scientific reports

Check for updates

OPEN

Certification of qubits in the prepare-and-measure scenario with large input alphabet and connections with the Grothendieck constant

Péter Diviánszky, István Márton, Erika Bene & Tamás Vértesi✉

We address the problem of testing the quantumness of two-dimensional systems in the prepare-and-measure (PM) scenario, using a large number of preparations and a large number of measurement settings, with binary outcome measurements. In this scenario, we introduce constants, which we relate to the Grothendieck constant of order 3. We associate them with the white noise resistance of the prepared qubits and to the critical detection efficiency of the measurements performed. Large-scale numerical tools are used to bound the constants. This allows us to obtain new bounds on the minimum detection efficiency that a setup with 70 preparations and 70 measurement settings can tolerate.

Quantum theory reveals interesting and counter-intuitive phenomena in even the simplest physical systems. Paradigmatic examples are Bell nonlocality[1,2] and Einstein-Podolsky-Rosen (EPR) steering[3–6]. These nonlocal phenomena appear as strong correlations between the outcomes of spatially separated measurements performed by independent observers. These correlations enable us to distinguish the classical and quantum origins of the experiments. Recently, a similar split between classical and quantum features was found in a setup closely related to quantum communication tasks, the so-called prepare-and-measure (PM) scenario[7]. This scenario can be viewed as a communication game[8] between two parties, Alice (the sender) and Bob (the receiver), where the dimension of the classical (versus quantum) system communicated from Alice to Bob is bounded from above.

The PM game is described as follows (see panel (a) of Fig. 1). Upon receiving an input $x = (1, \ldots, n)$, a preparation device (controlled by Alice) emits a physical system in a quantum state ρ_x. We assume $\rho_x \in \mathcal{L}(\mathbb{C}^d)$ for a given $d \geq 2$. In the following, however, we will focus explicitly on $d = 2$, that is, we assume that two-dimensional quantum systems (qubits) or classical systems (bits) are transmitted from Alice to Bob. The state ρ_x is passed to a measurement device which, upon receiving an input $y = (1, \ldots, m)$ performs a measurement and obtains an outcome $b = (1, \ldots, o)$. In this paper we will focus on the smallest, nontrivial case of $o = 2$, i.e., measurements with two outcomes, in which case we denote the outcomes by $b = \pm 1$.

Our goal in this scenario is to compare and quantify the performance of qubits with that of classical bits. This scenario has been discussed to some extent for a small number of preparations n and measurements m (see e.g. Refs.[7,9–14]. Note also that the emblematic protocol, the so-called quantum random access code[15] (QRAC), is a special instance of the PM game. See Ref.[8] for more references on communication protocols related to QRAC. These games have also found applications in randomness generation (see Refs.[16,17]). More recent notable generalizations of QRAC protocols have been considered in Refs.[18–21].

However, in this paper we would like to turn our attention to the case of large n and m (i.e. in the range of 70). We will see that the main bottleneck of the study is the computation of the relevant quantities associated with the classical bit case for which we develop large scale numerical tools in this paper. We first concentrate on the qubit case, and then we will elaborate on the classical bit case. In the qubit case we define $q(M)$, whereas in the classical bit case we define the quantities $S(M)$ and $L_2(M)$. These quantities in turn define the ratios $q(M)/L_2(M)$ and $(q(M) - S(M))/(L_2(M) - S(M))$, which upper-bound our new constants K_{PM} and K_{D}, respectively. These

MTA Atomki Lendület Quantum Correlations Research Group, Institute for Nuclear Research, P.O. Box 51, Debrecen H-4001, Hungary. ✉email: tvertesi@atomki.hu

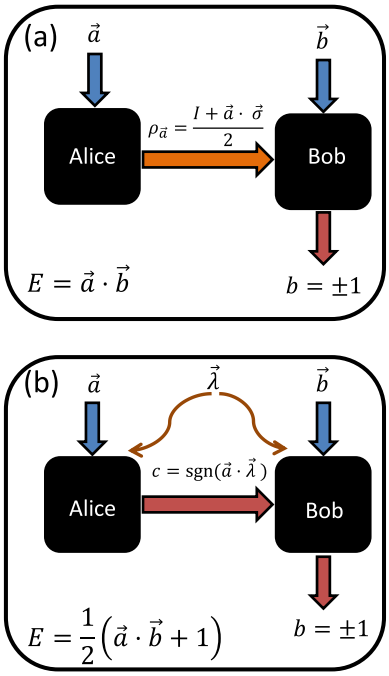

Figure 1. The prepare-and-measure setup for (**a**) qubit communication and (**b**) a classical model using one bit of communication. In (**a**) upon receiving the input settings $\vec{a}$ and $\vec{b}$, Alice sends to Bob a qubit in the quantum state $\rho_{\vec{a}}$. Then Bob performs a projective measurement $M_{b|\vec{b}} = (\mathbb{1} + b\vec{b} \cdot \sigma)/2$, where the two outcomes are labelled by $b = \pm 1$. As a result, the expectation value of Bob's ± 1 outcome becomes $E(\vec{a}, \vec{b}) = \vec{a} \cdot \vec{b}$ (see Eq. (5)). In (**b**) the classical one bit Gisin-Gisin protocol[27] is as follows. The shared randomness $\vec{\lambda}$ is distributed between the two parties, where the unit vector $\vec{\lambda} \in S^2$ is chosen uniformly at random from the sphere. After obtaining the settings $\vec{a}$ and $\vec{b}$, Alice communicates to Bob the classical binary message $c = \mathrm{sgn}(\vec{a} \cdot \vec{\lambda})$. Then Bob outputs $b = \mathrm{sgn}(c\vec{b} \cdot \vec{\lambda})$ with probability $|\vec{b} \cdot \vec{\lambda}|$, and $b = 0$ with probability $1 - |\vec{b} \cdot \vec{\lambda}|$. Finally, Bob performs a coarse graining on his outputs by grouping $b = 0$ with $b = 1$ and identifying both of them with outcome $b = 1$. As a result, as it is shown in Section "Adapting the Gisin-Gisin model to the PM scenario", the expectation value of Bob's $b = \pm 1$ outcome becomes $E(\vec{a}, \vec{b}) = (\vec{a} \cdot \vec{b} + 1)/2$.

constants have the physical meaning of defining the respective critical white noise tolerance and critical detection efficiency of the binary-outcome measurements in the qubit prepare-and-measure scenario.

In this paper, we relate these two introduced constants to the purely mathematical Grothendieck constant, K_G [22]. More generally, Grothendieck's problem has implications for many areas of mathematics. It first had a major impact on the theory of Banach spaces and then on C^*-algebras. More recently, it has influenced graph theory and computer science (see e.g. Ref.[23]). Furthermore, a connection of the Grothendieck problem to Bell nonlocality was noticed by Tsirelson[24]. Subsequently, Acin et al.[25], based on the work of Tsirelson, exploited this connection to show that the critical visibility of the Bell nonlocal two-qubit Werner state is given by $1/K_G(3)$, where $K_G(3)$ is a refined version of Grothendieck's constant[26]. Relating the local bound of correlation Bell scenarios to the classical bit bound of PM communication scenarios, we find in this paper that the new constant K_{PM} is equal to $K_G(3)$. We also introduce the constant K_{D}, which we relate to the critical detection efficiency η_{crit} of binary-outcome measurements in the qubit PM scenario. In particular, we find in our model for finite detection efficiency that $\eta_{\mathrm{crit}} = 1/K_{\mathrm{D}}$. Armed with our efficient numerical tools, we bound the constant K_{D} from below, which implies an upper bound of 0.6377 on η_{crit}.

Qubit case: In the qubit binary outcome ($o = 2$) case, the measurement is described by two positive operators $\{\Pi_{b|y}\}$, $b = \pm 1$ acting on $\mathbb{C}^2$ which sum to the identity $\Pi_{b=+1|y} + \Pi_{b=-1|y} = \mathbb{1}$ for each y, where $\mathbb{1}$ denotes the 2×2 identity matrix. The statistics of the experiment are then given by the formula

$$P(b|x, y) = \mathrm{Tr}(\rho_x \Pi_{b|y}). \tag{1}$$

It is important to note that both the preparations and the measurements are unknown to the observer, up to the fact that the dimension of the transmitted system is two. Since we have binary outcomes $b = \{+1, -1\}$ it becomes convenient to use expectation values

$$E_{x,y} = P(b = +1|x, y) - P(b = -1|x, y). \tag{2}$$

Note that $E_{x,y}$ can take up the values in $[-1,+1]$ for all x, y. However, if the Hilbert space dimension of the communicated particle is bounded, then in general not all expectation values $E_{x,y}$ in $[-1,+1]$ become possible. The simplest scenario that shows this effect appears already for $n = 3$, $m = 2$ and $o = 2$ (see Ref.[7] for an example).

With respect to the measurement operators $M_{b|y}$, one case, namely the set of projective rank-1 measurements, is of particular interest to us. In this case, we have

$$\Pi_{b|y} = \frac{\mathbb{1}_2 + b\vec{b}_y \cdot \vec{\sigma}}{2}, \tag{3}$$

where $\vec{b}_y \in S^2$, $b = \pm 1$ and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Hermitian 2×2 Pauli matrices. On the other hand, let us set

$$\rho_x = \frac{\mathbb{1}_2 + \vec{a}_x \cdot \vec{\sigma}}{2}, \tag{4}$$

where $\vec{a}_x \in S^2$. This density matrix corresponds to a pure state with Bloch vector $\vec{a}_x$. Note that in this case, the above equations give us

$$E_{x,y} = \vec{a}_x \cdot \vec{b}_y, \tag{5}$$

where $\vec{a}_x, \vec{b}_y \in S^2$.

Limits on the set of possible distributions in dimension two can be captured by the following expression

$$W = \sum_{x=1}^{n} \sum_{y=1}^{m} M_{x,y} E_{x,y}, \tag{6}$$

where $M_{x,y}$ are coefficients of a real witness matrix M of dimension $n \times m$. Let us then define the quantity

$$Q(M) = \max \sum_{x=1}^{n} \sum_{y=1}^{m} M_{x,y} E_{x,y}, \tag{7}$$

where $E_{x,y}$ is of the form (2), and where we maximize the expression over Bob's measurements $\{M_{b|y}\}$ and the qubit state ρ_x in Eq. (1). Thus, $Q(M)$ is the value that is achievable with the most general two-dimensional quantum resources in our PM setup. We further define the quantity

$$q(M) = \max \sum_{x=1}^{n} \sum_{y=1}^{m} M_{x,y} E_{x,y}, \tag{8}$$

where $E_{x,y} = \vec{a}_x \cdot \vec{b}_y$ and we maximize over the unit vectors $\vec{a}_x$ and $\vec{b}_y$ in the three-dimensional Euclidean space. It turns out that $Q(M)$ can be obtained with pure qubit states and projective measurements[11]. However, the optimal projective measurements are in general not of rank-1, they can be of rank-0 or rank-2 as well. Indeed, there are example matrices M (even in the simple $n = m = 3$, $o = 2$ case) for which $Q(M) > q(M)$. Note that $q(M)$ corresponds to projective qubit measurements of rank 1, in which case $E_{x,y} = \vec{a}_x \cdot \vec{b}_y$ (see Eq. (5)). Yet, as we will see, the set $\{E_{x,y}\}_{x,y}$ obtained by rank-1 projective measurements is a significant subset of the set $\{E_{x,y}\}_{x,y}$ corresponding to the most general qubit measurements. The tools for computing the value $Q(M)$ can be found in Refs.[28,29].

Importantly, the value of $Q(M)$ can serve as a dimension witness in the prepare-and-measure scenario[7]. Indeed, if $W > Q(M)$ for some M (where the witness W is defined by Eq. (6)), this implies that the set of states $\{\rho_x\}_{x=1}^{n}$ transmitted to Bob must have contained at least one state $\rho_{x=x'}$ of at least three dimensions (that is qutrit).

Classical bit versus qubit case—It turns out that the witness W can also serve as a quantumness witness. To this end, let us discuss the classical bit case. That is, we want to bound the expression (6) if Alice can only prepare classical two-dimensional systems (i.e. bits). Let us denote the bound on (6) by $L_2(M)$, which corresponds to this situation. If $W > L_2(M)$, this certifies that some of the measurements performed by Bob are true (incompatible) quantum measurements acting on true qubit states[7,30]. Mathematically, the classical bit case is equivalent to the qubit case discussed above, with the restriction that all qubits are sent in the same basis, and all measurements of Bob are carried out in the very same basis. That is, if we want to maximize (6) for correlations $E_{x,y}$ arising from classical two-dimensional systems, the maximum can be attained with pure states

$$\rho_x = \frac{\mathbb{1}_2 + a_x \cdot \sigma_z}{2}, \tag{9}$$

where $a_x = \pm 1$, and observables $B_y = \Pi_{0|y} - \Pi_{1|y}$ which have the form

$$B_y = b_y^+ |0\rangle\langle 0| + b_y^- |1\rangle\langle 1|, \tag{10}$$

where σ_z is the standard Pauli matrix

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and both b_y^+, b_y^- are ± 1 variables. Inserting these values into (2) we obtain

$$E_{x,y} = \frac{(1+a_x)b_y^+ + (1-a_x)b_y^-}{2}. \tag{11}$$

Since we have binary variables $a_x = \pm 1$, they translate to $E_{x,y} = b_y^+$ if $a_x = 1$ and $E_{x,y} = b_y^-$ if $a_x = -1$. Then the classical one-bit bound $L_2(M)$ is given by

$$L_2(M) = \max \sum_{x=1}^{n} \sum_{y=1}^{m} M_{x,y} E_{x,y}, \tag{12}$$

where $E_{x,y}$ is defined by (11) and we maximize over all binary variables $a_x, b_y^+, b_y^- \in \{-1, +1\}$. In words, the expression (11) corresponds to the following deterministic protocol. Alice, depending on x, prepares a bit $a_x = \pm 1$, which she sends to Bob, who outputs $b = \pm 1$ depending on the value of a_x and the measurement setting y. That is, Bob's output is a deterministic function $b = f(a_x, y)$, where the output assumes $b = \pm 1$. We can write

$$L_2(M) = \max \left(\sum_{x:a_x=+1} \sum_{y=1}^{m} M_{xy} b_y^+ + \sum_{x:a_x=-1} \sum_{y=1}^{m} M_{xy} b_y^- \right), \tag{13}$$

where the maximum is taken over all binary a_x, b_y^+ and b_y^- variables ± 1. We can eliminate the variables b_y^+ and b_y^- from the above expression and get the following formula for $L_2(M)$:

$$L_2(M) = \max_{a_x=\pm 1} \left(\left\| \sum_{x:a_x=+1} M_x \right\|_1 + \left\| \sum_{x:a_x=-1} M_x \right\|_1 \right), \tag{14}$$

which only consists of maximization over the binary variables $a_x = \pm 1$. In the above formula, M_x denotes the xth row of the real $n \times m$ matrix M, where $\|v\|_1$ denotes the Manhattan norm of the real vector v, i.e., $\|v\|_1 = \sum_x |v_x|$. We prove several interesting properties of $L_2(M)$ in the Methods Section "Properties of the L_2 and L_k, $k>_2$ norm". In particular, L_2 is proven to be a matrix norm. Let us recall that $L_2(M)$ is a key quantity in our study, as it enables witnessing both quantumness of preparations and quantumness of measurements. Indeed, $W > L_2(M)$, where W is defined in equation (6), certifies incompatible quantum measurements acting on true qubit states. That is, not all the performed measurements and not all prepared states originate from the same basis[7]. In Section "Properties of the L_2 and L_k, $k>_2$ norm" we do not restrict our study to the properties of the L_2 norm but generalize $L_2(M)$ to $L_k(M)$ for any $k > 2$ and prove that L_k is a norm as well, moreover $L_k(M)$ is a monotonic increasing function of k. Furthermore, in Section "Programming tips for the efficient implementation of the L_2 and L_k codes" we give tips for an efficient implementation of the branch-and-bound algorithm[31] for computing the $L_k(M)$ bound for $k = 2$ and for $k > 2$ as well.

Introducing the constants K_{PM} and K_{D}: We define two quantities K_{PM} and K_{D} which are related to $L_2(M)$ and $q(M)$, and are defined as follows. Let us first introduce K_{PM}, in which case we ask for the maximum ratio between $q(M)$ and $L_2(M)$. That is, we are interested in the value

$$K_{\mathrm{PM}} = \max_M \frac{q(M)}{L_2(M)}, \tag{15}$$

where the maximization is taken over all possible real $n \times m$ matrices M, where $q(M)$ is defined by (8) and $L_2(M)$ is defined by (12).

Let us now recall the Grothendieck constant of order 3[22,25,26,32,33], which is given by

$$K_G(3) = \max_M \frac{q(M)}{L(M)}, \tag{16}$$

where the maximization is taken over real matrices M of arbitrary dimensions $n \times m$, $q(M)$ is defined by (8) and $L(M)$ is defined as follows

$$L(M) = \max \sum_{x=1}^{n} \sum_{y=1}^{m} M_{x,y} a_x b_y, \tag{17}$$

where the maximum is taken over all $a_x, b_y \in \{-1, +1\}$. The value of $K_G(3)$ in (16), according to the recent work of Designolle et al.[34], is bounded by

$$1.4367 \leq K_G(3) \leq 1.4546, \tag{18}$$

where the lower bound is an improved version of that given in Ref.[35] and the upper bound is an improved version of that given in Refs.[36,37]. See Ref.[38] for some historical data on the best lower and upper bounds for $K_G(d)$. We prove that $K_{\mathrm{PM}} = K_G(3)$, which will be given in the Results Section "Proof of the relation K_{PM}=$K_{G(3)}$". We are interested in K_{D} as well, a quantity similar to K_{PM}. We define this quantity as follows

$$K_{\mathrm{D}} = \max_{M} \frac{q(M) - S(M)}{L_2(M) - S(M)}, \tag{19}$$

where

$$S(M) = \sum_{x=1}^{n} \sum_{y=1}^{m} M_{x,y}. \tag{20}$$

Note the relation

$$\frac{q(M) - S(M)}{L_2(M) - S(M)} \geq \frac{q(M)}{L_2(M)}, \tag{21}$$

whenever $L_2(M) > S(M)$ (also note that $q(M) \geq L_2(M)$), therefore we have $K_{\mathrm{D}} \geq K_{\mathrm{PM}} = K_G(3)$. From this we immediately obtain the lower bound $K_{\mathrm{D}} \geq 1.4367$. In this paper, we give efficient large-scale numerical methods to obtain even better lower bounds on the above quantity. Namely, we prove the lower bound $K_{\mathrm{D}} \geq 1.5682$. We also prove an upper bound of 2 on this quantity, so putting all together we have the following interval

$$1.5682 \leq K_{\mathrm{D}} \leq 2, \tag{22}$$

for the constant K_{D}. It is an open problem to close or at least reduce the gap between the lower and upper limits.

We next present the Results section, which contains our main findings in three subsections.

Results

Proof of the relation $K_{\mathrm{PM}} = K_G(3)$. To prove our claim, we relate $L(M')$ to $L_2(M')$, where M' is given by the following matrix (see also (67))

$$M' = \begin{pmatrix} M \\ -M \end{pmatrix} \tag{23}$$

where M is a real $n \times m$ matrix. Denote by M_x the x-th row of the matrix M. Note that according to the above definition M' has size $2n \times m$ and M' has rows such that $M'_x = M_x$ and $M'_{x+n} = -M_x$ for all $x = 1, \ldots, n$. Then the following lemma holds.

Lemma 2.1 *$L_2(M') = L(M') = 2L(M)$ for any matrix M' of the form (23), where L_2 is the L_2 norm given by the definition (12) and L is the local bound given by (17), (40).*

The proof of this lemma is given in Methods Section "*L*-norm and L_2-norm are the same for a special family of matrices *M*' ". Then we need to prove the following lemma.

Lemma 2.2 *$K_{\mathrm{PM}} \leq K_G(3)$.*

For an arbitrary matrix M, we have $L_2(M) \geq L(M)$. This has been proved in Methods Section "Properties of the L_2 and L_k, k>2 norm". Then the lemma follows from the definitions (16) and (15). Our next lemma reads

Lemma 2.3 *$K_{\mathrm{PM}} \geq K_G(3)$.*

Proof To prove this, it suffices to show that for an arbitrary real matrix M, there exists the matrix M' defined by (23) such that $q(M') = 2q(M)$ and $L_2(M') = 2L(M)$. The first relation follows from the special structure of M'. The second relation has been shown in Lemma 2.1. Therefore, K_{PM} cannot be less than $K_G(3)$, which proves our claim. □

Corollary 2.4 *As a corollary of the above Lemmas 2.2 and 2.3 we obtain $K_{\mathrm{PM}} = K_G(3)$.*

Hence we have the same bounds $1.4367 \leq K_{\mathrm{PM}} \leq 1.4546$ as for $K_G(3)$ (see (18)). From the corollary above, we have a matrix M' of size 48×24 with $q(M')/L_2(M') > \sqrt{2}$. Indeed, the construction is based on a matrix M of size 24×24, which provides $q(M)/L(M) > \sqrt{2}$[39]. To the best of our knowledge, this is the smallest M matrix that has the property $q(M)/L(M) > \sqrt{2}$. Then the 48-by-24 matrix M' follows from (23). On the other hand, $q(M)/L(M) = \sqrt{2}$ is already attained with a 2×2 matrix M in the CHSH-form[40]:

$$M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

It remains an open question to show that $K_{\mathrm{PM}} > \sqrt{2}$ with a matrix size smaller than 48×24, which might use a different construction than the one above.

Proof of the bounds $1.5682 \leq K_{\mathrm{D}} \leq 2$. *Upper bound*: We first prove the upper bound. Translating the Gisin-Gisin model[27] from the Bell nonlocality[1,2] to the PM scenario[7], we find that the following statistics can be obtained in the PM scenario with 1 bit of classical communication:

$$E(\vec{a},\vec{b}) = \frac{\vec{a}\cdot\vec{b}+1}{2}, \tag{24}$$

where $\vec{a} \in S^2$ denotes the preparation vector and $\vec{b} \in S^2$ denotes the measurement Bloch vector. We give the proof of this formula in the Methods Section "Adapting the Gisin-Gisin model to the PM scenario" and we show panel (b) in Fig. 1 for the description of the classical one-bit model. On one hand, due to the above Gisin-Gisin one-bit model, we have for an arbitrary $n \times m$ matrix M:

$$\max \sum_{x=1}^{n}\sum_{y=1}^{m} M_{x,y}E_{x,y} \leq L_2(M), \tag{25}$$

where $E_{x,y}$ has the form (24) and we maximized over the unit vectors $\vec{a}_x$ and $\vec{b}_y$ in the three-dimensional Euclidean space. On the other hand, substituting $E_{x,y} := E(\vec{a}_x,\vec{b}_y)$ in the formula (24) into (25) we find

$$\begin{aligned}\max \sum_{x=1}^{n}\sum_{y=1}^{m} M_{x,y}E_{x,y} &= \frac{\max \sum_{xy} M_{xy}\left(\vec{a}_x\cdot\vec{b}_y+1\right)}{2}\\ &= \frac{q(M)+S(M)}{2},\end{aligned} \tag{26}$$

where maximization is over the unit vectors $\vec{a}_x$ and $\vec{b}_y$ in the three-dimensional Euclidean space, and we also used the definition of $q(M)$ in (8) and the definition of $S(M)$ in (20). Comparing the right-hand side of (25) with (26), we have

$$\frac{q(M)-S(M)}{L_2(M)-S(M)} \leq 2, \tag{27}$$

where the left-hand side of (19) is just K_{D}, which proves the upper bound $K_{\mathrm{D}} \leq 2$. □

Lower bound: In the following, we prove the lower bound using large-scale numerical tools. Note, however, that the resulting bound is rigorous and in particular the final result is due to exact computations. The steps are as follows.

Given a fixed setup with Alice's Bloch vectors $\vec{a}_x$, $x = (1,\ldots,n)$ and Bob's Bloch vectors $\vec{b}_y$, $y = (1,\ldots,m)$ the method is the following. We define the $(n \times m)$-dimensional one-parameter family of matrices $E_{xy}(\eta)$ with entries

$$E_{x,y}(\eta) = \eta E_{x,y} + (1-\eta), \tag{28}$$

where $E_{x,y} = \vec{a}_x \cdot \vec{b}_y$. We wish to show that for some $\eta \in [0,1]$, the distribution (28) in the PM scenario cannot be simulated with one bit of classical communication. In fact, due to the expectation value (24) of the Gisin-Gisin model, it is enough to consider the interval $\eta \in [1/2,1]$. To show quantumness, we therefore need to find a matrix M of certain size $n \times m$ and a given $\eta \in [1/2,1]$ such that

$$\sum_{x=1}^{n}\sum_{y=1}^{m} M_{xy}E_{xy}(\eta) > L_2(M) \tag{29}$$

for $E_{xy}(\eta)$ defined by (28), and $L_2(M)$ is defined by (12). The above problem, i.e., finding a suitable M with the smallest possible η in (29), can be solved by a modified version[39] of the original Gilbert algorithm[41], a popular collision detection method used, for example, in the video game industry.

The algorithm is iterative, and the procedure adapted to our problem is given in Section "The modified Gilbert algorithm adapted to the PM scenario". Indeed, using the algorithm of Gilbert, we find the value

$$\eta^* = 0.6377 \tag{30}$$

and a corresponding 70×70 matrix M and $E_{xy}(\eta^*)$ in the form (28) which satisfies inequality (29). We will give more technical details of the input parameters and the implementation of the algorithm in Section "Parameters and implementation of Gilbert algorithm". Then, rearranging (29) and making use of equation (28), we find the bound

$$\frac{\sum_{xy} M_{xy}E_{xy} - S(M)}{L_2(M)-S(M)} > \frac{1}{\eta^*}, \tag{31}$$

where due to the definitions (8), (19) the lower bound

$$K_{\mathrm{D}} > (1/\eta^*) \simeq 1.5682 \tag{32}$$

on K_{D} follows.

Physical meaning of the constants K_{PM} and K_{D}. *The role of K_{PM} in the PM scenario*: The value of K_{PM} is interesting from a physical point of view as well, since it is related to the critical noise resistance of the experimental setup if the transmitted ρ_x goes through a noisy, fully depolarizing channel. That is, $1-p_{\mathrm{crit}}=1-(1/K_{\mathrm{PM}})$ gives the amount $(1-p_{\mathrm{crit}})$ of critical white noise $\mathbb{1}/2$ that the PM experiment with rank-1 projective qubit measurements can maximally tolerate while still being able to detect quantumness. Namely, for a fully depolarizing channel with visibility parameter p the qubits ρ_x emitted by Alice turn into $p\rho_x+(1-p)\mathbb{1}/2$, and the expectation value (5) becomes

$$E_{xy}=p\vec{a}_x\cdot\vec{b}_y, \tag{33}$$

where $\{\vec{a}_x\}_x$ are the Bloch vectors of Alice's qubits, whereas $\{\vec{b}_y\}_y$ are the Bloch vectors of Bob's measurements. To witness quantumness, there must exist expectation values E_{xy} in (33) and a matrix M of arbitrary size such that

$$\sum_{xy}M_{xy}E_{xy}>L_2(M). \tag{34}$$

Inserting (33) into (34) and making use of (8), we obtain

$$p_{\mathrm{crit}}=\min_M\frac{L_2(M)}{q(M)}=\frac{1}{K_{\mathrm{PM}}}=\frac{1}{K_G(3)} \tag{35}$$

for the critical noise tolerance. In fact, the value of $K_G(3)$ appears in the studies[25,36,42] of the Bell nonlocality of two-qubit Werner states[43]. Note that a recent approach in Ref.[44], based on the simulability of Werner states with local models, yields the same relation (35) between p_{crit} and $1/K_G(3)$.

From the upper and lower bounds on K_{PM}, the following bounds on the amount $(1-p_{\mathrm{crit}})$ of critical white noise follow:

$$0.3039\leq(1-p_{\mathrm{crit}})\leq 0.3125. \tag{36}$$

The role of K_{D} in the PM scenario: In Section "Proof of the bounds $1.5682\leq K_{\mathrm{D}}\leq 2$" we proved the lower bound of $K_{\mathrm{D}}\geq 1.5682$. Below we prove that this bound is related to the finite detection efficiency threshold of Bob's measurements. To this end, we assume that Bob's detectors are not perfect and only fire with probability η. Assume that when the measurement y fails to detect, Bob outputs $b_y=1$ (due to possible relabelings there is no loss of generality). Assume further that the probability of detection η is the same for all y. This is the problem of symmetric detection efficiency. A review of this problem in the Bell scenario can be found in Ref.[45]. On the other hand, the same problem in the PM scenario has been elaborated in Refs.[46,47] and the upper bound of $1/\sqrt{2}$ on the critical value of the symmetric detection efficiency was found.

Since η does not depend on y, the expectation value $E_{x,y}$ becomes $E_{x,y}(\eta)=\eta E_{x,y}+(1-\eta)$ for all x and y. Hence, the witness matrix M detects quantumness with finite detection efficiency η (assuming optimal preparation states and measurements) whenever we have

$$\eta q(M)+(1-\eta)\sum_{x,y}M_{x,y}>L_2(M). \tag{37}$$

Recalling $S(M)=\sum_{x,y}M_{x,y}$, solving the above relation for η, and optimizing over all M witness matrices, we obtain the critical detection efficiency η_{crit}:

$$\eta_{\mathrm{crit}}=\min_M\frac{L_2(M)-S(M)}{q(M)-S(M)}=\frac{1}{K_{\mathrm{D}}}, \tag{38}$$

where K_{D} is defined by (19). In particular using the lower bound value $K_{\mathrm{D}}\geq 1.5682$, we obtain the improved upper bound 0.6377 on η_{crit}.

It should be noted, however, that the above is not the most general detection efficiency model. Rather than outputting $b_y=1$, Bob can output a third result, which could potentially give a lower detection efficiency threshold. An open problem is whether this third outcome can lower the detection efficiency threshold. In the above, we also assumed that Bob's qubit measurements are rank-1 projectors that can achieve $q(M)$. However, it is known that the true qubit maximum $Q(M)$ (in (7)) can be larger than $q(M)$ (in (8)) for a given M. Hence, we can say that the most general symmetric detection efficiency threshold is upper bounded by $1/K_{\mathrm{D}}$, and it is an open problem whether this upper bound is tight or not.

Let us mention that in the two-outcome scenario a different type of modelling of the loss event due to the finite detection efficiency can also be imagined. Namely, let us assume that Bob associates the outcomes $+1$ and -1 to the no-detection event with equal probability. In this case, the expectation value $E_{x,y}(\eta)=\eta E_{x,y}+(1-\eta)$ when outcome $+1$ is assigned to the no-detection event becomes $\eta E_{x,y}$. This leads to the modified inequality $\eta q(M)>L_2(M)$ in Eq. (37) and the modified critical detection efficiency, $\eta_{\mathrm{crit}}=\min_M(L_2(M)/q(M))=1/K_{\mathrm{PM}}$. Therefore, using Bob's non-deterministic assignment of the ± 1 outcomes for the no-detection event, the critical detection efficiency can be linked to $K_G(3)=K_{\mathrm{PM}}$, i.e., the Grothendieck constant of order 3. Note, however, that due to our finding that $K_G(3)<K_{\mathrm{D}}$, the critical detection efficiency in this non-deterministic modelling of the no-detection event will be suboptimal compared to the deterministic assignment model, when we associate the no-detection event with a given outcome.

Methods

Properties of the L_2 and L_k, $k > 2$ norm.

Notations: We first introduce notation used throughout this subsection. Let $A^n, n = 0, 1, 2, \ldots$ be the set of n dimensional vectors over the set A. Let v_i denote the ith element of $v \in A^n (i = 1, 2, \ldots, n)$. Let $\_;\_ : A^n \times A^m \to A^{n+m}$ denote the concatenation of vectors. Let () the singleton element of A^0. Further let $(a) \in A^1$ if $a \in A$. The parenthesis may be omitted so (1); (2); (3) = 1; 2; $3 \in \mathbb{R}^3$, for example. Let $\overline{a}^n = a; a; \ldots; a \in A^n$ where $a \in A$. We write $\overline{a}$ instead of $\overline{a}^n$ if n can be inferred from the context. We define $\mathcal{M}_{n,m}$ as the set of real $n \times m$ matrices. Matrices are represented as vectors of their row vectors, i.e. $\mathcal{M}_{n,m} = (\mathbb{R}^m)^n$. Let $M^\top \in \mathcal{M}_{m,n}$ be the transposition of $M \in \mathcal{M}_{n,m}$ and let $\mathbb{I}^m \in \mathcal{M}_{m,m}$ denote the $m \times m$ identity matrix. Further, it is convenient to define by $\mathcal{W}_{n,k} = \{\mathbb{I}^k_j \mid j = 1, 2, \ldots, k\}^n \subset \mathcal{M}_{n,k}$ the set of matrices whose rows are all 0s, but exactly one is 1. Let $\mathcal{P}_n \subset \mathcal{M}_{n,n}$ denote the set of permutation matrices. Let $\|M\|_1 = \sum_{i=1}^n \|M_i\|_1$ denote the Manhattan norm of the matrix $M \in \mathcal{M}_{n,m}$.

Definition of L_k.—We first give the definition of L_k. Let $k \in \mathbb{N}^+$.

$$\begin{aligned} &L_k : \mathcal{M}_{n,m} \to \mathbb{R} \\ &L_k(M) = \max_{W \in \mathcal{W}_{n,k}} \left\| W^\top M \right\|_1. \end{aligned} \tag{39}$$

Note that W is defined above in *Notations* and $W^\top$ denotes the transposed matrix of W. We prove below that Eq. (39) corresponds to Eq. (14) in the case of $k = 2$. The proof is as follows

$$\begin{aligned} &\max_{a_x \in \{\pm 1\}} \left(\left\| \sum_{x:a_x=+1} M_x \right\|_1 + \left\| \sum_{x:a_x=-1} M_x \right\|_1 \right) \\ &= \max_{W \in \mathcal{W}_{n,2}} \left(\left\| W_1^\top M \right\|_1 + \left\| W_2^\top M \right\|_1 \right) \\ &= \max_{W \in \mathcal{W}_{n,2}} \left\| W^\top M \right\|_1 \\ &= L_2(M). \end{aligned}$$

Properties of L_k.—We prove several interesting properties of L_k. Note that our focus in the main text is on $k = 2$. However, the general case $k \geq 2$ is of interest for its own sake. Moreover, it is also motivated physically, corresponding to classical communication beyond bits[7,48]. First we prove that L_k is a norm for any $k \geq 2$. To this end, we prove its homogeneity, positive definiteness and subadditivity properties.

Lemma 3.1 *L_k is a norm.*

Homogeneity:

$$\begin{aligned} L_k(tM) &= \max_{W \in \mathcal{W}_{n,k}} \left\| W^\top (tM) \right\|_1 \\ &= \max_{W \in \mathcal{W}_{n,k}} |t| \left\| W^\top M \right\|_1 \\ &= |t| \max_{W \in \mathcal{W}_{n,k}} \left\| W^\top M \right\|_1 \\ &= |t| L_k(M), \end{aligned}$$

where $|t|$ denotes the absolute value of the scalar t and L_k is defined by (39).

Positive definiteness:

$$\begin{aligned} L_k(M) = 0 &\\ &\Rightarrow \max_{W \in \mathcal{W}_{n,k}} \left\| W^\top M \right\|_1 = 0 \\ &\Rightarrow \forall W \in \mathcal{W}_{n,k} : \left\| W^\top M \right\|_1 = 0 \\ &\Rightarrow \forall W \in \mathcal{W}_{n,k} : W^\top M = \overline{\overline{0}} \\ &\Rightarrow \forall i : M_i = \overline{0} \\ &\Rightarrow M = \overline{\overline{0}}. \end{aligned}$$

Triangle inequality:

$$\begin{aligned} L_k(M+N) &= \max_{W\in\mathcal{W}_{n,k}} \left\| W^\top (M+N) \right\|_1 \\ &\leq \max_{W\in\mathcal{W}_{n,k}} \left(\left\| W^\top M \right\|_1 + \left\| W^\top N \right\|_1 \right) \\ &\leq \max_{W\in\mathcal{W}_{n,k}} \left\| W^\top M \right\|_1 + \max_{W\in\mathcal{W}_{n,k}} \left\| W^\top N \right\|_1 \\ &= L_k(M) + L_k(N). \end{aligned}$$

□

Let us define $L(M)$ as follows

$$L(M) = \max_{v\in\{-1,+1\}^n} \|vM\|_1. \tag{40}$$

The above definition is consistent with the one given in (17). $L(M)$ is the local or classical bound of correlation Bell inequalities[24] defined by the correlation matrix M in (40). The $L(M)$ quantity also appears in computer science literature under the name of $K_{m,n}$-quadratic programming[49]. Let us note that recently an efficient computation of $L(M)$ has been proposed in Ref.[35] along with the code[50].

First we prove the basic property that $L_2(M) \geq L(M)$ for any M. Next we prove that $L_k(M) \leq L_{k+1}(M)$ for $k \geq 2$. Then we bound $L_k(M)$ from above by the value of $L(M)$ multiplied by k. However, we do not know whether the bound can be saturated or not. The lemma stating our first claim is as follows

Lemma 3.2

$$L(M) \leq L_2(M), \tag{41}$$

where the proof is given as the following chain of equations plus a single inequality invoked in the fourth line

$$\begin{aligned} L(M) &= \max_{v\in\{-1,+1\}^n} \|vM\|_1 \\ &= \max_{v\in\{-1,+1\}^n} \left\| \frac{1}{2}(\bar{1}+v)M - \frac{1}{2}(\bar{1}-v)M \right\|_1 \\ &= \max_{W\in\mathcal{W}_{n,2}} \left\| W_1^\top M - W_2^\top M \right\|_1 \\ &\leq \max_{W\in\mathcal{W}_{n,2}} \left(\left\| W_1^\top M \right\|_1 + \left\| W_2^\top M \right\|_1 \right) \\ &= \max_{W\in\mathcal{W}_{n,2}} \left\| W^\top M \right\|_1 \\ &= L_2(M). \end{aligned}$$

□

Our next lemma proves that $L_k(M)$ is monotone increasing with k.

Lemma 3.3

$$L_k(M) \leq L_{k+1}(M). \tag{42}$$

The proof is given below as the following chain:

$$\begin{aligned} L_k(M) &= \max_{W\in\mathcal{W}_{n,k}} \left\| W^\top M \right\|_1 \\ &= \max_{W\in\mathcal{W}_{n,k}} \sum_{i=1}^{k} \left\| \left(W^\top M \right)_i \right\|_1 \\ &= \max_{W\in\mathcal{W}_{n,k}} \left(\sum_{i=1}^{k} \left\| \left(W^\top M \right)_i \right\|_1 + \left\| \bar{0} M \right\|_1 \right) \\ &= \max_{W\in\mathcal{W}_{n,k}} \sum_{i=1}^{k+1} \left\| \left(\left(W^\top ; \bar{0} \right) M \right)_i \right\|_1 \\ &= \max_{W\in\mathcal{W}_{n,k}} \left\| \left(W^\top ; \bar{0} \right) M \right\|_1 \\ &\leq \max_{W\in\mathcal{W}_{k+1,n}} \left\| W^\top M \right\|_1 \\ &= L_{k+1}(M). \end{aligned}$$

□

Finally, we prove an upper bound on $L_k(M)$. Our lemma reads as follows

Lemma 3.4

$$L_k(M) \leq kL(M) \tag{43}$$

Proof

$$\begin{aligned}
L_k(M) &= \max_{W\in\mathcal{W}_{n,k}} \left\| W^\top M \right\|_1 \\
&= \max_{W\in\mathcal{W}_{n,k}} \sum_{i=1}^{k} \left\| (W^\top M)_i \right\|_1 \\
&= \max_{W\in\mathcal{W}_{n,k}} \sum_{i=1}^{k} \left\| W_i^\top M \right\|_1 \\
&= \max_{W\in\mathcal{W}_{n,k}} \sum_{i=1}^{k} \frac{1}{2} \left\| \left(2W_i^\top - \bar{1}\right) M + \bar{1}M \right\|_1 \\
&\leq \max_{W\in\mathcal{W}_{n,k}} \sum_{i=1}^{k} \frac{1}{2} \left(\left\| (2W_i^\top - \bar{1})M \right\|_1 + \left\| \bar{1}M \right\|_1 \right) \\
&\leq \max_{W\in\mathcal{W}_{n,k}} \sum_{i=1}^{k} \frac{1}{2} (L(M) + L(M)) \\
&= \max_{W\in\mathcal{W}_{n,k}} \sum_{i=1}^{k} L(M) \\
&= \max_{W\in\mathcal{W}_{n,k}} kL(M) \\
&= kL(M).
\end{aligned}$$

To arrive at the sixth line, we invoked the definition (40). □

It is an open question whether Lemma 3.4 is tight or not. However, we can find a family of matrices $M^{(k)}$, $k \geq 2$ such that the ratio $L_k(M^{(k)})/L(M^{(k)})$ tends to infinity with increasing k. More formally we have

Lemma 3.5 *For all $\varepsilon > 0$ there exists a matrix M and $k > 1$ such that*

$$\frac{L(M)}{L_k(M)} < \varepsilon. \tag{44}$$

The proof is based on an explicit construction of matrices M^k, $k = (2, \ldots, \infty)$ defined in Ref.[51]. See also Refs.[52,53].

Proof Let $M^k \in \mathcal{M}_{k,2^{k-1}}$, $k = (1, 2, \ldots, \infty)$ be a family of matrices such that[51]

$$M^k_{i,j} = (-1)^{\left\lfloor \frac{j}{2^{k-i-1}} \right\rfloor}. \tag{45}$$

For example,

$$M^4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}. \tag{46}$$

Now by explicit calculations we find

$$\frac{L(M^k)}{L_k(M^k)} = \frac{k\binom{k-1}{\lfloor \frac{k-1}{2} \rfloor}}{k2^{k-1}} \sim \sqrt{\frac{2}{\pi k}}. \tag{47}$$

□

Note that in the particular case of $k = 2$ the matrix $M^{(k)}$ is the CHSH expression[40], in which case $L(M^{(2)}) = 2$ and $L_2(M^{(2)}) = 4$. Hence, for $k = 2$ the upper bound in Lemma 3.4 is tight. We conjecture that the bound is not tight for greater values of k.

Finally, we show how L_2 and in general L_k behaves with the concatenation $(A; B)$ of two matrices A and B, where we defined

$$(A; B) = \begin{bmatrix} A \\ B \end{bmatrix}. \tag{48}$$

Lemma 3.6 *Let $A \in \mathcal{M}_{i,m}$, $B \in \mathcal{M}_{j,m}$. Then we have*

$$L_k(A; B) \leq L_k(A) + L_k(B). \tag{49}$$

Proof

$$\begin{aligned} L_k(A; B) &= \max_{W \in \mathcal{W}_{i+j,k}} \left\| W^\top (A; B) \right\|_1 \\ &= \max_{S \in \mathcal{W}_{i,k}} \max_{T \in \mathcal{W}_{j,k}} \left\| (S; T)^\top (A; B) \right\|_1 \\ &= \max_{S \in \mathcal{W}_{i,k}} \max_{T \in \mathcal{W}_{j,k}} \left\| S^\top A + T^\top B \right\|_1 \\ &\leq \max_{S \in \mathcal{W}_{i,k}} \max_{T \in \mathcal{W}_{j,k}} \left(\left\| S^\top A \right\|_1 + \left\| T^\top B \right\|_1 \right) \\ &\leq \max_{S \in \mathcal{W}_{i,k}} \left\| S^\top A \right\|_1 + \max_{T \in \mathcal{W}_{j,k}} \left\| T^\top B \right\|_1 \\ &= L_k(A) + L_k(B). \end{aligned}$$

□

Note that $L_k(A) \leq L_k(A; B)$ does not hold in general. For example, let us have

$$A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{50}$$

and

$$B = \begin{pmatrix} -1 & 0 \end{pmatrix}. \tag{51}$$

Then by explicit calculation we obtain

$$4 = L_2(A) > L_2(A; B) = 3. \tag{52}$$

Finally, it is shown that L_k relates to the cut norm C, a matrix norm introduced by Frieze and Kannan in Ref.[54] (see also[55] for several applications in graph theory). This norm is defined as follows:

$$C(M) = \max \sum_{x=1}^{n} \sum_{y=1}^{m} M_{x,y} a_x b_y, \tag{53}$$

where the maximum is taken over all $a_x, b_y \in \{0, 1\}$. Note the similarity in the definition with the $L(M)$ norm (17) which is equivalent to (40). It has been shown that $C(M)$ is related to $L(M)$ as follows[54,56]:

$$C(M) \leq L(M) \leq 4C(M). \tag{54}$$

Using the above relation (54) along with Lemma 3.4, we find that

$$C(M) \leq L_k(M) \leq 4kC(M), \tag{55}$$

and for the special case of L_2 we have the following lower and upper bounds:

$$C(M) \leq L_2(M) \leq 8C(M). \tag{56}$$

Generalization of the L_k norm: Below we generalize the norm $L_k(M)$ to F_M, which extension will prove to be a key property in the Branch-and-Bound[31] implementation of the L_k algorithm. To do so, first we define the following function

Definition 3.7

$$F_M : \mathcal{W}_{i,k} \to \mathbb{R}$$
$$F_M(P) = \max_{W \in \mathcal{W}_{n-i,k}} \left\| (P;\, W)^\top M \right\|_1 \tag{57}$$

where $i = (0, 1, 2, \ldots, n)$ and $M \in \mathcal{M}_{n,m}$.

In other words, $F_M(P)$ is the maximum of $\left\| W^\top M \right\|_1$ where $W \in \mathcal{W}_{k,n}$ and the prefix of W is P. F_M can be considered as a generalization of $L_k(M)$. The following lemma introduces a key property which is made use of in the Branch-and-Bound method.

Lemma 3.8

$$F_{A;B}(P) \leq \left\| P^\top M \right\|_1 + L_k(B) \tag{58}$$

Proof

$$\begin{aligned}
F_{A;B}(P) &= \max_{W \in \mathcal{W}_{n-i,k}} \left\| (P;\, W)^\top (A;\, B) \right\|_1 \\
&= \max_{W \in \mathcal{W}_{n-i,k}} \left\| (P^\top A + W^\top B) \right\|_1 \\
&\leq \max_{W \in \mathcal{W}_{n-i,k}} \left(\left\| P^\top A \right\|_1 + \left\| W^\top B \right\|_1 \right) \\
&= \left\| P^\top A \right\|_1 + \max_{W \in \mathcal{W}_{n-i,k}} \left\| W^\top B \right\|_1 \\
&= \left\| P^\top A \right\|_1 + L_k(B).
\end{aligned}$$

□

Let us now give the following definition further generalizing $F_M(P)$:

Definition 3.9

$$f_M(P)(c) = \max(F_M(P), c) \tag{59}$$

The computation of f_M can be optimized such that for big enough c values $f_M(P)(c)$ returns c without computing $F_M(P)$. This is expressed by the following lemma.

Lemma 3.10

$$f_M(P)(c) = \begin{cases} \max\left(\left\| P^\top M \right\|_1, c \right) & \text{if } P \in \mathcal{W}_{n,k}, \\ c \quad \text{if } \left\| P^\top A \right\|_1 + L_k(B) \leq c, & A; B = M, \\ (f_M(P; \mathbb{I}_0^k) \circ \cdots \circ f_M(P; \mathbb{I}_k^k))(c) & \text{otherwise} \end{cases} \tag{60}$$

The proof given below is split into three cases.
Case 1: If $P \in \mathcal{W}_{n,k}$, then

$$\begin{aligned}
f_M(P)(c) &= \max\left(\max_{W \in \mathcal{W}_{n-n,k}} \left\| (P;\, W)^\top M \right\|_1, c \right) \quad \text{by (57) and (59)} \\
&= \max\left(\left\| (P;\, ())^\top M \right\|_1, c \right) \\
&= \max\left(\left\| P^\top M \right\|_1, c \right).
\end{aligned}$$

Case 2:

$$\begin{aligned}
&\left\| P^\top A \right\|_1 + L_k(B) \leq c \\
&\quad \Rightarrow F_M(P) \leq c \quad \text{by (58)} \\
&\quad \Rightarrow \max(F_M(P), c) = c \\
&\quad \Rightarrow f_M(P)(c) = c \quad \text{by (59)}
\end{aligned}$$

Case 3:

$$
\begin{aligned}
f_M(P)(c) &= \max\left(\max_{W\in\mathcal{W}_{n-i,k}} \left\|(P;\,W)^\top M\right\|_1, c\right) \quad \text{by (57, 59)}\\
&= \max\left(\max_{S\in\mathcal{W}_{1,k},W\in\mathcal{W}_{n-i-1,k}} \left\|(P;\,S;\,W)^\top M\right\|_1, c\right)\\
&= \max\left(\max_j \max_{W\in\mathcal{W}_{n-i-1,k}} \left\|(P;\,\mathbb{I}_j^k;\,W)^\top M\right\|_1, c\right)\\
&= \max(\max_j F_M(P;\,\mathbb{I}_j^k), c)\\
&= \max(F_M(P;\,\mathbb{I}_0^k), \max(F_M(P;\,\mathbb{I}_1^k), \max(\ldots, c)))\\
&= (f_M(P;\,\mathbb{I}_0^k)\circ\cdots\circ f_M(P;\,\mathbb{I}_k^k))(c).
\end{aligned}
$$

□

Our last lemma in this subsection reads

Lemma 3.11

$$L_k(M) = f_M(())(0) \tag{61}$$

and it can be proved as follows:

$$
\begin{aligned}
&f_M(())(0)\\
&\quad= \max\left(\max_{W\in\mathcal{W}_{n,k}} \left\|(();\,W)^\top M\right\|_1, 0\right) \quad \text{by (57, 59)}\\
&\quad= \max_{W\in\mathcal{W}_{n,k}} \left\|W^\top M\right\|_1\\
&\quad= L_k(M)
\end{aligned}
$$

□

Programming tips for the efficient implementation of the L_2 and L_k codes. In this subsection, we give programming tips for the branch-and-bound[31] implementation of the exact computation of $L_k(M)$ for any $k \geq 2$. For $k = 2$ and $k = 3$ our algorithms are even faster than the L_k solver for general k due to specialization which we detail below. First, we remind the reader of the notation defined in Section "Properties of the L_2 and L_k, k>2 norm". The Haskell code can be downloaded from Github[57]. Instructions installing and using the code (including parallel execution and using guessed results) can also be found there.

Branch-and-bound calculation of L_k: The norm $L_k(M)$ for $k \geq 2$ can be calculated using the following definition and the following lemma.

Definition 3.12 For all $M \in \mathcal{M}_{n,m}$, $0 \leq i \leq n$ let

$$
\begin{aligned}
&f_M : \mathcal{W}_{i,k} \to (\mathbb{R} \to \mathbb{R})\\
&f_M(P)(c) = \begin{cases} \max(\left\|P^\top M\right\|_1, c) & \text{if } P \in \mathcal{W}_{n,k},\\ c \quad \text{if } \left\|P^\top A\right\|_1 + L_k(B) \leq c, & A;\,B = M,\\ (f_M(P;\,\mathbb{I}_0^k)\circ\cdots\circ f_M(P;\,\mathbb{I}_k^k))(c) & \text{otherwise.}\end{cases}
\end{aligned} \tag{62}
$$

The function f_M recursively calls itself with larger and larger P prefixes until the prefix size reaches n. The middle case is a conditional exit from the recursion, which speeds up the computation crucially.

Lemma 3.13

$$L_k(M) = f_M(())(0). \tag{63}$$

Reducing cost by sharing sub-calculations.—In the definition 3.12, the most expensive calculations are $L_k(B)$, $\left\|P^\top M\right\|_1$ and $\left\|P^\top A\right\|_1$. We show how to reduce the cost of these calculations. The cost of $L_k(B)$ can be reduced by memoizing the previously computed L_k values in a table.

If $M = (v_1; v_2; v_3; \ldots; v_n)$ then $L_k(M)$ depends on $L_k(v_i; v_{i+1}; \ldots; v_n)$, where $i = 2, 3, 4, \ldots, n$. Note that $L_k(v_i; v_{i+1}; \ldots; v_n)$ itself depends on $L_k(v_j; v_{j+1}; \ldots; v_n)$, where $j = i+1, i+2, \ldots, n$. If we take into account all dependencies, the correct order of calculating L_k values is $L_k(v_n)$, $L_k(v_{n-1}, v_n)$, $L_k(v_{n-2}, v_{n-1}, v_n)$, ..., $L_k(v_2, v_3, \ldots, v_n)$.

There is an option to skip the $\left\|P^\top A\right\|_1 + L_k(B) \leq c$ test for large B matrices. This means that $L_k(B)$ should not be calculated, and the trade-off is that we miss opportunities for exiting recursion. In our experience, skipping the test for $B \in \mathcal{M}_{k,m}, k \geq (3n/4)$ results in about 2× speedup.

The cost of calculating $\left\|P^\top A\right\|_1$ is $O(km)$ if $A \in \mathcal{M}_{k,m}$. Note that

$$(P;\,Q)^\top (A;\,B) = P^\top A + Q^\top B. \tag{64}$$

$P^\top A$ is already computed by the time when $(P; \mathbb{I}_i^k)^\top (A; v)$ is needed, so the cost of $\left\|P^\top A\right\|_1$ can be reduced to $O(m)$ by (64). The cost of $P^\top M$ can be reduced in the same way. This implies a considerable speedup; for example, for $M \in \mathcal{M}_{70,70}$ the calculation of $L_2(M)$ can be made nearly 70 times faster by this optimization.

The cost of $\left\|P^\top A\right\|_1$ can be further reduced by caching the previously calculated Manhattan norms of the rows of the matrix $P^\top A$.

Reducing cost by symmetries.—For all $S \in \mathcal{P}_k$ permutation matrices

$$\left\|W^\top M\right\|_1 = \left\|(WS)^\top M\right\|_1. \tag{65}$$

The cost of L_2 can be halved by (65) as follows. Let

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathcal{P}_2.$$

From $\left\|(\mathbb{I}_2^2;\ W)^\top M\right\|_1 = \left\|(\mathbb{I}_1^2;\ WS)^\top M\right\|_1$ it follows that $f_M(\mathbb{I}_2^2, c) = f_M(\mathbb{I}_1^2, c)$. This means that we can skip the calculation of $f_M(\mathbb{I}_2^2, c)$ for all c, thus $L_2(M) = f_M((\mathbb{I}_1^2), 0)$, i.e., we start the calculation with a non-empty prefix which saves work.

Harnessing (65) in the general L_k case is a bit more complex. First we define the set of canonical prefixes. A prefix $P = \mathbb{I}_{i_1}^k; \mathbb{I}_{i_2}^k; \ldots \mathbb{I}_{i_j}^k$ is canonical if the first occurrences of the numbers in the indices $i_1, i_2, \ldots, i_j$ is the sequence $1, 2, 3, \ldots$. For example, the prefix $\mathbb{I}_1^k; \mathbb{I}_2^k; \mathbb{I}_1^k; \mathbb{I}_3^k$ is canonical but $\mathbb{I}_1^k; \mathbb{I}_3^k; \mathbb{I}_1^k; \mathbb{I}_2^k$ is non-canonical. For each prefix P, there exists a permutation S such that PS is canonical, so that, $f_M(P, c) = f_M(PS, c)$, which means that it is enough to examine only the canonical prefixes to compute L_k.

Parallel and concurrent execution.—For parallel execution one can use the following equation:

$$f_M(P)(c) = \max_{i \in \{1,\ldots,k\}} f_M(P; \mathbb{I}_i^k)(c)\,. \tag{66}$$

We used Eq. (66) for $P \in \mathcal{W}_{i,k}, i < d$, where d is a "parallel depth" for fine-tuning the execution for different architectures. Higher depth is better for more cores.

Parallel execution may miss opportunities of exiting recursion because there is no communication between threads about the best known L_k values at a certain point of time. Therefore we implemented concurrent execution where threads share the best known L_k values.

Reducing cost by guessed L_k values.—Optionally, the computation can be sped up by providing a guessed $L_k(M)$ value by the user. This value will be used instead of 0 in Eq. (63). The guessed value may be lower than $L_k(M)$. Higher guessed values are better, unless the guessed value is higher than $L_k(M)$, in which case f_M returns the guessed value. We compared the result of f_M with the witness W of the maximal $\left\|W^\top M\right\|_1$ value, to be able to detect whether the guessed value was too high or not.

L-norm and L_2-norm are the same for a special family of matrices M'. We relate $L(M')$ to $L_2(M')$, where M' is given by the following matrix

$$M' = \begin{pmatrix} M \\ -M \end{pmatrix}, \tag{67}$$

where M is a matrix of size $n \times m$ with arbitrary real entries. Note that M' has size $2n \times m$ and M' has rows such that $M'_x = M_x$ and $M'_{x+m} = -M_x$ for all $x = 1, \ldots, m$. Then the following lemma holds.

Lemma 3.14 *$L_2(M') = L(M') = 2L(M)$ for any matrix M' of the form (67), where L_2 is the L_2 norm given by the definition (14) and L is the local bound given by (40). Note that L_k is defined by (39), where the case $k = 2$ corresponds to the definition of L_2 in (14).*

Proof We fix a matrix M of dimension $n \times m$ which specifies M' by the virtue of (67). Let $a_x \in \{-1, 1\}$, $x = 1, \ldots, n$ and $b_y \in \{-1, 1\}$, $y = 1, \ldots, m$ be the optimal vectors giving $L(M)$ in (40). Note that these values are not unique in general, different optimal configurations may exist, however, we choose one such optimal vectors a_x and b_y. We then choose $a_{x+n} = -a_x$ for $x = 1, \ldots, n$, and $b_y^+ = b_y^- = b_y$ for $y = 1, \ldots, m$. With these values, we obtain the lower bound $L_2(M') \geq 2L(M)$ on $L_2(M')$ in (12). Now we show the upper bound $L_2(M') \leq 2L(M)$, which implies $L_2(M') = 2L(M)$.

As a contradiction of the lemma, assume that $L_2(M') > 2L(M)$. Then, not all a_x vectors corresponding to the $L_2(M')$ value have the property $a_{x+m} = -a_x$ for each x. That is, there exists at least one x, call it x', for which $a'_x = a_{x'+n}$. Suppose that there is one such an x' (the proof for multiple x' indices for which $a'_x = a_{x'+n}$ is very similar). Then in the formula (14) for $L_2(M')$ the two rows x' and $x' + n$ in question will appear within the same norm (either in the first or second norm, depending on whether $a'_x = a_{x'+n}$ takes the value $+1$ or -1). However, in both cases they cancel each other from the norm in question. As a result, two rows of M' in (67) are eliminated, one from the matrix M and one from the matrix $-M$. However, any matrix $\pm M$ from which one row has been eliminated cannot have a local bound greater than $L(M)$. The same applies to a matrix $\pm M$ from which we have removed several rows. Therefore, $L_2(M') > 2L(M)$ cannot be true either. Thus we arrived at a contradiction. □

Adapting the Gisin-Gisin model to the PM scenario. We now adapt the LHV model of Ref.[27] which exploits the finite efficiency of the detectors to reproduce the quantum correlations of the singlet state exactly. We show that the LHV model in Ref.[27] can be adapted to the PM communication scenario to produce the expectation value:

$$E(\vec{a},\vec{b}) = P(b=+1|\vec{a},\vec{b}) - P(b=-1|\vec{a},\vec{b}) = \frac{\vec{a}\cdot\vec{b}+1}{2}, \tag{68}$$

where $\vec{a} \in S^2$ denotes the preparation Bloch vector and $\vec{b} \in S^2$ denotes the measurement Bloch vector. First we show that the outcomes $b = \pm 1$ giving the expectation value

$$E(\vec{a},\vec{b}) = P(b=+1|\vec{a},\vec{b}) - P(b=-1|\vec{a},\vec{b}) = \vec{a}\cdot\vec{b} \tag{69}$$

can be obtained with probability 1/2 and $b = 0$ outcome with probability 1/2. Then by coarse-graining the above distribution by grouping $b = 0$ outcome with $b = +1$, we obtain the expectation value (68).

The classical model, using one bit of classical communication from Alice to Bob, is as follows.

Protocol: Alice and Bob share a classical variable, which is in the form of a unit vector $\vec{\lambda}$, chosen uniformly at random from the unit sphere S^2.

- *Alice*: Alice sends a binary message $c = \mathrm{sgn}(\vec{a}\cdot\vec{\lambda})$ to Bob. That is, $c = +1$ if $\vec{a}\cdot\vec{\lambda} \leq 0$ and $c = -1$ if $\vec{a}\cdot\vec{\lambda} > 0$.
- *Bob*: Bob outputs $b = \mathrm{sgn}(c\vec{b}\cdot\vec{\lambda})$ with probability $|\vec{b}\cdot\vec{\lambda}|$ (corresponding to the detection event $b = \pm 1$) and Bob outputs $b = 0$ with probability $1 - |\vec{b}\cdot\vec{\lambda}|$ (corresponding to the non-detection event).

Our claim is as follows. The above protocol yields the correlations $E(\vec{a},\vec{b}) = \vec{a}\cdot\vec{b}$, that is, it reproduces the correlations in Eq. (69) with probability 1/2 and returns $b = 0$ in the other cases.

Proof.—We need to calculate the expectation value $E(\vec{a},\vec{b}) = P(b=+1|\vec{a},\vec{b}) - P(b=-1|\vec{a},\vec{b})$ which according to the above protocol in the detection events $b = \pm 1$ is given by[27]

$$E(\vec{a},\vec{b}) = \int_{S^2} d\vec{\lambda} q(\vec{\lambda}|b=\pm 1)\mathrm{sgn}(\vec{a}\cdot\vec{\lambda})\mathrm{sgn}(\vec{b}\cdot\vec{\lambda}), \tag{70}$$

where $q(\vec{\lambda}|b=\pm 1)$ is the conditional density probability distribution of choosing $\vec{\lambda}$ given a detection event (either output $b = +1$ or $b = -1$). This function can be calculated from

$$q(\vec{\lambda}|b=\pm 1) = \frac{q(\vec{\lambda} \text{ and } b=\pm 1)}{p(b=\pm 1)}, \tag{71}$$

where the detection efficiency is $\eta = p(b=\pm 1)$ and the probability of detection failure is $1-\eta = p(b=0)$. The value of η is given by

$$\eta = p(b=\pm 1) = \int_{S^2} \frac{d\vec{\lambda}}{4\pi} |\vec{b}\cdot\lambda| = \frac{1}{2}, \tag{72}$$

as stated and the protocol gives the density probability distribution $q(\lambda \text{ and } b=\pm 1) = (\vec{b}\cdot\vec{\lambda})/(4\pi)$. Inserting these values into (71) gives $q(\lambda|b=\pm 1) = (\vec{b}\cdot\vec{\lambda})/(2\pi)$, which in turn is inserted into (70) to obtain the integral[27]:

$$E(\vec{a},\vec{b}) = \frac{1}{2\pi}\int_{S^2} d\vec{\lambda}(\vec{b}\cdot\vec{\lambda})\mathrm{sgn}(\vec{a}\cdot\vec{\lambda}). \tag{73}$$

The above integral can be calculated using spherical symmetries. In particular, one can choose w.l.o.g. the vectors

$$\vec{a} = (0,0,1)$$
$$\vec{b} = (\sin\alpha, 0, \cos\alpha)$$

as in Ref.[27], and then obtain

$$E(\vec{a},\vec{b}) = \cos\alpha = \vec{a}\cdot\vec{b} \tag{74}$$

with probability 1/2, which we wanted to prove. □

The modified Gilbert algorithm adapted to the PM scenario. For a given $\eta \in [1/2, 1]$ and correlation matrix $E(\eta)$ defined by (28), the algorithm yields the following matrix M satisfying

$$\sum_{x=1}^{n}\sum_{y=1}^{m} M_{xy}E_{xy}(\eta) > L_2(M). \tag{75}$$

Algorithm:

Input: The number of preparations n and the number of measurement settings m that define the setup. The unit vectors $\{\vec{a}_x\}_{x=1}^{n}$ (i.e., the Bloch vectors of Alice's prepared states) and $\{\vec{b}_y\}_{y=1}^{m}$ (i.e., the Bloch vectors of Bob's projective rank-1 measurements). The $(n \times m)$-dimensional matrix $E(\eta)$ given by the entries $E_{xy}(\eta)$ in (28). The values of ϵ and $i_{\max}$ that define the stopping criteria.

Output: The matrix M of size $n \times m$.

1. Set $i = 0$ and set $E^{(i)}$ the $n \times m$ zero matrix.
2. Given a matrix $E^{(i)}$ and the matrix $E(\eta)$, run a heuristic oracle that maximizes the overlap $\sum_{xy}(E_{xy}(\eta) - E_{xy}^{(i)})E_{xy}^{\det}$ over all deterministic one-bit correlations $E_{xy}^{\det}$ in (11). The description of this heuristic (see-saw) oracle is given in Section "Lower bound to $L_{2(M)}$ using the see-saw iterative algorithm". Denote the point $E_{xy}^{\det}$ returned by the oracle by $E_{xy}^{\det,i}$.
3. Find the convex combination $E^{(i+1)}$ of $E^{(i)}$ and $E_{xy}^{\det,i}$ that minimizes the distance $\sqrt{\sum_{xy}\left(E_{xy}(\eta) - E_{xy}^{(i)}\right)^2}$. Let us denote this distance by $\mathrm{dist}(i)$.
4. Let $i = i + 1$ and go to Step 2 until $\mathrm{dist}(i) \leq \epsilon$ or $i = i_{\max}$.
5. Return the matrix M with coordinates $M_{xy} = E_{xy}(\eta) - E_{xy}^{(i)}$.

Note that $\mathrm{dist}(i)$ is a decreasing function of i. Since maximizing the overlap of $\sum_{xy}(E_{xy}(\eta) - E_{xy}^{(i)})E_{xy}^{\det}$ over all deterministic one-bit correlations vectors is an NP-hard problem, in Step 2 we use a heuristic method to do it, which we describe in Section "Lower bound to $L_{2(M)}$ using the see-saw iterative algorithm". On the other hand, the description of an exact branch-and-bound type algorithm can be found in Section "Programming tips for the efficient implementation of the L_2 and L_k codes". We use the exact method, which is generally more time-consuming than the see-saw method to check that the output matrix M satisfies the condition (75) with the chosen parameter η. If this is true, then it implies the lower bound $K_D \geq (1/\eta)$, as proved in Section "Proof of the bounds $1.5682 \leq K_D \leq 2$". It should also be noted that the branch-and-bound-type algorithm is much faster than the brute force algorithm (the implemented algorithm using parallelism can be found in[57]). On a multi-core desktop computer, it can solve problems in range $n = m = 70$ in a day, while the brute force algorithm is limited to about $n = m = 40$ settings.

Parameters and implementation of Gilbert algorithm. Here we specify the explicit parameters that are used to obtain the lower bound $K_D \leq 1.5682$. On the three-dimensional unit sphere, we choose the vectors $\{\vec{a}_x\}_{x=1}^{n}$ and $\{\vec{b}_y\}_{y=1}^{m}$ to be equal to each other, $\vec{v}_i = \vec{a}_i = \vec{b}_i$ for $i = 1, \ldots, n$, where $n = m = 70$. The 70 unit vectors chosen define the optimal packing configuration in the Grassmannian space which can be downloaded from Neil Sloane's database[58]. The advantage of this type of packing is that the points and their antipodal points are located as far apart as possible on the three-dimensional unit sphere.

We implemented the modified Gilbert algorithm (of Section "The modified Gilbert algorithm adapted to the PM scenario") in Matlab with and without a memory buffer (see more details on the memory buffer in Ref.[39]). In the case of using memory buffer, the step 3 is modified in the algorithm so that instead of calculating the convex combination of the points $E^{(i)}$ and $E_{xy}^{\det,i}$ (see section "The modified Gilbert algorithm adapted to the PM scenario"), we compute the convex combination of $E^{(i)}$ and the points $E_{xy}^{\det,i-j}$, $j = 0, \ldots, m-1$, where m is the size of the memory buffer. In our explicit computations, we use a buffer size $m = 40$ and a stopping condition of $k = 2 \times 10^5$ with $\eta = 0.665$. Details on the performance of this modification can be found in Ref.[39]. In step 2 of the Gilbert algorithm, the oracle uses the see-saw heuristic described in Section "Lower bound to $L_{2(M)}$ using the see-saw iterative algorithm" to obtain a good (typically tight) lower bound to $L_2(M)$. On the other hand, we used the branch-and-bound-type algorithm described in Section "Programming tips for the efficient implementation of the L_2 and L_k codes" to calculate $L_2(M)$ exactly for integer M. The algorithm was implemented in Haskell. See the GitHub site[57] for the downloadable version.

The Matlab file `eta_70.m`, which can also be downloaded from GitHub[57] (located in the subdirectory `L2_eta_70`) gives detailed results on the input parameters. In particular, it gives the unit vectors $\vec{a}_i = \vec{b}_i = \vec{v}_i$, the lower bound $\sum_{xy} M_{xy}\vec{a}_x \cdot \vec{b}_y = \sum_{xy} M_{xy}\vec{v}_x \cdot \vec{v}_y$ to $q(M)$ and the value $L_2(M)$. The input matrix M is placed in subdirectory `L2_eta_70` under the name `W70i.txt`. The running time of the Gilbert algorithm (in Section "The modified Gilbert algorithm adapted to the PM scenario") implemented in Matlab was about one week. Note, however, that most of the computation time was spent on the oracle (the see-saw part) described in Section "Lower bound to $L_{2(M)}$ using the see-saw iterative algorithm". On the other hand, the Haskell code to compute the exact $L_2(M)$ value of the 70×70 witness matrix M took about 8 hours to run on a HP Z8 workstation using 56 physical cores. The memory usage of the computation was negligible.

The Matlab `eta_70.m` routine defines the 70×70 matrix M, and gives the $\vec{v}_i := \vec{a}_i = \vec{b}_i$ the unit vectors from Sloane's database[58] for all $i = 1, \ldots, 70$. Note that M is integer (by multiplying the output M matrix in the Gilbert algorithm by 1000 and truncating the non-integer part). This calculation yields $S(M) = \sum_{x,y} M_{x,y} = 194369$ and $Q(M) = \sum_{x,y} M_{x,y}\vec{a}_x \cdot \vec{b}_y \simeq 5.3672235 \times 10^5$. On the other hand, the branch-and-bound-type Haskell code[57] gives the exact value $L_2(M) = 412667$, which is matched by the see-saw search (in Section "Lower bound to $L_{2(M)}$ using the see-saw iterative algorithm"). From these numbers we then obtain

$$K_{\mathrm{D}} \geq \frac{Q(M) - S(M)}{L_2(M) - S(M)} > \frac{342353}{218298} = 1.5682 + \varepsilon \tag{76}$$

and $1/K_{\mathrm{D}} = 0.6377 - \varepsilon'$ is the upper bound to the critical detection efficiency η_{crit}, where ε and ε' are small positive numbers.

Lower bound to $L_2(M)$ using the see-saw iterative algorithm. Below we give an iterative algorithm based on see-saw heuristics to compute $L_2(M)$. This algorithm forms the oracle part of step 2 of the Gilbert algorithm, which is described in Section "The modified Gilbert algorithm adapted to the PM scenario".

Algorithm:
Input: Integer matrix M of size $n \times m$.
Output: Lower bound $l_2(M)$ to $L_2(M)$ defined by formula (12).

1. Let $l_2 = 0$.
2. Choose random assignments $a_x = \pm 1$: That is, a_x are (random) elements of a vector a of size n. Its elements are binary having value +1 or -1 only.
3. Set $b^+ = \mathrm{sgn}(aM)$, where sgn denotes the (modified) sign function: $\mathrm{sgn}(x) = +1$ if $x \geq 0$ and -1 otherwise. Let us transpose b^+.
4. Set $b^- = \mathrm{sgn}(aM)$. Let us transpose b^-.
5. Form the column vector $s^+ = Mb^+$ of size n.
6. Form the column vector $s^- = Mb^-$ of size n.
7. Form the column vector $s = \max(s^+, s^-)$ of size n. That is, $s_x = \max(s_x^+, s_x^-)$ for all $x = 1, \ldots, n$.
8. Form the ± 1-valued column vector a as follows: Let $a_x = +1$ if $s_x^+ \geq s_x^-$, otherwise let $a_x = -1$ for all $x = 1, \ldots, n$.
9. Let $l_2 = \sum_{x=1}^{n} s_x$.
10. With the new vector a, return to point 3. Repeat the algorithm until two values of l_2 are equal in two consecutive iterations.

Note that at each iteration step, objective value $l_2(M)$ is guaranteed not to decrease. Therefore, the output of the algorithm is a heuristic lower bound on the exact value of $L_2(M)$.

Discussion

We have tested the quantumness of two-dimensional systems in the prepare-and-measure (PM) scenario, with n preparations and m binary-outcome measurement settings, where n and m fall well into the range of 70. In the one-qubit PM scenario, a two-level system is transmitted from the sender to the receiver. In this setup, a real $n \times m$ matrix M defines the coefficients of a linear witness. We denote by $L_2(M)$ the exact value of the one-bit bound associated with matrix M. We found efficient numerical algorithms for computing $L_2(M)$. If this bound is exceeded, we can detect both the quantumness of the prepared qubits and the quantumness (i.e. incompatibility) of the measurements.

We introduced new constants K_{M} and K_{D} which are related to the Grothendieck constant of order 3. Our large-scale tools are crucial for the efficient bounding of $L_2(M)$ and hence for bounding of the constants K_{M} and K_{D}. We further relate these new constants to the white noise resistance of the prepared qubits and the critical detection efficiency of the measurements performed.

For large M matrices, we have given two algorithms for computing $L_2(M)$: a simple iterative see-saw-type algorithm and a branch-and-bound-type algorithm. The former is a heuristic algorithm that usually gives a tight lower bound on $L_2(M)$. However, sometimes it fails to find the exact value of $L_2(M)$. This happens more and more often as the size of the matrix M gets larger and larger. In contrast, the latter branch-and-bound-type algorithm gives the exact value of $L_2(M)$ and can be used to compute $L_2(M)$ for matrix sizes as large as 70×70. As an application of the algorithms, we established the bounds $1.5682 \leq K_{\mathrm{D}} \leq 2$ on the new constant and an upper bound of $\eta_{\mathrm{crit}} \leq 0.6377$ on the critical detection efficiency of qubit measurements in the PM scenario.

Data availability

The dataset (the 70×70 matrix M) used to prove the lower bound (22) on K_D is available in Github[57].

Code availability

The Haskell and MATLAB codes used to prove the lower bound (22) on K_D is available in Github[57].

Received: 6 November 2022; Accepted: 26 July 2023
Published online: 14 August 2023

References

1. Bell, J. S. On the Einstein-Poldolsky-Rosen paradox. *Physics* **1**, 195–200. https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195 (1964).
2. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478. https://doi.org/10.1103/RevModPhys.86.419 (2014).
3. Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.* **98**, 140402. https://doi.org/10.1103/PhysRevLett.98.140402 (2007).

4. Bowles, J., Vértesi, T., Quintino, M. T. & Brunner, N. One-way Einstein-Podolsky-Rosen steering. *Phys. Rev. Lett.* **112**, 200402. https://doi.org/10.1103/PhysRevLett.112.200402 (2014).
5. Jevtic, S., Hall, M. J. W., Anderson, M. R., Zwierz, M. & Wiseman, H. M. Einstein-Podolsky-Rosen steering and the steering ellipsoid. *JOSA B* **32**, A40. https://doi.org/10.1364/JOSAB.32.000A40 (2015).
6. Uola, R., Costa, A. C. S., Nguyen, H. C. & Gühne, O. Quantum steering. *Rev. Mod. Phys.* **92**, 015001. https://doi.org/10.1103/RevModPhys.92.015001 (2020).
7. Gallego, R., Brunner, N., Hadley, C. & Acín, A. Device-independent tests of classical and quantum dimensions. *Phys. Rev. Lett.* **105**, 230501. https://doi.org/10.1103/PhysRevLett.105.230501 (2010).
8. Buhrman, H., Cleve, R., Massar, S. & de Wolf, R. Nonlocality and communication complexity. *Rev. Mod. Phys.* **82**, 665. https://doi.org/10.1103/revmodphys.82.665 (2010).
9. Ahrens, J., Badziag, P., Cabello, A. & Bourennane, M. Experimental device-independent tests of classical and quantum dimensions. *Nat. Phys.* **8**, 592–595. https://doi.org/10.1038/nphys2333 (2012).
10. Hendrych, M. *et al.* Experimental estimation of the dimension of classical and quantum systems. *Nat. Phys.* **8**, 588–591. https://doi.org/10.1038/nphys2334 (2012).
11. Ahrens, J., Badziąg, P., Pawłowski, M., Żukowski, M. & Bourennane, M. Experimental tests of classical and quantum dimensionality. *Phys. Rev. Lett.* **112**, 140401. https://doi.org/10.1103/PhysRevLett.112.140401 (2014).
12. Poderini, D., Brito, S., Nery, R., Sciarrino, F. & Chaves, R. Criteria for nonclassicality in the prepare-and-measure scenario. *Phys. Rev. Res.* **2**, 043106. https://doi.org/10.1103/PhysRevResearch.2.043106 (2020).
13. de Gois, C. *et al.* General method for classicality certification in the prepare and measure scenario. *PRX Quantum* **2**, 030311. https://doi.org/10.1103/PRXQuantum.2.030311 (2021).
14. Drótos, G., Pál, K. F. & Vértesi, T. Self-testing of semisymmetric informationally complete measurements in a qubit prepare-and-measure scenario. *arXiv* https://doi.org/10.48550/arXiv.2306.07248 *(2023).*
15. Ambainis, A., Nayak, A., Ta-Shma, A. & Vazirani, U. Dense quantum coding and quantum finite automata. *J. ACM* **49**, 496. https://doi.org/10.1145/581771.581773 (2002).
16. Mannalath, V. & Pathak, A. Bounds on semi-device-independent quantum random-number expansion capabilities. *Phys. Rev. A* **105**, 022435. https://doi.org/10.1103/physreva.105.022435 (2022).
17. Li, H.-W., Pawłowski, M., Yin, Z.-Q., Guo, G.-C. & Han, Z.-F. Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random access codes. *Phys. Rev. A* **85**, 052308. https://doi.org/10.1103/physreva.85.052308 (2012).
18. Vaisakh, M. *et al.* Mutually unbiased balanced functions and generalized random access codes. *Phys. Rev. A* **104**, 012420. https://doi.org/10.1103/physreva.104.012420 (2021).
19. Krishna Patra, R. *et al.* Classical analogue of quantum superdense coding and communication advantage of a single quantum. *arXiv* https://doi.org/10.48550/arXiv.2202.06796 *(2022).*
20. Doriguello, J. F. & Montanaro, A. Quantum random access codes for Boolean functions. *Quantum* **5**, 402. https://doi.org/10.22331/q-2021-03-07-402 (2021).
21. Alves, G. P., Gigena, N. & Kaniewski, J. Biased random access codes. *arXiv* https://doi.org/10.48550/arXiv.2302.08494 *(2023).*
22. Grothendieck, A. "Résumé de la théorie métrique des produits tensoriels topologiques," *Bol. Soc. Mat. São Paulo* **8**, 1. https://www.ime.usp.br/acervovirtual/textos/estrangeiros/grothendieck/produits_tensoriels_topologiques/files/produits_tensoriels_topologiques.pdf (1953).
23. Khot, S. & Naor, A. Grothendieck-type inequalities in combinatorial optimization. *Commun. Pure Appl. Math.* **65**, 992–1035. https://doi.org/10.1002/cpa.21398 (2012).
24. Tsirelson, B. S. Some results and problems on quantum Bell-type inequalities. *Hadronic J. Suppl.* **8**, 329–345 (1993).
25. Acín, A., Gisin, N. & Toner, B. Grothendieck's constant and local models for noisy entangled quantum states. *Phys. Rev. A* **73**, 062105. https://doi.org/10.1103/PhysRevA.73.062105 (2006).
26. Krivine, J. Constantes de Grothendieck et fonctions de type positif sur les spheres. *Adv. Math.* **31**, 16–30. https://doi.org/10.1016/0001-8708(79)90017-3 (1979).
27. Gisin, N. & Gisin, B. A local hidden variable model of quantum correlation exploiting the detection loophole. *Phys. Lett. A* **260**, 323. https://doi.org/10.1016/S0375-9601(99)00519-8 (1999).
28. Navascués, M. & Vértesi, T. Bounding the set of finite dimensional quantum correlations. *Phys. Rev. Lett.* **115**, 020501. https://doi.org/10.1103/PhysRevLett.115.020501 (2015).
29. Tavakoli, A., Rosset, D. & Renou, M.-O. Enabling computation of correlation bounds for finite-dimensional quantum systems via symmetrization. *Phys. Rev. Lett.* **122**, 070501. https://doi.org/10.1103/PhysRevLett.122.070501 (2019).
30. Tavakoli, A., Kaniewski, J., Vértesi, T., Rosset, D. & Brunner, N. Self-testing quantum states and measurements in the prepare-and-measure scenario. *Phys. Rev. A* **98**, 062307. https://doi.org/10.1103/PhysRevA.98.062307 (2018).
31. Land, A. H. & Doig, A. G. An automatic method of solving discrete programming problems. *Econometrica* **28**, 497. https://doi.org/10.2307/1910129 (1960).
32. Pisier, G. Grothendieck's Theorem, past and present. *Bull. Amer. Math. Soc.* **49**, 237–323 (2012).
33. Hua, B. *et al.* Towards Grothendieck constants and LHV models in quantum mechanics. *J. Phys. A: Math. Theor.* **48**, 065302. https://doi.org/10.1088/1751-8113/48/6/065302 (2015).
34. Designolle, S. *et al.* Improved local models and new Bell inequalities via Frank-Wolfe algorithms. *arXiv* https://doi.org/10.48550/arXiv.2302.04721 *(2023).*
35. Diviánszky, P., Bene, E. & Vértesi, T. Qutrit witness from the Grothendieck constant of order four. *Phys. Rev. A* **96**, 012113. https://doi.org/10.1103/PhysRevA.96.012113 (2017).
36. Hirsch, F., Quintino, M. T., Vértesi, T., Navascués, M. & Brunner, N. Better local hidden variable models for two-qubit Werner states and an upper bound on the Grothendieck constant $K_G(3)$. *Quantum* **1**, 3. https://doi.org/10.22331/q-2017-04-25-3 (2017).
37. Finch, S. R. *Mathematical constants*. Cambridge University Press, (2003). http://www.cambridge.org/catalogue/catalogue.asp?isbn=0521818052
38. Wikipedia.org: Grothendieck inequality https://en.wikipedia.org/wiki/Grothendieck_inequality.
39. Brierley, S., Navascues, M. & Vertesi, T. Convex separation from convex optimization for large-scale problems. Preprint at https://arXiv.org/quant-ph/1609.05011 (2016).
40. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 15. https://doi.org/10.1103/PhysRevLett.23.880 (1969).
41. Gilbert, E. G. An iterative procedure for computing the minimum of a quadratic form on a convex set. *SIAM J. Control* **4**, 61–80. https://doi.org/10.1137/0304007 (1966).
42. Vértesi, T. More efficient Bell inequalities for Werner states. *Phys. Rev. A* **78**, 032112. https://doi.org/10.1103/PhysRevA.78.032112 (2008).
43. Werner, R. F. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A* **40**, 4277–4281. https://doi.org/10.1103/PhysRevA.40.4277 (1989).
44. Bowles, J., Brunner, N. & Pawlowski, M. Testing dimension and nonclassicality in communication networks. *Phys. Rev. A* **92**, 022351. https://doi.org/10.1103/PhysRevA.92.022351 (2015).
45. Larsson, J. A. Loopholes in Bell inequality tests of local realism. *J. Phys. A: Math. Theor.* **47**, 424003. https://doi.org/10.1088/1751-8113/47/42/424003 (2014).

46. Dall'Arno, M., Passaro, E., Gallego, R. & Acin, A. Robustness of device-independent dimension witnesses. *Phys. Rev. A* **86**, 042312. https://doi.org/10.1103/PhysRevA.86.042312 (2012).
47. Li, H.-W., Yin, Z.-Q., Pawłowski, M., Guo, G.-C. & Han, Z.-F. Detection efficiency and noise in a semi-device-independent randomness-extraction protocol. *Phys. Rev. A* **91**, 032305. https://doi.org/10.1103/PhysRevA.91.032305 (2015).
48. Brunner, N., Navascués, M. & Vértesi, T. Dimension witnesses and quantum state discrimination. *Phys. Rev. Lett.* **110**, 150501. https://doi.org/10.1103/PhysRevLett.110.150501 (2013).
49. Raghavendra, P. & Steurer, D. "Towards computing the Grothendieck constant," In *Proceedings of the Twentieth Annual ACM-SIAM Symposium on Discrete Algorithms*, 525. https://doi.org/10.1137/1.9781611973068.58 (2009).
50. Diviánszky, P. https://github.com/divipp/kmn-programming (2017).
51. Vértesi, T. & Pál, K. F. Generalized Clauser-Horne-Shimony-Holt inequalities maximally violated by higher-dimensional systems. *Phys. Rev. A* **77**, 042106. https://doi.org/10.1103/PhysRevA.77.042106 (2008).
52. Epping, M., Kampermann, H. & Bruß, D. Designing Bell inequalities from a Tsirelson bound. *Phys. Rev. Lett.* **111**, 240404. https://doi.org/10.1103/PhysRevLett.111.240404 (2013).
53. Epping, M., Kampermann, H. & Bruß, D. Optimization of Bell inequalities with invariant Tsirelson bound. *J. Phys. A* **47**, 424015. https://doi.org/10.1088/1751-8113/47/42/424015 (2014).
54. Frieze, A. & Kannan, R. Quick approximation to matrices and applications. *Combinatorica* **19**, 175–220. https://doi.org/10.1007/s004930050052 (1997).
55. Borgs, C., Chayes, J. T., Lovász, L., Sós, V. T. & Vesztergombi, K. Convergent sequences of dense graphs. I. Subgraph frequencies, metric properties and testing. *Adv. Math.* **219**, 1801–1851. https://doi.org/10.1016/j.aim.2008.07.008 (2008).
56. Alon, N. & Naor, A. "Approximating the cut-norm via Grothendieck's inequality", In *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*https://doi.org/10.1145/1007352.1007371 *(2004).*
57. Diviánszky, P. https://github.com/divipp/l2-norm (2023).
58. Sloane, N.J.A. http://neilsloane.com/grass/.

Acknowledgements
We thank Mátyás Barczy, Emmanuel Zambrini Cruzeiro and Armin Tavakoli for valuable discussions. We are particularly indebted to Mátyás Barczy for pointers to the literature regarding the cut norm. T. V. acknowledges the support of the EU (QuantERA eDICT) and the National Research, Development and Innovation Office NKFIH (No. 2019-2.1.7-ERA-NET-2020-00003).

Author contributions
All authors contributed equally to this work.

Funding
Open access funding provided by ELKH Institute for Nuclear Research.

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to T.V.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.