mathbb{C}^{t_1} \oplus \mathbb{C}^{t_2}) \equiv \mathbb{C}^3 \otimes \mathbb{C}^{t_1+t_2},$$

which gives rise to the projectors Q_1 and Q_2. □

This proposition allows us to prove the results stated in the main text. The commutation relation $B_2^\dagger = -\omega\{B_0, B_1\}$ implies that the anticommutator $\{B_0, B_1\}$ is unitary, which allows us to determine the exact form of B_0 and B_1. Finally, the observable B_2 can be computed from the same relation.

C Quadratic Gauss sums

In this appendix we compute certain quadratic Gauss sums which we use in our considerations in Appendix D.

Observation C.1. *Let a and b be two integers and let $\omega = \exp(2\pi\mathbb{i}/d)$ with d being a prime number. Then,*

$$\sum_{i=0}^{d-1} \omega^{a(i^2+bi)} = \varepsilon_d \sqrt{d} \left(\frac{a}{d}\right) \begin{cases} \omega^{-\frac{1}{4}ab^2}, & b \equiv 0 \bmod 2 \\ \omega^{-\frac{1}{4}a(d-b)^2}, & b \equiv 1 \bmod 2 \end{cases} \tag{42}$$

Proof. Assuming first b to be even, we have the following chain of equalities

$$\sum_{i=0}^{d-1} \omega^{ai^2+abi} = \omega^{-\frac{1}{4}ab^2} \sum_{i=0}^{d-1} \omega^{a\left[i+\frac{b}{2}\right]^2} = \omega^{-\frac{1}{4}ab^2} \sum_{i=\frac{b}{2}}^{d-1+\frac{b}{2}} \omega^{ai^2} = \omega^{-\frac{1}{4}ab^2} \sum_{i=0}^{d-1} \omega^{ai^2} = \varepsilon_d \sqrt{d} \left(\frac{a}{d}\right) \omega^{-\frac{1}{4}ab^2}, \tag{43}$$

where to get the third expression we shifted the summation range by an integer $b/2$, while the third equality is a result of the fact that for prime d this shifting does not change the value of the Gauss sum.

Let us then consider the case of odd b. We notice that although $b/2$ is not an integer, $(d-b)/2$ is due to the fact that d is odd and a difference of two odd numbers is an even number. Moreover, $\omega^{-ndi} = 1$, and therefore we can follow the same reasoning as above, which gives

$$\sum_{i=0}^{d-1} \omega^{a(i^2+bi)} = \sum_{i=0}^{d-1} \omega^{ai^2} \omega^{-a(d-b)i} = \omega^{-\frac{1}{4}a(d-b)^2} \sum_{i=0}^{d-1} \omega^{a\left(i-\frac{d-b}{2}\right)^2} = \varepsilon_d \sqrt{d} \left(\frac{a}{d}\right) \omega^{-\frac{a}{4}(d-b)^2}. \tag{44}$$

□

Observation C.2. *Let a be an even integer and $b = c/2$ for some odd integer c and let $\omega = \exp(2\pi\mathbb{i}/d)$ with d being a prime number. Then, the following identities hold true*

$$\sum_{i=0}^{d-1} \omega^{a(i^2+bi)} = \varepsilon_d \sqrt{d} \left(\frac{a}{d}\right) \begin{cases} \omega^{-\frac{1}{4}ab'^2}, & b' \equiv 0 \bmod 2 \\ \omega^{-\frac{1}{4}a(d-b')^2}, & b' \equiv 1 \bmod 2, \end{cases} \tag{45}$$

where $b' = b + d/2$.

Proof. We could follow the above reasoning, however, b is not an integer. To overcome this difficulty, we exploit the fact that d is odd and therefore $b' \equiv b + d/2$ is an integer. Moreover, due to the fact that a is even $\omega^{aid/2} = 1$ for any i, and consequently,

$$\sum_{i=0}^{d-1} \omega^{a(i^2+bi)} = \sum_{i=0}^{d-1} \omega^{a\left[i^2+\left(b+\frac{d}{2}\right)i\right]} = \sum_{i=0}^{d-1} \omega^{a(i^2+b'i)}. \tag{46}$$

We then obtain (45) by applying Eq. (42) to the last term in the above expression, which completes the proof. □

D Determining the phases λ_n

Here we will show how the phases λ_n appearing in the Bell operator (12) can be fixed so that the maximal quantum violation of the corresponding Bell inequality is achieved by the maximally entangled state (21); in other words, we will justify the choice of phases defined in Eqs. (18) and (20). We will also justify the choice of Alice's observables made in the main text.

To make this section self-contained let us recall the definition of the Bell operator stated already in Eq. (12):

$$W_d = \frac{1}{d^2\sqrt{d}} \sum_{n=0}^{d-1} \sum_{j=0}^{d-1} A_j^{(n)} \otimes C_j^{(n)}, \tag{47}$$

where

$$C_j^{(n)} := \frac{\lambda_n}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{njk} B_k^{(n)}. \tag{48}$$

We begin by deriving the optimal observables of Alice. For this purpose, let us first show that for a suitable choice of λ_1, the operators $C_j^{(1)} \equiv C_j$, defined as

$$C_j = \frac{\lambda_1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{jk} B_k, \tag{49}$$

are proper observables in our scenario, that is, they are unitary and have eigenvalues ω^i with $i = 0, \ldots, d-1$. In fact, it is not difficult to see, with the aid of formula (42), that for any choice of the phase λ_1, the operators C_j are indeed unitary. Let us then determine the value of λ_1 for which the second condition is satisfied too. To this aim, we demand that $C_j^d = \mathbb{1}$ for any j, which is equivalent to say that C_j have the required spectrum.

Before exploiting the above condition, let us first obtain a simpler matrix form of C_j. From (48) and the fact that $B_k = \omega^{k(k+1)} XZ^k$ we have

$$C_j = \frac{\lambda_1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{jk} \omega^{k(k+1)} XZ^k = \frac{\lambda_1}{\sqrt{d}} \sum_{i=0}^{d-1} \left[\sum_{k=0}^{d-1} \omega^{k^2+k(j+1+i)} \right] |i+1\rangle\langle i| \equiv \frac{\lambda_1}{\sqrt{d}} \sum_{i=0}^{d-1} G(i,j,d) |i+1\rangle\langle i|, \tag{50}$$

where to obtain second equality we have used the explicit matrix form of the Z operator and we have denoted

$$G(i,j,d) = \sum_{k=0}^{d-1} \omega^{k^2+k(i+j+1)}. \tag{51}$$

The last sum has already been computed in Appendix C and its closed formula is given in Eq. (42).

Now, taking the dth power of C_j we obtain

$$C_j^d = \frac{\lambda_1^d}{\sqrt{d}^d} \sum_{i=0}^{d-1} G(i,j,d) \cdot G(i+1,j,d) \cdot \ldots \cdot G(i+d-1,j,d) |i\rangle\langle i|. \tag{52}$$

After quite tedious algebra one finds, by virtue of Eq. (42), that the above product of Gauss sums amounts to $G(i,j,d) \cdot \ldots \cdot G(i+d-1,j,d) = \varepsilon_d^d \, d^{d/2} \omega^{-d(d^2-1)/12}$ and thus $C_j^d = \mathbb{1}$ if $\lambda_1 = \omega^{(d^2-1)/12}/\varepsilon_d$ which agrees with Eqs. (18) and (20).

Having established that C_j are proper observables in Bell scenario, we define Alice's observables as $A_j = C_j^*$, with the main reason being the fact that in such a case $A_j \otimes C_j$ is a stabilizing operator of $|\Phi_{AB}\rangle$ for any j, that is,

$$A_j \otimes C_j |\Phi_{AB}\rangle = |\Phi_{AB}\rangle. \tag{53}$$

Let us now determine the phases λ_n for $n > 1$. To this aim we impose the following condition

$$A_j^{(n)} \otimes C_j^{(n)} |\Phi_{AB}\rangle = |\Phi_{AB}\rangle \tag{54}$$

for any j and n, which we will use to determine the explicit values of λ_n. Owing to the well-known property of the maximally entangled state that $X \otimes Y |\Phi_{AB}\rangle = \mathbb{1} \otimes YX^T |\psi_{AB}\rangle$ for any pair of matrices X, Y, the condition (54) can be stated equivalently as

$$C_j^{(n)} = A_j^{(n)*} = [A_j^*]^n = C_j^n. \tag{55}$$

In order to exploit this condition, we need to find the matrix form of each of its sides. We begin with $C_j^{(n)}$. Using the explicit form of B_k and the fact that

$$(XZ^k)^n = \sum_{l=0}^{d-1} \omega^{k\frac{n(n-1)}{2}} \omega^{nkl} |l+n\rangle\langle l|, \tag{56}$$

we can write $C_j^{(n)}$ as

$$C_j^{(n)} = \frac{\lambda_n}{\sqrt{d}} \sum_{l=0}^{d-1} \left[\sum_{k=0}^{d-1} \omega^{nk^2} \omega^{nk\left(j+l+\frac{n+1}{2}\right)} \right] |l+n\rangle\langle l| \tag{57}$$

Using Eqs. (42) and (45), we finally arrive at

$$C_j^{(n)} = \lambda_n \, \varepsilon_d \left(\frac{n}{d}\right) \sum_{l=0}^{d-1} |l+n\rangle\langle l| \begin{cases} \omega^{-\frac{n}{4}\left(j+l+\frac{n+1}{2}\right)^2}, & j+l+\frac{n+1}{2} \equiv 0 \bmod 2 \\ \omega^{-\frac{n}{4}\left(j+l+\frac{n+1}{2}-d\right)^2}, & j+l+\frac{n+1}{2} \equiv 1 \bmod 2, \end{cases} \tag{58}$$

for odd n and

$$C_j^{(n)} = \lambda_n \, \varepsilon_d \left(\frac{n}{d}\right) \sum_{l=0}^{d-1} |l+n\rangle\langle l| \begin{cases} \omega^{-\frac{n}{4}\left(j+l+\frac{n+1+d}{2}\right)^2}, & j+l+\frac{n+1+d}{2} \equiv 0 \bmod 2 \\ \omega^{-\frac{n}{4}\left(j+l+\frac{n+1-d}{2}\right)^2}, & j+l+\frac{n+1+d}{2} \equiv 1 \bmod 2. \end{cases} \tag{59}$$

for even n.

Let us now move on to C_j^n. Using Eq. (50) we can write

$$\begin{aligned} C_j^n &= \frac{\lambda_1^n}{\sqrt{d}^n}\sum_{i=0}^{d-1} G(i,j,d)\cdot G(i+1,j,d)\cdot\ldots\cdot G(i+n-1,j,d)|i+n\rangle\langle i| \\ &= \frac{\lambda_1^n}{\sqrt{d}^n}\left[\sum_{k=0}^{(d-1)/2} G(2k,j,d)\cdot G(2k+1,j,d)\cdot\ldots\cdot G(2k+n-1,j,d)|2k+n\rangle\langle 2k| \right. \\ &\qquad \left. + \sum_{k=0}^{(d-3)/2} G(2k+1,j,d)\cdot G(2k+2,j,d)\cdot\ldots\cdot G(2k+1+n-1,j,d)|2k+1+n\rangle\langle 2k+1|\right], \end{aligned} \tag{60}$$

where to facilitate computation of the above products of Gauss sums we have split the sum into two sums, one over even and one over odd i's. Then, to compute these products we use Eqs. (42) and (45), dividing our analysis into four cases:

- odd n, odd j,

$$G(2k,j,d)\ldots G(2k+n-1,j,d) = \varepsilon_d^n\, d^{n/2}\,\omega^{-\frac{1}{24}\{3d^2(n-1)+n-3d(n-1)(1+2j+4k+n)+n[6(j+2k)(1+j+2k)+3(1+2j+4k)n+2n^2]\}} \tag{61}$$

$$G(2k+1,j,d)\ldots G(2k+1+n-1,j,d) = \varepsilon_d^n\, d^{n/2}\,\omega^{-\frac{1}{24}\{13n+3d^2(1+n)-3d(1+n)(3+2j+4k+n)+n[6(j+2k)(3+j+2k)+3(3+2j+4k)n+2n^2]\}} \tag{62}$$

- odd n, even j,

$$G(2k,j,d)\ldots G(2k+n-1,j,d) = \varepsilon_d^n\, d^{n/2}\,\omega^{-\frac{1}{24}\{n+3d^2(n+1)-3d(n+1)(1+2j+4k+n)+n[6(j+2k)(j+1+2k)+3(1+2j+4k)n+2n^2]\}} \tag{63}$$

$$G(2k+1,j,d)\ldots G(2k+1+n-1,j,d) = \varepsilon_d^n\, d^{n/2}\,\omega^{-\frac{1}{24}\{3d^2(n-1)-3d(n-1)(3+4k+n)+n[13+24k^2+12k(3+n)+n(9+2n)]\}} \tag{64}$$

- even n, odd j,

$$G(2k,j,d)\ldots G(2k+n-1,j,d) = \varepsilon_d^n\, d^{n/2}\,\omega^{-\frac{n}{24}\{1+3d^2+6j+12k+6(j+2k)^2+3n+6(j+2k)n+2n^2-3d(2+2j+4k+n)\}} \tag{65}$$

$$G(2k+1,j,d)\ldots G(2k+1+n-1,j,d) = \varepsilon_d^n\, d^{n/2}\,\omega^{-\frac{n}{24}\{13+3d^2+18j+36k+6(j+2k)^2+9n+6(j+2k)n+2n^2-3d(2+2j+4k+n)\}} \tag{66}$$

- Even n, even j,

$$G(2k,j,d)\ldots G(2k+n-1,j,d) = \varepsilon_d^n\, d^{n/2}\,\omega^{-\frac{n}{24}\{1+3d^2+6j+12k+6(j+2k)^2+3n+6(j+2k)n+2n^2-3d(2j+4k+n)\}} \tag{67}$$

$$G(2k+1,j,d)\ldots G(2k+1+n-1,j,d) = \varepsilon_d^n\, d^{n/2}\,\omega^{-\frac{n}{24}\{13+3d^2+18j+36k+6(j+2k)^2+9n+6(j+2k)n+2n^2-3d(4+2j+4k+n)\}} \tag{68}$$

Having determined both sides of Eq. (55), we can now compare them. Traditionally, we will consider the cases of odd and even n separately.

Odd n. Let us assume that $n \mod 4 \equiv 1$, i.e., $n = 4m+1$ with $m \in \mathbb{N}$. Let also j be odd. Then, to determine λ_n we compare Eq. (61) and the first formula in Eq. (58) with $l = 2k$, which, after some algebra, gives us

$$\lambda_n = \frac{1}{\varepsilon_d\left(\frac{n}{d}\right)}\omega^{-\frac{1}{48}[n(n^2+3)+2d^2(-5n+3)]}. \tag{69}$$

We then, check that if we compare Eq. (62) with the second formula in Eq. (58) with $l = 2k+1$, we obtain exactly the same phases.

On the other hand, if we assume that $n \mod 4 \equiv 3$, i.e., $n = 4m+3$ with $m \in \mathbb{N}$ and also that j is odd, we compare Eq. (62) with the first formula in Eq. (58) with $l = 2k+1$, which leads us to

$$\lambda_n = \frac{1}{\varepsilon_d\left(\frac{n}{d}\right)}\omega^{-\frac{1}{48}[n(n^2+3)+2d^2(n+3)]}. \tag{70}$$

The same formula is obtained when comparing Eq. (61) with the second formula in Eq. (58) with $l = 2k$.

On can check that exactly the same formulas are obtained in the case of even j.

Even n. Assume first that j is odd and $n \mod 4 \equiv 0$, meaning that $n = 4m$ with $m \in \mathbb{N}$. Let us also assume that $d = 4p+1$ with $p \in \mathbb{N}$. Then, comparison of Eq. (65) with the first formula in Eq. (59) for $l = 2k$ as well as Eq. (66) with the second formula in Eq. (59) for $l = 2k+1$, gives

$$\lambda_n = \frac{1}{\varepsilon_d\left(\frac{n}{d}\right)}\omega^{-\frac{n}{48}[n^2-d(d-6)+3]}. \tag{71}$$

If we then assume that $d = 4p+3$ with $p \in \mathbb{N}$ and compare Eq. (65) with the second formula in (59) with $l = 2k$, we obtain

$$\lambda_n = \frac{1}{\varepsilon_d\left(\frac{n}{d}\right)}\omega^{-\frac{n}{48}[n^2-d(d+6)+3]}. \tag{72}$$

Comparison of Eq. (66) with the first formula in Eq. (59) with $l = 2k+1$, leads to the same formula.

Let us finally consider the case of $n = 4m+2$ for any $m \in \mathbb{N}$. Then, as before we consider two cases $d = 4p+1$ and $d = 4p+3$ with $p \in \mathbb{N}$. In the first case, we use Eq. (65) and the second formula in Eq. (59) to get (72). As the same time, the same formula for λ_n is obtained from Eq. (66) and the first formula in Eq. (59) with $l = 2k$.

Then, in the second case, i.e., $d = 4p+3$, we exploit Eq. (65) with the first formula in Eq. (59), which leads us to λ_n given in Eq. (71). At the same time, comparison of Eq. (66) with the second formula in Eq. (59) with $l = 2k+1$ gives exactly the same formula.

One then checks that the same phases are obtained under the assumption that j is even.

Summary. To summarize, depending on the value of n we use the following λ's:

- $n = 4m$. We use Eq. (71) for $d = 4p+3$ and Eq. (72) for $d = 4p+1$.
- $n = 4m+1$. We use Eq. (70) for any d.
- $n = 4m+2$. We use Eq. (71) for $d = 4p+1$ and Eq. (72) for $d = 4p+3$.
- $n = 4m+3$. We use Eq. (69) irrespectively of the dimension.

References

[ABB+17] O. Andersson, P. Badziąg, I. Bengtsson, I. Dumitru, and A. Cabello. Self-testing properties of Gisin's elegant Bell inequality. *Phys. Rev. A*, 96: 032119, 2017. DOI: 10.1103/PhysRevA.96.032119.

[ABG+07] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98: 230501, 2007. DOI: 10.1103/PhysRevLett.98.230501.

[AFDF+18] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.*, 9: 459, 2018. DOI: 10.1038/s41467-017-02307-4.

[AGM06] A. Acín, N. Gisin, and L. Masanes. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.*, 97: 120405, 2006. DOI: 10.1103/PhysRevLett.97.120405.

[AMP12] A. Acín, S. Massar, and S. Pironio. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.*, 108: 100402, 2012. DOI: 10.1103/PhysRevLett.108.100402.

[BBRV02] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34: 512, 2002. DOI: 10.1007/s00453-002-0980-7.

[BCP+14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86: 419, 2014. DOI: 10.1103/RevModPhys.86.419.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1: 195, 1964.

[BHK05] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95: 010503, 2005. DOI: 10.1103/PhysRevLett.95.010503.

[BKP06] J. Barrett, A. Kent, and S. Pironio. Maximally nonlocal and monogamous quantum correlations. *Phys. Rev. Lett.*, 97: 170409, 2006. DOI: 10.1103/PhysRevLett.97.170409.

[BLM+09] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani. Device independent state estimation based on Bell's inequalities. *Phys. Rev. A*, 80: 062327, 2009. DOI: 10.1103/PhysRevA.80.062327.

[BM05] H. Buhrman and S. Massar. Causality and Tsirelson's bounds. *Phys. Rev. A*, 72: 052103, 2005. DOI: 10.1103/PhysRevA.72.052103.

[BP15] C. Bamps and S. Pironio. Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing. *Phys. Rev. A*, 91: 052111, 2015. DOI: 10.1103/PhysRevA.91.052111.

[BPA+08] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani. Testing the dimension of Hilbert spaces. *Phys. Rev. Lett.*, 100: 210503, 2008. DOI: 10.1103/PhysRevLett.100.210503.

[BPPP14] J. Bouda, M. Pawłowski, M. Pivoluska, and M. Plesch. Device-independent randomness extraction from an arbitrarily weak min-entropy source. *Phys. Rev. A*, 90: 032313, 2014. DOI: 10.1103/PhysRevA.90.032313.

[BS15] M. Bavarian and P. W. Shor. Information causality, Szemerédi-Trotter and algebraic variants of CHSH. *Proc. Conference on Innovations in Theoretical Computer Science*, 2015. DOI: 10.1145/2688073.2688112.

[CBLC16] S.-L. Chen, C. Budroni, Y.-C. Liang, and Y.-N. Chen. Natural framework for device-independent quantification of quantum steerability, measurement incompatibility, and self-testing. *Phys. Rev. Lett.*, 116: 240401, 2016. DOI: 10.1103/PhysRevLett.116.240401.

[CGL+02] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88: 040404, 2002. DOI: 10.1103/PhysRevLett.88.040404.

[CGS17] A. Coladangelo, K. T. Goh, and V. Scarani. All pure bipartite entangled states can be self-tested. *Nat. Commun.*, 8: 15485, 2017. DOI: 10.1038/ncomms15485.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23: 880, 1969. DOI: 10.1103/PhysRevLett.23.880.

[CK11] R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *J. Phys. A: Math. Theor.*, 44: 095305, 2011. DOI: 10.1088/1751-8113/44/9/095305.

[Col06] R. Colbeck. *Quantum and relativistic protocols for secure multi-party computation.* PhD thesis, University of Cambridge, 2006.

[Col18] A. Coladangelo. Generalization of the Clauser-Horne-Shimony-Holt inequality self-testing maximally entangled states of any local dimension. *Phys. Rev. A*, 98: 052115, 2018. DOI: 10.1103/PhysRevA.98.052115.

[CS16] D. Cavalcanti and P. Skrzypczyk. Quantitative relations between measurement incompatibility, quantum steering, and nonlocality. *Phys. Rev. A*, 93: 052112, 2016. DOI: 10.1103/PhysRevA.93.052112.

[CS17] A. Coladangelo and J. Stark. Robust self-testing for linear constraint system games. 2017.

[CS18] A. Coladangelo and J. Stark. Unconditional separation of finite and infinite-dimensional quantum correlations. 2018.

[DPP17] K. Dykema, V. I. Paulsen, and J. Prakash. Non-closure of the set of quantum correlations via graphs. 2017.

[dV15] J. I. de Vicente. Simple conditions constraining the set of quantum correlations. *Phys. Rev. A*, 92: 032103, 2015. DOI: 10.1103/PhysRevA.92.032103.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47: 777, 1935. DOI: 10.1103/PhysRev.47.777.

[GKW+18] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani. Geometry of the set of quantum correlations. *Phys. Rev. A*, 97: 022104, 2018. DOI: 10.1103/PhysRevA.97.022104.

[JLL+08] S.-W. Ji, J. Lee, J. Lim, K. Nagata, and H.-W. Lee. Multisetting Bell inequality for qudits. *Phys. Rev. A*, 78: 052103, 2008. DOI: 10.1103/PhysRevA.78.052103.

[Kan17] J. Kaniewski. Self-testing of binary observables based on commutation. *Phys. Rev. A*, 95: 062323, 2017. DOI: 10.1103/PhysRevA.95.062323.

[KW16] J. Kaniewski and S. Wehner. Device-independent two-party cryptography secure against sequential attacks. *New J. Phys.*, 18: 055004, 2016. DOI: 10.1088/1367-2630/18/5/055004.

[LLD09] Y.-C. Liang, C.-W. Lim, and D.-L. Deng. Reexamination of a multisetting Bell inequality for qudits. *Phys. Rev. A*, 80: 052116, 2009. DOI: 10.1103/PhysRevA.80.052116.

[LRY+10] J. Lim, J. Ryu, S. Yoo, C. Lee, J. Bang, and J. Lee. Genuinely high-dimensional nonlocality optimized by complementary measurements. *New J. Phys.*, 12: 103012, 2010. DOI: 10.1088/1367-2630/12/10/103012.

[MBL+13] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne. Device-independent entanglement quantification and related applications. *Phys. Rev. Lett.*,

111: 030501, 2013.
DOI: 10.1103/PhysRevLett.111.030501.

[McK14] M. McKague. Self-testing graph states. *Theory of Quantum Computation, Communication, and Cryptography. TQC 2011. Lecture Notes in Computer Science*, 6745: 104, 2014.
DOI: 10.1007/978-3-642-54429-3_7.

[MM11] M. McKague and M. Mosca. Generalized self-testing and the security of the 6-state protocol. *Theory of Quantum Computation, Communication, and Cryptography. TQC 2010. Lecture Notes in Computer Science*, 6519: 113, 2011.
DOI: 10.1007/978-3-642-18073-6_10.

[MS16] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM*, 63: 33, 2016.
DOI: 10.1145/2885493.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. *Proceedings 39th Annual Symposium on Foundations of Computer Science*, 1998.
DOI: 10.1109/SFCS.1998.743501.

[MY04] D. Mayers and A. Yao. Self testing quantum apparatus. *Quant. Inf. Comp.*, 4: 273, 2004.

[MYS12] M. McKague, T. H. Yang, and V. Scarani. Robust self-testing of the singlet. *J. Phys. A: Math. Theor.*, 45: 455304, 2012.
DOI: 10.1088/1751-8113/45/45/455304.

[PAM+10] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464: 1021, 2010.
DOI: 10.1038/nature09008.

[PR92] S. Popescu and D. Rohrlich. Which states violate Bell's inequality maximally? *Phys. Lett. A*, 169: 411, 1992.
DOI: 10.1016/0375-9601(92)90819-8.

[PR94] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Found. Phys.*, 24: 379, 1994.
DOI: 10.1007/BF02058098.

[RMW16] J. Ribeiro, G. Murta, and S. Wehner. Fully general device-independence for two-party cryptography and position verification. 2016.

[RMW18] J. Ribeiro, G. Murta, and S. Wehner. Fully device-independent conference key agreement. *Phys. Rev. A*, 97: 022307, 2018.
DOI: 10.1103/PhysRevA.97.022307.

[RTK+18] J. Ribeiro, L. P. Thinh, J. Kaniewski, J. Helsen, and S. Wehner. Device independence for two-party cryptography and position verification with memoryless devices. *Phys. Rev. A*, 97: 062307, 2018.
DOI: 10.1103/PhysRevA.97.062307.

[RUV13] B. W. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496: 456, 2013.
DOI: 10.1038/nature12035.

[ŠASA16] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín. Self-testing protocols based on the chained Bell inequalities. *New J. Phys.*, 18: 035013, 2016.
DOI: 10.1088/1367-2630/18/3/035013.

[SAT+17] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.*, 119: 040402, 2017.
DOI: 10.1103/PhysRevLett.119.040402.

[SCA+11] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully distrustful quantum bit commitment and coin flipping. *Phys. Rev. Lett.*, 106: 220501, 2011.
DOI: 10.1103/PhysRevLett.106.220501.

[ŠCAA18] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín. Self-testing multipartite entangled states through projections onto two systems. *New J. Phys.*, 20: 083041, 2018.
DOI: 10.1088/1367-2630/aad89b.

[SLK06] W. Son, J. Lee, and M. S. Kim. Generic Bell inequalities for multipartite arbitrary dimensional systems. *Phys. Rev. Lett.*, 96: 060406, 2006.
DOI: 10.1103/PhysRevLett.96.060406.

[Slo17] W. Slofstra. The set of quantum correlations is not closed. 2017.

[SW87] S. J. Summers and R. F. Werner. Maximal violation of Bell's inequalities is generic in quantum field theory. *Commun. Math. Phys.*, 110: 247, 1987.
DOI: 10.1007/BF01207366.

[Tsi87] B. S. Tsirelson. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *J. Soviet Math.*, 36: 557, 1987.
DOI: 10.1007/BF01663472.

[Tsi93] B. S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic J. Suppl.*, 8: 329, 1993.

[VV12] U. Vazirani and T. Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. *Proceedings 44th Annual ACM Symposium on Theory of Computing*, 2012.
DOI: 10.1145/2213977.2213984.

[VV14] U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113: 140501, 2014. DOI: 10.1103/PhysRevLett.113.140501.

[WWS16] Y. Wang, X. Wu, and V. Scarani. All the self-testings of the singlet for two binary measurements. *New J. Phys.*, 18: 025021, 2016. DOI: 10.1088/1367-2630/18/2/025021.

[YN13] T. H. Yang and M. Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A*, 87: 050102(R), 2013. DOI: 10.1103/PhysRevA.87.050102.