Bell inequalities for maximally entangled states : Supplemental Material

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, The 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, Pg. Lluis Companys 23, 08010 Barcelona, Spain*
[6] *Laboratoire d'Information Quantique, CP 224, Université libre de Bruxelles (ULB), 1050 Bruxelles, Belgium*

In this Supplemental Material, we provide a detailed derivation of the coefficients of our class of Bell inequalities, detailed proofs of the Theorems from the main text, and a study of the bounds of our Bell expressions and their scaling. We also discuss how the Bell expressions can be used in device-independent quantum key distribution, and the link between our results and the structure of the set of quantum correlations.

OPTIMAL CGLMP MEASUREMENTS

We present here the "optimal CGLMP measurements" first introduced in [1] and generalized to an arbitrary number of inputs in [2], as we use them throughout our work. They are defined as follows

$$A_x = U_x^\dagger F \Omega F^\dagger U_x, \qquad B_y = V_y F^\dagger \Omega F V_y^\dagger, \tag{S.1}$$

where $\Omega = \mathrm{diag}[1, \omega, \omega^2, \dots, \omega^{d-1}]$, with $\omega = \exp(2\pi i/d)$, and F is the $d \times d$ discrete Fourier transform matrix given by

$$F_d = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{ij} |i\rangle\langle j|. \tag{S.2}$$

Then, U_x and V_x are unitary operations defining Alice's and Bob's measurements and read explicitly

$$U_x = \sum_{j=0}^{d-1} \omega^{j\theta_x} |j\rangle\langle j|, \qquad V_y = \sum_{j=0}^{d-1} \omega^{j\zeta_y} |j\rangle\langle j| \tag{S.3}$$

with the phases $\theta_x = (x - 1/2)/m$ and $\zeta_y = y/m$ for $x, y = 1, \dots, m$.

When applying these measurements on a normalised state of the form $|\psi\rangle = \sum_{q=0}^{d-1} \gamma_q |qq\rangle$, we obtain the probabilities

$$P(A_x = a, B_y = b) = \left| \frac{1}{d} \sum_{q=0}^{d-1} \gamma_q \exp\left(\frac{2\pi i}{d} q(a - b - \theta_x + \zeta_y) \right) \right|^2. \tag{S.4}$$

One can observe that this depends only on the difference $k = a - b$ and not on a and b separately. This means that:

$$P(A_x = B_y + k) = dP(A_x = k, B_y = 0). \tag{S.5}$$

Thus, all the terms $P(A_x = B_y + k)$ computed for those measurements and state have identical subterms $P(A_x = b + k, B_y = b)$. Moreover, using the values of the phases θ_x and ζ_y, one can verify straightforwardly that expression (S.4) has the same value if $x = y$ and $a - b = k$, and if $x = y + 1$ and $a - b = -k$. Thus :

$$P(A_i = B_i + k) = P(B_i = A_{i+1} + k), \tag{S.6}$$

for $i = 1, \dots, m$. Note that if one wishes to write $A_{m+1} = A_1$, the symmetry is not valid anymore and requires the definition $A_{m+1} = A_1 + 1$, which we adopt. To sum up, all the $\mathbb{P}_k$ and $\mathbb{Q}_k$ from our class of inequalities have identical subterms for those state and optimal CGLMP measurements (in particular the state can be the maximally entangled state). These symmetries justify the form of our Bell expressions: terms who have the same value appear with the same coefficient α_k or β_k, thus forming "blocks". Different blocks have different values and are multiplied by different coefficients.

DERIVATION OF COEFFICIENTS α_k AND β_k

We present the details on the derivation of coefficients α_k and β_k whose value is stated in the main text. The departure point of the determination of α_k and β_k is the set of matrix conditions

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

with $i = 1, \ldots, m$, and $l = 1, \ldots, \lfloor d/2 \rfloor$. This number $\lfloor d/2 \rfloor$ of equations stems from the fact that

$$A_x^{d-l} = (A_x^l)^\dagger, \tag{S.8}$$

$$\bar{B}_y^{d-l} = (\bar{B}_y^l)^\dagger. \tag{S.9}$$

Recall that the barred quantities $\bar{B}_i^l$ are defined as

$$\bar{B}_i^l = a_l B_i^{d-l} + a_l^* B_{i-1}^{d-l} \tag{S.10}$$

for $i = 2, \ldots, m$ and $\bar{B}_1^l = a_l B_1^{d-l} + a_l^* \omega^l B_m^{d-l}$, and the numbers a_l are given by

$$a_l = \sum_{k=0}^{\lfloor d/2 \rfloor - 1} \left[\alpha_k \omega^{-kl} - \beta_k \omega^{(k+1)l} \right]. \tag{S.11}$$

Notice that $a_l = a_{d-l}^*$. Let us notice in passing that the properties (S.8) and (S.9) imply that the Bell expression we consider, i.e.,

$$\widetilde{I}_{d,m} = \sum_{i=1}^{m} \sum_{l=1}^{d-1} \langle A_i^l \bar{B}_i^l \rangle \tag{S.12}$$

is real. This is because the sum in (S.12) can be split into two sums: for $l = 1, \ldots, \lfloor d/2 \rfloor$ and $l = \lfloor d/2 \rfloor + 1, \ldots, d-1$ for odd d, and for $l = 1, \ldots, d/2 - 1$ and $l = d/2 + 1, \ldots, d-1$ (plus a single term corresponding to $l = d/2$ which is always real) for even d. Now, due to Eqs. (S.8) and (S.9) one realizes that all terms in the second sum are complex conjugations of those in the first sum.

In order to solve the system (S.7) one has to find explicit forms of A_x^l and B_y^l. Introducing Eqs. (S.2) and (S.3) into Eq. (S.1), one obtains

$$A_x^l = \omega^{-(d-l)\theta_x} \sum_{n=0}^{l-1} |d-l+n\rangle\langle n| + \omega^{l\theta_x} \sum_{n=l}^{d-1} |n-l\rangle\langle n| \tag{S.13}$$

and

$$B_y^l = \omega^{-(d-l)\zeta_y} \sum_{n=0}^{l-1} |n\rangle\langle d-l+n| + \omega^{l\zeta_y} \sum_{n=l}^{d-1} |n\rangle\langle n-l|. \tag{S.14}$$

Then, one combines these formulas with equations (S.10) and (S.7), and compares the matrix elements, which yields the following system of equations

$$\begin{aligned} a_l \omega^{-l\zeta_i} + a_l^* \omega^{-l\zeta_{i-1}} &= \omega^{-l\theta_i} \\ a_l \omega^{(d-l)\zeta_i} + a_l^* \omega^{(d-l)\zeta_{i-1}} &= \omega^{(d-l)\theta_i}, \end{aligned} \tag{S.15}$$

with $i = 1, \ldots, m$ and $l = 1, \ldots, \lfloor d/2 \rfloor$, where it is assumed that $\zeta_0 = 0$. Simple algebra implies finally that

$$a_l = \frac{\omega^{\frac{2l-d}{4m}}}{2\cos(\pi/2m)} \qquad (l = 1, \ldots, \lfloor d/2 \rfloor). \tag{S.16}$$

Having determined a_l, one can turn to the system (S.11). It consists of $\lfloor d/2 \rfloor$ equations containing $2\lfloor d/2 \rfloor$ variables, meaning that it cannot be uniquely solved, and, in particular, the solutions will be generally complex. To handle the latter problem we equip this system with $\lfloor d/2 \rfloor$ additional equations

$$\sum_{k=0}^{\lfloor d/2 \rfloor - 1} \left[\alpha_k \omega^{kl} - \beta_k \omega^{-(k+1)l} \right] = a_l^*. \tag{S.17}$$

for $l = 1, \ldots, \lfloor d/2 \rfloor$. Now, both systems (S.11) and (S.17) can be condensed into the following single one

$$\sum_{k=0}^{\lfloor d/2 \rfloor - 1} \left[\alpha_k \omega^{-kl} - \beta_k \omega^{(k+1)l} \right] = c_l, \tag{S.18}$$

in which $c_l = a_l$ for $l = 1, \ldots, \lfloor d/2 \rfloor$ and $c_l = c_{-l}^*$ for $l = -\lfloor d/2 \rfloor, \ldots, -1$. In what follows we solve (S.17) for even and odd d separately.

Odd d. We begin by noting that in this case, the system (S.18) consists of $d-1$ equations and involves the same number of variables, and therefore one expects it to have a unique solution. To find it, we denote the set $I := \{-(d-1)/2, \ldots, -1, 1, \ldots, (d-1)/2\}$ and note that for any pair $k, n \in \{0, \ldots, \lfloor d/2 \rfloor - 1\}$, the following identity holds:

$$\sum_{l \in I} \omega^{-lk} \omega^{ln} = \sum_{l \in I \cup \{0\}} \omega^{-lk} \omega^{ln} - 1 = d\delta_{n,k} - 1. \tag{S.19}$$

We then multiply (S.18) by ω^{nl} for some $n \in \{0, \ldots, \lfloor d/2 \rfloor - 1\}$ and add the resulting equations over $l \in I$, which by virtue of Eq. (S.19) gives

$$\alpha_n = \frac{1}{d} S + \frac{1}{d} \sum_{l \in I} c_l \omega^{nl} \qquad (n = 0, \ldots, \lfloor d/2 \rfloor - 1), \tag{S.20}$$

where we have denoted

$$S = \sum_{k=0}^{\lfloor d/2 \rfloor - 1} (\alpha_k - \beta_k). \tag{S.21}$$

The coefficients β_n can be determined in an analogous way and we obtain:

$$\beta_n = -\frac{1}{d} S - \frac{1}{d} \sum_{l \in I} c_l \omega^{-(n+1)l} \qquad (n = 0, \ldots, \lfloor d/2 \rfloor - 1). \tag{S.22}$$

To fully determine α_n and β_n, it is in fact enough to compute the sum in Eq. (S.20) as the second one and S can be obtained from it by replacing n by $-(n+1)$ and $\lfloor d/2 \rfloor$, respectively. To compute this sum, we first express it as

$$\begin{aligned} \sum_{l \in I} c_l \omega^{nl} &= \frac{1}{\cos(\pi/2m)} \sum_{l=1}^{\lfloor d/2 \rfloor} \mathrm{Re} \left(\omega^{(2l-d)/4m} \omega^{nl} \right) \\ &= \frac{1}{\cos(\pi/2m)} \left[\cos\left(\frac{\pi}{2m}\right) \sum_{l=1}^{\lfloor d/2 \rfloor} \cos\left(\frac{2\pi l}{d}\xi\right) + \sin\left(\frac{\pi}{2m}\right) \sum_{l=1}^{\lfloor d/2 \rfloor} \sin\left(\frac{2\pi l}{d}\xi\right) \right] \end{aligned} \tag{S.23}$$

where we have denoted $\xi = n + 1/2m$. Using the Euler representations of the cosine and sine functions the above two sums can be easily computed and they read

$$\sum_{l=1}^{\lfloor d/2 \rfloor} \cos\left(\frac{2\pi l}{d}\xi\right) = \frac{1}{2} \left[\frac{\sin(\pi\xi)}{\sin(\pi\xi/d)} - 1 \right] \tag{S.24}$$

and

$$\sum_{l=1}^{\lfloor d/2 \rfloor} \sin\left(\frac{2\pi l}{d}\xi\right) = \frac{1}{2} \left[\cot\left(\frac{\pi\xi}{d}\right) - \frac{\cos(\pi\xi)}{\sin(\pi\xi/d)} \right]. \tag{S.25}$$

Introducing them into Eq. (S.23) and with the aid of some trigonometric formulas, one obtains

$$\begin{aligned} \sum_{l \in I} c_l \omega^{nl} &= \frac{1}{2} \left\{ \frac{\sin(\pi\xi)}{\sin(\pi\xi/d)} - 1 + \tan\left(\frac{\pi}{2m}\right) \left[\cot\left(\frac{\pi\xi}{d}\right) - \frac{\cos(\pi\xi)}{\sin(\pi\xi/d)} \right] \right\} \\ &= \frac{1}{2} \left\{ \tan\left(\frac{\pi}{2m}\right) \cot\left[\frac{\pi}{d}\left(n + \frac{1}{2m}\right)\right] - 1 \right\}. \end{aligned} \tag{S.26}$$

By replacing n with $-(n+1)$ in the above formula we then arrive at the expression for the sum in Eq. (S.22), that is,

$$\sum_{l\in I} c_l\omega^{-(n+1)l} = -\frac{1}{2}\left\{\tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(n+1-\frac{1}{2m}\right)\right]+1\right\}. \tag{S.27}$$

Finally, setting $n=\lfloor d/2\rfloor=(d-1)/2$ in Eq. (S.26) one obtains a formula for S:

$$S=\frac{1}{2}\left\{1-\tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(\left\lfloor\frac{d}{2}\right\rfloor+\frac{1}{m}\right)\right]\right\}. \tag{S.28}$$

Substituting Eqs. (S.26), (S.27), and (S.28) into Eqs. (S.20) and (S.22), we eventually obtain the coefficients α_n and β_n in the following form

$$\alpha_n=\frac{1}{2d}\tan\left(\frac{\pi}{2m}\right)\left\{\cot\left[\frac{\pi}{d}\left(n+\frac{1}{2m}\right)\right]-\cot\left[\frac{\pi}{d}\left(\left\lfloor\frac{d}{2}\right\rfloor+\frac{1}{2m}\right)\right]\right\} \tag{S.29}$$

and

$$\beta_n=\frac{1}{2d}\tan\left(\frac{\pi}{2m}\right)\left\{\cot\left[\frac{\pi}{d}\left(n+1-\frac{1}{2m}\right)\right]+\cot\left[\frac{\pi}{d}\left(\left\lfloor\frac{d}{2}\right\rfloor+\frac{1}{2m}\right)\right]\right\}. \tag{S.30}$$

with $n=1,\ldots,\lfloor d/2\rfloor$. As in the main text, the coefficients can be expressed using the function $g(x):=\cot(\frac{\pi}{d}(x+\frac{1}{2m}))$.

Even d. Clearly, in the case of even d, one can solve the system (S.18) analogously. The difference is, however, that (S.18) is the same equation for $l=-d/2$ and $l=d/2$, and therefore the system consists of $d-1$ equations for d variables. A non-unique solution is then expected.

Denoting $I_e=\{-(d-1)/2,\ldots,-1,1,\ldots,d/2\}$ and following the same methodology as above with the set I replaced by I_e one arrives at α_n and β_n given by

$$\alpha_n=\frac{1}{2d}\left\{\tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(n+\frac{1}{2m}\right)\right]-1\right\}+\frac{1}{d}S \tag{S.31}$$

and

$$\beta_n=\frac{1}{2d}\left\{\tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(n+1-\frac{1}{2m}\right)\right]+1\right\}-\frac{1}{d}S, \tag{S.32}$$

where S is given by the same formula as in Eq. (S.21). Here, the quantity S (or, equivalently, one of the variables α_n or β_n) cannot be uniquely determined. We fix it in such a way that the resulting α_n and β_n are given by the same formulas as those in the odd d case, that is,

$$S=\frac{1}{2}\left\{1-\tan\left(\frac{\pi}{2m}\right)\cot\left[\frac{\pi}{d}\left(\left\lfloor\frac{d}{2}\right\rfloor+\frac{1}{2m}\right)\right]\right\}. \tag{S.33}$$

As a consequence the coefficients α_n and β_n are given by Eqs. (S.29) and (S.30), both in the odd and even d cases.

It is finally worth mentioning that the values of the two Bell expressions—in terms of probabilities $I_{d,m}$ and in terms of generalized correlators $\widetilde{I}_{d,m}$ —are related in the following way:

$$\widetilde{I}_{d,m}=dI_{d,m}-2mS, \tag{S.34}$$

where S is given by equation (S.28).

Special cases. Let us now consider two special cases of $d=2$ and any m, and $m=2$ and any d. In the first one, the Bell expression in the probability form simplifies to

$$I_{2,m}=\alpha_0\mathbb{P}_0-\beta_0\mathbb{Q}_0 \tag{S.35}$$

where

$$\mathbb{P}_0=\sum_{i=1}^{m}[P(A_i=B_i)+P(B_i=A_{i+1})],\qquad \mathbb{Q}_0=\sum_{i=1}^{m}[P(A_i=B_i-1)+P(B_i=A_{i+1}-1)] \tag{S.36}$$

and

$$\alpha_0 = \frac{1}{2\cos(\pi/2m)}, \qquad \beta_0 = 0. \tag{S.37}$$

Moreover, there is a unique coefficient a_1 and it simplifies to $1/[2\cos(\pi/2m)]$, so that in the correlator form our Bell expression for $d = 2$ becomes

$$\widetilde{I}_{2,m} = \frac{1}{2\cos(\pi/2m)}\left[\langle A_1B_1\rangle - \langle A_1B_m\rangle + \sum_{i=2}^{m}\left(\langle A_iB_i\rangle + \langle A_iB_{i-1}\rangle\right)\right], \tag{S.38}$$

and Theorems 1, 2, and 3 from the main text give $\widetilde{C}_b = (m-1)/\cos[\pi/2m]$, $\widetilde{Q}_b = m$, and $\widetilde{NS}_b = m/\cos[\pi/2m]$, respectively. This is the well-known chained Bell inequality [3], which was recently used in Ref. [4] to self-test the maximally entangled state of two qubits and the corresponding measurements.

In the second case, i.e., that of $m = 2$ and any d, the Bell expression $I_{d,2}$ in the probability form is given by Eq.

$$I_{d,2} := \sum_{k=0}^{\lfloor d/2\rfloor-1}\left(\alpha_k\mathbb{P}_k - \beta_k\mathbb{Q}_k\right), \tag{S.39}$$

with the expressions $\mathbb{P}_k$ and $\mathbb{Q}_k$ simplifying to

$$\mathbb{P}_k = P(A_1 = B_1 + k) + P(B_1 = A_2 + k) + P(A_2 = B_2 + k) + P(B_2 = A_1 + k + 1) \tag{S.40}$$

and

$$\mathbb{Q}_k = P(A_1 = B_1 - k - 1) + P(B_1 = A_2 - k - 1) + P(A_2 = B_2 - k - 1) + P(B_2 = A_1 - k), \tag{S.41}$$

where we have exploited the convention that $A_3 = A_1 + 1$. Then, the coefficients α_k and β_k are given by

$$\alpha_k = \frac{1}{2d}\left[g(k) + (-1)^d\tan\left(\frac{\pi}{4d}\right)\right], \qquad \beta_k = \frac{1}{2d}\left[g\left(k + 1/2\right) - (-1)^d\tan\left(\frac{\pi}{4d}\right)\right], \tag{S.42}$$

with $g(k) = \cot[\pi(k + 1/4)/d]$. On the other hand, in the correlator form one obtains

$$\widetilde{I}_{d,2} = \sum_{l=1}^{d-1}\left[a_l\langle A_1^lB_1^{d-l}\rangle + a_l^*\omega^l\langle A_1^lB_2^{d-l}\rangle + a_l\langle A_2^lB_2^{d-l}\rangle + a_l^*\langle A_2^lB_1^{d-l}\rangle\right], \tag{S.43}$$

where $a_l = \omega^{(2l-d)/8}/\sqrt{2}$. In this case Theorems 1, 2, and 3 give

$$\widetilde{C}_b = \frac{1}{2}\left[3\cot\left(\frac{\pi}{3d}\right) - \cot\left(\frac{3\pi}{4d}\right)\right] - 2, \tag{S.44}$$

$\widetilde{Q}_b = 2(d-1)$, and $\widetilde{NS}_b = 2\cot[\pi/(4d)] - 2$. It should be noticed that this Bell inequality previously studied in Refs. [5] and [16], and, in particular in Refs. [16] and [7] the maximal quantum violation was found using two different methods.

CLASSICAL BOUND OF THE INEQUALITIES

We present here a detailed proof of Theorem 1 from the main text. Let us start with our Bell expression in the probability form $I_{d,m}$ and note that we can rewrite it as:

$$I_{d,m} := \sum_{k=0}^{d-1}\alpha_k\sum_{i=1}^{m}[P(A_i = B_i + k) + P(B_i = A_{i+1} + k)], \tag{S.45}$$

with $A_{m+1} = A_1 + 1$. This is possible because of the form (S.29) and (S.30) of coefficients α_k and β_k. Indeed, since $\alpha_k = -\beta_{d-k-1}$, the terms of the sum which were attached to the β_k coefficients can be shifted to indices

$k = \lfloor d/2 \rfloor, \dots, d-1$ and now associated to an α_k. In the odd case, we should in principle impose that the term $k = \lfloor d/2 \rfloor$ disappears, but it happens naturally since $\alpha_{\lfloor d/2 \rfloor} = 0$.

As stated in the main text, finding the classical bound of expression (S.45) reduces to computing the optimal deterministic strategy. Thus, to describe the difference between the outcomes associated to A_x and B_y, we can assign one value q such that $P(A_x = B_y + k) = \delta_{kq}$. As q depends on inputs x and y but not all pairs of A_x and B_y appear in the Bell expression, we thus define $2m$ variables $q_i \in \{0, 1 \dots, d-1\}$ such that:

$$\begin{aligned} A_1 - B_1 &= q_1, \\ B_1 - A_2 &= q_2, \\ A_2 - B_2 &= q_3, \\ &\vdots \\ A_m - B_m &= q_{2m-1}, \\ B_m - A_1 &= q_{2m} + 1. \end{aligned} \tag{S.46}$$

Due to the chained character of these equations, q_{2m} must obey a superselection rule involving the other q_i's, which is

$$q_{2m} = -1 - \sum_{i=1}^{2m-1} q_i, \tag{S.47}$$

where the sum is modulo d. Due to the fact that the dependence of the coefficients α_k on k is only through the cotangent function, proving Theorem 1 boils down to the following maximization problem.

Theorem 1. *Let*

$$\hat{\alpha}_k := \cot\left[\frac{\pi}{d}\left(k + \frac{1}{2m}\right)\right],$$

and let

$$\hat{C}_b := \max_{0 \le q_1, \dots, q_{2m-1} < d} \left(\sum_{i=1}^{2m-1} \hat{\alpha}_{q_i} + \hat{\alpha}_{-1-\sum_{i=1}^{2m-1} q_i \mod d} \right). \tag{S.48}$$

Then, $\hat{C}_b = (2m-1)\hat{\alpha}_0 + \hat{\alpha}_{d-1}$.

Notice that to recover the exact expression $\widetilde{C}_b$ from the main text, one needs to reintroduce the constant factors appearing in the definition of α_k and use Eq. (S.34). To prove the theorem, we first demonstrate two lemmas. Note that throughout this section, we assume that $m \geq 2$ and $d \geq 2$. Although these are not tight conditions to prove our results, they are in any case satisfied by the definition of a Bell test.

Lemma 1. *Let* $g(x) = \cot[\pi(x + \frac{1}{2m})/d]$. *For all* x, y *satisfying* $0 \le x < y < d - \frac{1}{2m}$, *we have*

$$(1 + 2mx)g(x) > (1 + 2my)g(y). \tag{S.49}$$

Proof. Let us consider the function $f(z) := z \cot z$, which is strictly decreasing in the interval $0 < z < \pi$. This can be shown for instance by noting that f is holomorphic and by studying the sign of the coefficients of its Laurent series in a ball of radius π centered at $z = 0$. Thus, for every $c \in (0, \pi)$, $f(c) > f(z)$ for all $c < z < \pi$. In particular, we can pick $c := \frac{\pi}{2dm}(1 + 2mx)$ so that:

$$\frac{\pi}{2dm}(1 + 2mx)\cot\left(\frac{\pi}{2dm}(1 + 2mx)\right) > zf(z), \tag{S.50}$$

for $\frac{\pi}{2dm}(1 + 2mx) < z < \pi$. By introducing the change of variables $z = \frac{\pi}{2dm}(1 + 2my)$, equation (S.49) follows. Note that for integer values of x and y, namely k and l, Lemma 1 becomes:

$$(1 + 2Mk)\hat{\alpha}_k > (1 + 2Ml)\hat{\alpha}_l, \qquad \forall 0 \le k < l < d. \tag{S.51}$$

□

Lemma 2. *For integer indices k, l, p such that $0 < k, l < d$ and $0 \leq p < d$, we have:*

$$\hat{\alpha}_0 + \hat{\alpha}_p > \hat{\alpha}_k + \hat{\alpha}_l. \tag{S.52}$$

Proof. Because all the alphas are ordered $\hat{\alpha}_0 > \hat{\alpha}_1 > \hat{\alpha}_2 > \cdots > \hat{\alpha}_{d-1}$, we have that $\hat{\alpha}_0 + \hat{\alpha}_p \geq \hat{\alpha}_0 + \hat{\alpha}_{d-1}$ and $\hat{\alpha}_1 + \hat{\alpha}_1 \geq \hat{\alpha}_k + \hat{\alpha}_l$. Hence, it suffices to prove that

$$\hat{\alpha}_0 + \hat{\alpha}_{d-1} > 2\hat{\alpha}_1. \tag{S.53}$$

Let us rewrite this inequality using the function g introduced in Lemma 1. To this end, we note that the symmetry of the function $\cot(x) = -\cot(-x)$ translates to $g(x)$ in the following manner : $g(x) = -g(-x - 1/m)$. Thus, in order to prove (S.53), we need to show:

$$g(0) > 2g(1) + g(1 - 1/m). \tag{S.54}$$

Using Lemma 1 twice, we can express that:

$$g(0) > (2m-1)g(1-1/m) > g(1-1/m) + 2(m-1)\frac{(1+2m)}{(2m-1)}g(1). \tag{S.55}$$

To obtain the second inequality, one of the $2m-1$ terms was isolated, and Lemma 1 was applied only on the remaining $2(m-1)$ terms. The minimum of $2(m-1)(1+2m)/(2m-1)$ is found for $m = 2$ and it is equal to $10/3$. Since $g(1)$ is positive, and $10/3 > 2$, we can conclude that $g(0) > g(1-1/m) + 2g(1)$, which is exactly relation (S.54). □

Proof of Theorem 1. To demonstrate the theorem, we employ a dynamic programming procedure which allows us to rewrite Eq. (S.48) as a chain of maximizations, each over a single variable. Let us first define

$$h(x) := \max_{0 \leq y < d} \left(\hat{\alpha}_y + \hat{\alpha}_{-1-x-y}\right), \tag{S.56}$$

where the indices are taken to be modulo d. As a direct consequence of Lemma 2, $h(x) = \hat{\alpha}_0 + \hat{\alpha}_{-1-x}$. Indeed, the lemma implies that $\hat{\alpha}_0 + \hat{\alpha}_{-1-x} > \hat{\alpha}_y + \hat{\alpha}_{-1-x-y}$ if $y > 0$ and $x \neq d-1-y$. For the cases where $y = 0$ or $x = d-1-y$, the maximum is directly attained. This allows us to write the classical bound as:

$$\hat{C}_b = \max_{q_1}\left(\hat{\alpha}_{q_1} + \max_{q_2}\left(\hat{\alpha}_{q_2} + \ldots + \max_{q_{2m-2}}\left(\hat{\alpha}_{q_{2m-2}} + h\left(\sum_{i=1}^{2m-2} q_i\right)\right)\ldots\right)\right). \tag{S.57}$$

Using the properties of h, we find that

$$\max_{q_k}\left[\hat{\alpha}_{q_k} + h\left(\sum_{i=1}^{k} q_i\right)\right] = \hat{\alpha}_0 + h\left(\sum_{i=1}^{k-1} q_i\right) \tag{S.58}$$

for all k. By applying this step $2(m-1)$ times to expression (S.57), we obtain:

$$\hat{C}_b = (2m-2)\hat{\alpha}_0 + h(0) = (2m-1)\hat{\alpha}_0 + \hat{\alpha}_{-1}. \tag{S.59}$$

□

TSIRELSON BOUND OF THE INEQUALITIES

Here, we present more details on the SOS decomposition of any Bell operator corresponding to our new Bell inequality $\widetilde{I}_{d,m}$, thus complementing the proof of Theorem 2 from the main text. Concretely, we show that the identity

$$\widetilde{Q}_b\mathbb{1} - \mathcal{B} = \frac{1}{2}\sum_{i=1}^{m}\sum_{k=1}^{d-1} P_{ik}^{\dagger}P_{ik} + \frac{1}{2}\sum_{i=1}^{m-2}\sum_{k=1}^{d-1} T_{ik}^{\dagger}T_{ik}, \tag{S.60}$$

is valid independently of the choice of A_i^k and B_i^k. The operators are thus not specified. Here, $P_{ik} = \mathbb{1}\otimes\bar{B}_i^k - (A_i^k)^\dagger\otimes\mathbb{1}$, and

$$T_{ik} = \mu_{i,k}B_2^{d-k} + \nu_{i,k}B_{i+2}^{d-k} + \tau_{i,k}B_{i+3}^{d-k}, \tag{S.61}$$

where the coefficients μ_{ik}, ν_{ik} and τ_{ik} are given by

$$\begin{aligned}
\mu_{i,k} &= \frac{\omega^{(i+1)(d-2k)/2m}}{2\cos(\pi/2m)}\frac{\sin(\pi/m)}{\sqrt{\sin(\pi i/m)\sin\left[\pi(i+1)/m\right]}},\\
\nu_{i,k} &= -\frac{\omega^{(d-2k)/2m}}{2\cos(\pi/2m)}\sqrt{\frac{\sin\left[\pi(i+1)/m\right]}{\sin(\pi i/m)}},\\
\tau_{i,k} &= \frac{1}{2\cos(\pi/2m)}\sqrt{\frac{\sin(\pi i/m)}{\sin\left[\pi(i+1)/m\right]}} = -\frac{\omega^{(d-2k)/2m}}{4\cos^2(\pi/2m)}\nu_{ik}^{-1},
\end{aligned} \tag{S.62}$$

for $i = 1,\ldots,m-3$ and $k = 1,\ldots,d-1$, while for $i = m-2$ and $k = 1,\ldots,d-1$ they are given by

$$\begin{aligned}
\mu_{m-2,k} &= -\frac{\omega^{-(d-2k)/2m}}{2\sqrt{2}\cos(\pi/2m)\sqrt{\cos(\pi/m)}},\\
\nu_{m-2,k} &= -\frac{\omega^k\omega^{(d-2k)/2m}}{2\sqrt{2}\cos(\pi/2m)\sqrt{\cos(\pi/m)}},\\
\tau_{m-2,k} &= \frac{\sqrt{\cos(\pi/m)}}{\sqrt{2}\cos(\pi/2m)}.
\end{aligned} \tag{S.63}$$

Now, in order to check the validity of the SOS decomposition (S.60) let us first introduce the explicit form of P_{ik} into the first term of the right-hand side of (S.60), which gives

$$\sum_{i=1}^{m}\sum_{k=1}^{d-1}P_{ik}^\dagger P_{ik} = \widetilde{Q}_b\mathbb{1} - 2\mathcal{B} + \mathbb{1}\otimes\sum_{i=1}^{m}\sum_{k=1}^{d-1}(\bar{B}_i^k)^\dagger(\bar{B}_i^k), \tag{S.64}$$

where we have used the fact that the Bell operator $\mathcal{B}$ is Hermitian.

Let us then introduce the explicit form of the operators T_{ik} into the last term of the right-hand side of (S.60), which, after some simple algebra, leads us to

$$\begin{aligned}
\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}T_{ik}^\dagger T_{ik} = &\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}\left(|\mu_{i,k}|^2 + |\nu_{i,k}|^2 + |\tau_{i,k}|^2\right)\mathbb{1}\\
&+\sum_{k=1}^{d-1}\left[\mu_{1,k}^*\nu_{1,k}(B_2^{d-k})^\dagger(B_3^{d-k}) + \mu_{1,k}\nu_{1,k}^*(B_3^{d-k})^\dagger(B_2^{d-k})\right]\\
&+\sum_{k=1}^{d-1}\left[\mu_{m-2,k}^*\tau_{m-2,k}(B_2^{d-k})^\dagger(B_1^{d-k}) + \mu_{m-2,k}\tau_{m-2,k}^*(B_1^{d-k})^\dagger(B_2^{d-k})\right]\\
&+\sum_{i=1}^{m-3}\sum_{k=1}^{d-1}\left[(\mu_{i,k}^*\tau_{i,k} + \mu_{i+1,k}^*\nu_{i+1,k})(B_2^{d-k})^\dagger(B_{i+3}^{d-k})\right.\\
&\qquad\qquad\left.+(\mu_{i,k}\tau_{i,k}^* + \mu_{i+1,k}\nu_{i+1,k}^*)(B_{i+3}^{d-k})^\dagger(B_2^{d-k})\right]\\
&+\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}\left[\nu_{i,k}^*\tau_{i,k}(B_{i+2}^{d-k})^\dagger(B_{i+3}^{d-k}) + \nu_{i,k}\tau_{i,k}^*(B_{i+3}^{d-k})^\dagger(B_{i+2}^{d-k})\right].
\end{aligned} \tag{S.65}$$

Now, it follows from Eqs. (S.62) and (S.63) that $\mu_{i,k}^*\tau_{i,k} + \mu_{i+1,k}^*\nu_{i+1,k} = 0$ for $i = 1,\ldots,m-3$ and $k = 1,\ldots,d-1$, which means that the fourth and fifth lines in the above vanish. Then, one notices that $\mu_{1,k}^*\nu_{1,k} = \mu_{m-2,k}\tau_{m-2,k}^* = \nu_{i,k}^*\tau_{i,k} = -a_k^2$ for $i = 1,\ldots,m-3$ and $k = 1,\ldots,d-1$, and $\nu_{m-2,k}\tau_{m-2,k}^* = -\omega^k(a_k^*)^2$ for $k = 1,\ldots,d-1$, where, as before, $a_k = \omega^{-(d-2k)/4m}/[2\cos(\pi/2m)]$. Therefore, the remaining terms on the right-hand side of Eq. (S.65) can be wrapped up as

$$\begin{aligned}\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}T_{ik}^{\dagger}T_{ik} = &\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}\left(|\mu_{ik}|^2+|\nu_{ik}|^2+|\tau_{ik}|^2\right)\mathbb{1}\\ &-\sum_{i=1}^{m-1}\sum_{k=1}^{d-1}\left[a_k^2(B_i^{d-k})^{\dagger}(B_{i+1}^{d-k})+(a_k^*)^2(B_{i+1}^{d-k})^{\dagger}(B_i^{d-k})\right]\\ &-\sum_{k=1}^{d-1}\left[\omega^k(a_k^*)^2(B_1^{d-k})^{\dagger}(B_m^{d-k})+\omega^{-k}a_k^2(B_m^{d-k})^{\dagger}(B_1^{d-k})\right].\end{aligned}\tag{S.66}$$

By substituting Eqs. (S.64) and (S.66) into Eq. (S.60) and exploiting the explicit form of the operators $\bar{B}_i^k$, one obtains

$$\begin{aligned}\frac{1}{2}\sum_{i=1}^{m}\sum_{k=1}^{d-1}P_{ik}^{\dagger}P_{ik}+\frac{1}{2}\sum_{i=1}^{m-2}\sum_{k=1}^{d-1}T_{ik}^{\dagger}T_{ik} = &\frac{1}{2}\widetilde{Q}_b\mathbb{1}-\mathcal{B}\\ &+\sum_{k=1}^{d-1}\left[m|a_k|^2+\frac{1}{2}\sum_{i=1}^{m-2}\left(|\mu_{i,k}|^2+|\nu_{i,k}|^2+|\tau_{i,k}|^2\right)\right]\mathbb{1}.\end{aligned}\tag{S.67}$$

It is easy to finally realize that the last two terms in the above formula amount to $(1/2)\widetilde{Q}_b=(1/2)m(d-1)$, which completes the proof.

NO-SIGNALLING BOUND OF THE INEQUALITIES

Here, we present details on the proof of Theorem 3 from the main text. As for the section on the classical bound of our inequalities, we start from the Bell expression written as:

$$I_{d,m}:=\sum_{k=0}^{d-1}\alpha_k\sum_{i=1}^{m}[P(A_i=B_i+k)+P(B_i=A_{i+1}+k)],\tag{S.68}$$

with $A_{m+1}=A_1+1$. Following considerations from that section, it is clear that the coefficient α_0 is the largest of the sum. Thus, the algebraic bound of $I_{d,m}$ is then $2m\alpha_0$. To complete the proof, we provide a no-signalling behaviour that reaches this bound. Let us recall the no-signalling conditions for a probability distribution:

$$\begin{aligned}\sum_b P(A_x=a,B_y=b)=\sum_b P(A_x=a,B_{y'}=b)\qquad&\forall a,x,y,y'\\ \sum_a P(A_x=a,B_y=b)=\sum_a P(A_{x'}=a,B_y=b)\qquad&\forall b,y,x,x',\end{aligned}\tag{S.69}$$

which express that the marginals on Alice's side do not depend on Bob's input, and conversely. The behaviour that we present is the following. For inputs x and y such that $x=y$ or $x=y+1$:

$$P(A_y=a,B_y=b)=P(A_{y+1}=a,B_y=b)=\begin{cases}1/d & \text{if}\quad a=b\\ 0 & \text{if}\quad a\neq b.\end{cases}\tag{S.70}$$

There is a special case for $x=1$ and $y=m$:

$$P(A_1=a,B_m=b)=\begin{cases}1/d & \text{if}\quad a=b-1\\ 0 & \text{if}\quad a\neq b-1,\end{cases}\tag{S.71}$$

where the addition is modulo d. For all the other input combinations (i.e. the ones not appearing in the inequalities), we have:

$$P(A_x=a,B_y=b)=1/d^2\qquad\forall a,b.\tag{S.72}$$

One can easily verify that this distribution satisfies conditions (S.69). To obtain the expression from Theorem 3, it suffices to write explicitly $2m\alpha_0$ and to use relation (S.34).

SCALING OF THE BOUNDS

Here, we study the asymptotic behaviour of the bounds of our Bell expressions for large numbers of inputs m and outputs d. This can be of interest when studying applications in device-independent protocols, for instance. We also show that for any values of m and d, the classical bound is strictly smaller than the quantum bound, which is strictly smaller than the no-signalling bound. This ensures in particular that the Bell inequality is never trivial.

Let us start with the quantity:

$$\frac{\widetilde{Q}_b}{\widetilde{C}_b} = \frac{2m(d-1)}{\tan\left(\frac{\pi}{2m}\right)\left[(2m-1)\cot\left(\frac{\pi}{2dm}\right) - \cot\left(\frac{\pi}{d}(1-\frac{1}{2m})\right)\right] - 2m} \tag{S.73}$$

which is the ratio between the quantum and classical bounds. We also consider the ratio between the no-signalling and quantum bounds, which is:

$$\frac{\widetilde{NS}_b}{\widetilde{Q}_b} = \frac{\tan\left(\frac{\pi}{2m}\right)\cot\left(\frac{\pi}{2dm}\right) - 1}{d-1}. \tag{S.74}$$

To observe the behaviour of these quantities for high number of inputs m and outputs d, we can use the Taylor series expansion in two variables, $1/m$ and $1/d$, and keep the dominant terms. We obtain:

$$\frac{\widetilde{Q}_b}{\widetilde{C}_b} = 1 + \frac{1}{2m} - \frac{\pi^2 - 6}{12m^2} + \cdots \tag{S.75}$$

$$\frac{\widetilde{NS}_b}{\widetilde{Q}_b} = 1 + \frac{\pi^2/12 - \pi^2/12d^2}{m^2} + \cdots \tag{S.76}$$

Thus, when the parameters m and d are of the same order and both very large, i.e. $m = \Theta(d)$, both ratios tend to 1. It is interesting to consider how fast the bounds tend towards each other: since the ratio between the no-signalling and quantum bounds lacks a term in $1/m$, it is clear that the quantum bound approaches the no-signalling bound faster than the classical bound approaches the quantum bound.

If we fix the number of outputs d and consider the limit of a large number of inputs m, the ratios still tend to 1. However, if we fix m and considers the limit of large d, both ratios tend to constants which are a bit bigger than 1. They are :

$$\lim_{d\to\infty} \widetilde{Q}_b/\widetilde{C}_b = \frac{(2m-1)\,\pi\cot\left(\pi/2m\right)}{4m(m-1)} \tag{S.77}$$

$$\lim_{d\to\infty} \widetilde{NS}_b/\widetilde{Q}_b = \frac{2}{\pi} m \tan\left(\frac{\pi}{2m}\right). \tag{S.78}$$

It is worth mentioning that both functions of m appearing on the right-hand sides of the above formulas attain their maxima for $m = 2$ which are $4/\pi$ and $3\pi/8$, respectively. To give the reader more insight, we present in Tables I and II the numerical values of these ratios for low values of m and d.

Now, let us show that these ratios are strictly larger than 1 for any value of m and d consistent with a Bell scenario.

Lemma 3. *For any $m, d \geq 2$, the quantum bound of $\widetilde{I}_{d,m}$ is strictly larger than the classical one, that is,*

$$\widetilde{Q}_b/\widetilde{C}_b > 1. \tag{S.79}$$

Proof. We prove that $\widetilde{Q}_b - \widetilde{C}_b > 0$, which is equivalent to (S.79) since both bounds are larger than 0. This inequality can be written as:

$$2md\cot\left(\frac{\pi}{2m}\right) - 2m\cot\left(\frac{\pi}{2dm}\right) + \cot\left(\frac{\pi}{2dm}\right) + \cot\left(\frac{\pi}{d}\left(1 - \frac{1}{2m}\right)\right) > 0. \tag{S.80}$$

If we define $a = 1/d$ and $x = \pi/2m$, it becomes:

$$ax\cot(a(\pi - x)) + a(x - \pi)\cot(ax) + \pi\cot(x) > 0, \tag{S.81}$$

for $0 < a \leq 1/2$ and $0 < x \leq \pi/4$. Since the first term is positive for these intervals, it suffices to show that

$$u(a, x) := a(x - \pi)\cot(ax) + \pi\cot(x) > 0. \tag{S.82}$$

Clearly, $u(a,x) \geq \min_a(u(a,x))$. This minimum corresponds to the limit $a \to 0$, since the derivative $\partial u(a,x)/\partial a$ of $u(a,x)$ with respect to a is strictly positive on the considered intervals of a and x. Indeed, it holds that

$$\frac{\partial u(a,x)}{\partial a} = (x-\pi)\cot(ax) - \frac{ax(x-\pi)}{\sin^2(ax)}, \tag{S.83}$$

which can be rewritten as

$$\frac{\partial u(a,x)}{\partial a} = \frac{\pi - x}{2\sin^2(ax)}\left[2ax - \sin(2ax)\right]. \tag{S.84}$$

Now, due to the fact that $y > \sin y$ for $0 < y \leq \pi/8$, one has that $2ax > \sin(2ax)$ for $0 < a \leq 1/2$ and $0 < x \leq \pi/4$, and therefore the right-hand side of Eq. (S.84) is strictly positive within the above intervals.

Now, computing the limit of $u(a,x)$ when $a \to 0$, one obtains

$$\lim_{a\to 0} u(a,x) = 1 - \frac{\pi}{x} + \pi\cot(x). \tag{S.85}$$

It can be verified straightforwardly that this expression is strictly positive in the interval $0 < x \leq \pi/4$, by comparing the two functions $\pi\cot(x)$ and $\frac{\pi}{x} - 1$, and noticing that the former upper bounds the latter in the interval $0 < x \leq \pi/4$. Indeed, at $x = \pi/4$, we have that $\pi\cot(\pi/4) > 3$, and in this interval, both their derivatives are negative, with the derivative of the first function smaller than the derivative of the second one. Thus, $u(a,x) > 0$. □

Lemma 4. *For any $m, d \geq 2$, the no-signalling bound of $\tilde{I}_{d,m}$ is strictly larger than the quantum one, that is,*

$$\widetilde{NS}_b/\widetilde{Q}_b > 1. \tag{S.86}$$

Proof. Writing the inequality explicitely as in (S.74), it follows that it is enough to show that $\tan(\pi/2m)\cot(\pi/2dm) > d$. Let us prove a slightly simpler inequality:

$$\tan(\pi/2m) > d\tan(\pi/2dm). \tag{S.87}$$

To this end, we show that $\tan(ax) > a\tan(x)$ for any $0 < x \leq \pi/2a$ and any integer $a \geq 2$. We notice that for $x = 0$, $\tan(0) = a\tan(0)$, and that $[\tan(ax)]' \geq [a\tan(x)]' \geq 0$, meaning that both $\tan(ax)$ and $a\tan(x)$ are monotonically increasing functions and that the former grows faster than the latter. The inequality for the derivatives holds true because $\cos(x)$ is a monotonically decreasing function for $0 \leq x \leq \pi/2a$ which implies that $\cos(x) \geq \cos(ax)$.

To complete the proof we note that $\tan(\pi/2m) = \tan[d(\pi/2dm)]$ and using $x = \pi/2dm$ and $a = d$, one can exploit the above inequality to obtain Eq. (S.87). This finally implies Eq. (S.86). □

m d	2	3	4	5	6
2	1.414	1.299	1.232	1.189	1.159
3	1.291	1.214	1.167	1.137	1.116
4	1.252	1.186	1.146	1.120	1.102
5	1.233	1.173	1.136	1.112	1.095
6	1.222	1.165	1.130	1.107	1.091

TABLE I. Numerical values of the ratio $\widetilde{Q}_b/\widetilde{C}_b$ for low number of inputs m and outputs d. For $m = d = 2$, one recovers the well-known CHSH $\sqrt{2}$ ratio.

DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

We clarify here our claim that using the maximally entangled state in DI quantum key distribution can lead to better key generation rates, and illustrate it with a simple example. This example shows a case where our inequalities can be more useful than the CGLMP inequalities, despite their lower resistance to noise. We leave out a more general analysis of the key generation rates to a work focused on DIQKD.

d \ m	2	3	4	5	6
2	1.414	1.155	1.082	1.051	1.035
3	1.366	1.137	1.073	1.046	1.031
4	1.342	1.128	1.069	1.043	1.029
5	1.328	1.123	1.066	1.041	1.028
6	1.319	1.120	1.064	1.040	1.027

TABLE II. Numerical values of the ratio $\widetilde{NS}_b/\widetilde{Q}_b$ for low number of inputs m and outputs d. For $m = d = 2$, one recovers the well-known CHSH $\sqrt{2}$ ratio.

We consider the class of protocols studied for instance in [8]. As explained there, the first step of the protocol consists of Alice and Bob making measurements on the copies of bipartite quantum systems that are distributed to them. For a number of rounds N, their inputs are set to fixed values, $x = x^*$ and $y = y^*$, and the outcomes they obtain constitute their two versions of the raw key $\vec{a} = (a_1, a_2, \cdots, a_N)$ and $\vec{b} = (b_1, b_2, \cdots, b_N)$. For a small number of rounds, which can be taken for instance as $N_{\text{est}} = \sqrt{N}$, the inputs are chosen uniformly at random, and the outputs are used to estimate the degree of nonlocality of their correlations, for instance through the violation of a Bell inequality. Note that the type of the rounds is not predetermined, so that an eavesdropper cannot know if a given round will be a key generation round or a Bell inequality violation round. The next steps of the protocol are classical, with an error-correcting stage, where Alice publishes a message about $\vec{a}$ which is used by Bob to correct his errors so that they possess the same secret key at the end.

As stated in [8], the length of this secret key is lower bounded by $H_{\min}(\vec{a}|E) - N_{\text{pub}}$, i.e. the min-entropy of Alice's raw key $\vec{a}$ conditioned on an eavesdropper's information, minus the length of the message published by Alice in the error-correcting step. The idea behind our claim is that if Alice and Bob have perfect correlations, the term N_{pub} amounts to 0 and leads to a longer secret key. For simplicity, we work in an ideal case (no finite size corrections) and the quantity we study is the asymptotic key generation rate K, which can be lower bounded by

$$K \geq H_{\min}(A_{x^*}|E) - H(A_{x^*}|B_{y^*}). \tag{S.88}$$

The first term corresponds to the guessing probability since $H_{\min}(A_{x^*}|E) = -\log_d P_{\text{guess}}(a|x^*)$ and can be bounded numerically using the Navascués-Pironio-Acín (NPA) hierarchy [9], based on the violation of a Bell inequality. The second term is the conditional Shannon entropy defined as $H(A_{x^*}|B_{y^*}) = \sum_{a,b} -P(ab|x^*y^*)\log_d P(a|bx^*y^*)$. Thus, the more the outcomes of Alice and Bob are correlated for the settings x^* and y^*, the smaller this second term is.

Let us consider an example, for the simple scenario of $m = 2$ and $d = 3$. Alice and Bob test the violation of a Bell inequality (CGLMP or ours, $I_{3,2}$) to certify the security of their outcomes. The guessing probability in both cases is found to be equal to 1/3 at the maximal violation. To generate the key, Alice uses her first setting A_1 and Bob a third measurement B_3 which is chosen to be the same as A_1 (defined in expression (S.1)). For our inequality, in the optimal case, this leads to $H(A_1|B_3) = 0$, since the state is the maximally entangled state and the correlations are thus perfect. For CGLMP, $H(A_1|B_3) = 0.0618$ since the optimal state is $|\psi_\gamma\rangle = \frac{|00\rangle+\gamma|11\rangle+|22\rangle}{\sqrt{2+\gamma^2}}$, with $\gamma = (\sqrt{11} - \sqrt{3})/2$ as found in [10, 11]. A numerical optimization on the measurement B_3 shows that the best choice to minimize $H(A_1|B_3)$ is indeed to set B_3 to be the same as A_1. Thus, in the ideal case where the maximal violation is observed, we have

$$K_{I_{3,2}} \geq 1, \tag{S.89}$$

$$K_{\text{CGLMP}} \geq 0.9382, \tag{S.90}$$

i.e. our inequality guarantees a key rate of 1 trit, while CGLMP guarantees a key rate of 0.9382 trits.

Let us now consider the effect of white noise on this example. The noise is described by parameter η, and affects the optimal state $|\psi\rangle$ as:

$$\rho' = (1-\eta)|\psi\rangle\langle\psi| + \eta\frac{\mathbb{I}}{d^2}, \tag{S.91}$$

which leads to a non-maximal violation of the Bell inequality. The results are shown in Figure 1, which also appears in the main text. Up until a noise level of $\eta \approx 0.0428$, i.e. 4.3 percent, our inequality leads to a higher key rate than CGLMP. Around $\eta \approx 0.102$, the key rate has fallen to 0 for both inequalities.

Note that our bounds on the guessing probability were obtained numerically, thus this method is limited to simple scenarios. Proving such bounds analytically remains an open question, both for CGLMP and for our inequalities. Nevertheless, we can make some conjectures about the general case.

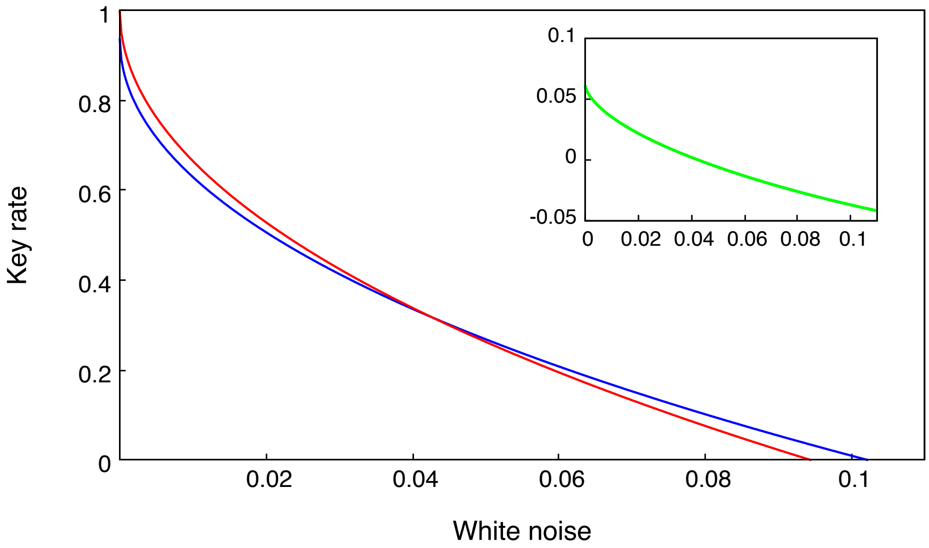

FIG. 1. Asymptotic key rate K as a function of the white noise η. The red curve corresponds to the key rate certified with our inequality $I_{3,2}$, while the blue curve corresponds to key rate with CGLMP. On the top right, the difference between the two key rates is plotted as a function of the white noise η.

In particular, when the maximal violation is observed without any noise, we expect that the eavesdropper does not possess any information, i.e. $H_{\min}(A_{x^*}|E) = 1$. This conjecture allows us to connect the key rate to the quantum mutual information $I(A:B)$:

$$K^{\eta=0} \geq H_{\min}(A_{x^*}|E) - H(A_{x^*}|B_{y^*}) = H(A_{x^*}) - H(A_{x^*}|B_{y^*}) \equiv I(A_{x^*} : B_{y^*}). \tag{S.92}$$

One can easily compute the mutual information for the case when projective measurements are applied on a bipartite pure state $|\psi_{AB}\rangle$. It is straightforward to see that the mutual information is upper bounded by the entanglement entropy of the state, $I(A:B) \leq E(|\psi_{AB}\rangle)$. For a state $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, the entropy of entanglement [12] is defined as

$$E(|\psi_{AB}\rangle) = -\mathrm{Tr}(\rho_A \log \rho_A) = -\mathrm{Tr}(\rho_B \log \rho_B), \tag{S.93}$$

with the reduced density matrices $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B = \mathrm{Tr}_A(\rho_{AB})$ (here we use logarithm to base d). The bound is tight, i.e. $I(A:B) = E(|\psi_{AB}\rangle)$, when the measurements are performed in the Schmidt basis of the state, which corresponds to the best possible choice of measurements x^*, y^* to generate a secret key, given that state. Note that implementing these Schmidt basis measurements in the protocol may not be possible, depending on the Bell inequality used and its own optimal measurements.

In [13], the authors investigated numerically the states that maximally violate the CGLMP inequalities, and they found that their entanglement entropy decreases as a function of d. On the other hand, the entanglement entropy of the maximally entangled state is equal to 1 and independent of the dimension. Since this quantity upper bounds the mutual information, these results indicate that the key rate for $\eta = 0$ would decrease monotonically with d for the CGLMP states, while our key rate would remain equal to 1. In conclusion, we can conjecture in the noiseless case that the advantage of our inequality over CGLMP grows with the dimension of the systems used for DIQKD.

STRUCTURE OF THE SET OF QUANTUM CORRELATIONS

We discuss in this section an aspect of our results that is linked to the fundamental question of the study of the set of quantum correlations. In particular, our results allow us to gain insight into the structure of the boundary of this set. Indeed, a feature of our inequalities worth highlighting is that their Tsirelson bound corresponds to the bound obtained using the NPA hierarchy at the first level $\mathcal{Q}_1$. This is a rare property, which has been previously observed only for XOR games (see, e.g., [14]) and follows from our SOS decomposition (see Eq. (S.60)). Indeed, the degree of an optimal SOS decomposition for a Bell operator is directly linked to the level of the NPA hierarchy at which the quantum bound is obtained [15]. An SOS of degree one, as in our case, corresponds to the first level $\mathcal{Q}_1$.

This means that the boundaries of the sets $\mathcal{Q}$ and $\mathcal{Q}_1$ intersect at the maximal violation of our inequalities. This observation along with the results of Ref. [16] seem to suggest that the boundaries of $\mathcal{Q}$ and $\mathcal{Q}_1$ intersect at points that correspond to the maximal violation of Bell inequalities attained by maximally entangled states. Notice, however, that the opposite implication is not true. That is, there exist Bell inequalities whose maximal violation by the maximally entangled state does not correspond to the intersection of $\mathcal{Q}$ and $\mathcal{Q}_1$ [17]. The above property, if proven in general, could be used to characterize $\mathcal{Q}_1$.

[1] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).
[2] J. Barrett, A. Kent, and S. Pironio, Phys. Rev. Lett. **97**, 170409 (2006).
[3] P. A. Pearle, Phys. Rev. D **2**, 1418 (1970); S. L. Braunstein and C. Caves, Ann. Phys. (N.Y.) **202**, 22 (1990).
[4] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, New J. Phys. **18**, 035013 (2016).
[5] W. Son, J. Lee, and M. S. Kim, Phys. Rev. Lett. **96**, 060406 (2006).
[6] J. de Vicente, Phys. Rev. A **92**, 032103 (2015).
[7] S.-W. Lee, Y. W. Cheong, and J. Lee, Phys. Rev. A **76**, 032108 (2007).
[8] Ll. Masanes, S. Pironio, and A. Acín, Nature Communications **2**, 238 (2011).
[9] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007); New J. Phys. **10**, 073013 (2008).
[10] A. Acín, T. Durt, N. Gisin, and J. I. Latorre, Phys. Rev. A **65**, 052325 (2002).
[11] T.H. Yang, and T. Vértesi, J-D. Bancal, V. Scarani, and M. Navascués, Phys. Rev. Lett. **113**, 040401 (2014).
[12] D. Bruss, J. Math. Phys **43**, 4237 (2002).
[13] S. Zohren, and R. Gill, Phys. Rev. Lett. **100**, 120406 (2008).
[14] S. Wehner, Phys. Rev. A **73**, 022110 (2006).
[15] S. Pironio, M. Navascués, A. Acín, SIAM J. Optim. **20**, 2157 (2010).
[16] J. de Vicente, Phys. Rev. A **92**, 032103 (2015).
[17] Y.-C. Liang, C.-W. Lee, and D.-L. Deng, Phys. Rev. A **80**, 052116 (2009).