PHYSICS

Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments

Armin Tavakoli[1]*†, Máté Farkas[2,3‡], Denis Rosset[4], Jean-Daniel Bancal[1], Jedrzej Kaniewski[5]

Mutually unbiased bases (MUBs) and symmetric informationally complete projectors (SICs) are crucial to many conceptual and practical aspects of quantum theory. Here, we develop their role in quantum nonlocality by (i) introducing families of Bell inequalities that are maximally violated by *d*-dimensional MUBs and SICs, respectively, (ii) proving device-independent certification of natural operational notions of MUBs and SICs, and (iii) using MUBs and SICs to develop optimal-rate and nearly optimal-rate protocols for device-independent quantum key distribution and device-independent quantum random number generation, respectively. Moreover, we also present the first example of an extremal point of the quantum set of correlations that admits physically inequivalent quantum realizations. Our results elaborately demonstrate the foundational and practical relevance of the two most important discrete Hilbert space structures to the field of quantum nonlocality.

INTRODUCTION

Measurements are crucial and compelling processes at the heart of quantum physics. Quantum measurements, in their diverse shapes and forms, constitute the bridge between the abstract formulation of quantum theory and concrete data produced in laboratories. Crucially, the quantum formalism of measurement processes gives rise to experimental statistics that elude classical models. Therefore, appropriate measurements are indispensable for harvesting and revealing quantum phenomena. Sophisticated manipulation of quantum measurements is both at the heart of the most well-known features of quantum theory such as contextuality (*1*) and the violation of Bell inequalities (*2*) as well as its most groundbreaking applications such as quantum cryptography (*3*) and quantum computation (*4*). In the broad landscape of quantum measurements (*5*), certain classes of measurements are outstanding because of their breadth of relevance in foundations of quantum theory and applications in quantum information processing.

Two widely celebrated, intensively studied, and broadly useful classes of measurements are known as mutually unbiased bases (MUBs) and symmetric informationally complete measurements (SICs). Two measurements are said to be mutually unbiased if by preparing any eigenstate of the first measurement and then performing the second measurement, one finds that all outcomes are equally likely (*6*). A typical example of MUBs corresponds to measuring two perpendicular components of the polarization of a photon. A SIC is a quantum measurement with the largest number of possible outcomes such that all measurement operators have equal magnitude overlaps (*7*, *8*). Thus, the former is a relationship between two different measurements, whereas the latter is a relationship within a single measurement. Since MUBs and SICs are both conceptually natural, elegant, and (as it turns out) practically important classes of measurements, they are often studied in the same context (*9*–*14*). Let us briefly review their importance to foundational and applied aspects of quantum theory.

MUBs are central to the concept of complementarity in quantum theory, i.e., how the knowledge of one quantity limits (or erases) the knowledge of another quantity [see, e.g., (*15*) for a review of MUBs]. This is often highlighted through variants of the famous Stern-Gerlach experiment in which different Pauli observables are applied to a qubit. For instance, after first measuring (say) σ_x, we know whether our system points up or down the x axis. If we then measure σ_z, our knowledge of the outcome of yet another σ_x measurement is entirely erased since σ_z and σ_x are MUBs. This phenomenon leads to an inherent uncertainty for the outcomes of MUB measurements on all quantum states, which can be formalized in terms of entropic quantities, leading to so-called entropic uncertainty relations. It is then natural that MUBs give rise to the strongest entropic uncertainties in quantum theory (*16*). Moreover, MUBs play a prominent role in quantum cryptography, where they are used in many of the most well-known quantum key distribution protocols (*17*–*21*) and in secret sharing protocols (*22*–*24*). Their appeal to cryptography stems from the idea that eavesdroppers who measure an eigenstate of one basis in another basis unbiased to it obtain no useful information, while they also induce a large disturbance in the state that allows their presence to be detected. Furthermore, complete (i.e., largest possible in a given dimension) sets of MUBs are tomographically complete, and their symmetric properties make them pivotal for quantum state tomography (*25*, *26*). In addition, MUBs are useful for a range of other problems such as quantum random access coding (*27*–*31*), quantum error correction (*32*, *33*), and entanglement detection (*34*). This broad scope of relevance has motivated much effort toward determining the largest number of MUBs that exist in general Hilbert space dimensions (*15*).

The motivations behind the study of SICs are quite similar to the ones discussed for MUBs. It has been shown that SICs are natural

[1]Department of Applied Physics, University of Geneva, 1211 Geneva, Switzerland. [2]Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdansk, 80-952 Gdansk, Poland. [3]International Centre for Theory of Quantum Technologies, University of Gdansk, 80-308 Gdansk, Poland. [4]Perimeter Institute for Theoretical Physics, 31 Caroline St. N, Waterloo, Ontario N2L 2Y5, Canada. [5]Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warsaw, Poland.
*Corresponding author. Email: armin.tavakoli@oeaw.ac.at
†Present address: Institute for Quantum Optics and Quantum Information (IQOQI) Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria.
‡Present address: Institut de Ciencies Fotoniques (ICFO), Barcelona Institute of Science and Technology, Av. Carl Friedrich Gauss 3, 08860 Castelldefels, Barcelona, Spain

measurements for quantum state tomography (*35*), which has also prompted several experimental realizations of SICs (*36*–*38*). In addition, some protocols for quantum key distribution derive their success directly from the defining properties of SICs (*39*, *40*), which have also been experimentally demonstrated (*41*). Furthermore, a key property of SICs is that they have the largest number of outcomes possible while still being extremal measurements, i.e., they cannot be simulated by stochastically implementing other measurements. This gives SICs a central role in a range of applications, which include random number generation from entangled qubits (*42*), certification of nonprojective measurements (*43*–*46*), semi–device-independent self-testing (*45*), and entanglement detection (*47*, *48*). Moreover, SICs have a key role in quantum Bayesianism (*49*), and they exhibit interesting connections to several areas of mathematics, for instance, Lie and Jordan algebras (*50*) and algebraic number theory (*51*). Because of their broad interest, much research effort has been directed toward proving the existence of SICs in all Hilbert space dimensions (presently known, at least, up to dimension 193) (*7*, *8*, *52*–*55*). See, e.g., (*54*) for a recent review of SICs.

In this work, we broadly investigate MUBs and SICs in the context of Bell nonlocality experiments. In these experiments, two separated observers perform measurements on entangled quantum systems that can produce nonlocal correlations that elude any local hidden variable model (*56*). In recent years, Bell inequalities have played a key role in the rise of device-independent quantum information processing where they are used to certify properties of quantum systems. Naturally, certification of a physical property can be achieved under different assumptions of varying strength. Device-independent approaches offer the strongest form of certification since the only assumptions made are space-like separation and the validity of quantum theory. The advent of device-independent quantum information processing has revived interest in Bell inequalities, as these can now be tailored to the purpose of certifying useful resources for quantum information processing. The primary focus of such certification has been on various types of entangled states (*57*). However, quantum measurements are equally important building blocks for quantum information processing. Nevertheless, our understanding of which arrangements of high-dimensional measurements can be certified in a device-independent manner is highly limited. We speak of arrangements of measurements because for a single measurement (acting on a quantum system with no internal structure), no interesting property can be certified. The task becomes nontrivial when at least two measurements are present and we can certify the relation between them. The simplest approach relies on combining known self-testing results for two-qubit systems, which allows us to certify high-dimensional measurements constructed out of qubit building blocks (*58*, *59*). Alternatively, device-independent certification of high-dimensional structures can be proven from scratch, but to the best of our knowledge, only two results of this type have been proven: (i) a triple of MUBs in dimension three (*60*) and (ii) the measurements conjectured to be optimal for the Collins-Gisin-Linden-Massar-Popescu Bell inequality (the former is a single result, while the latter is a family parameterized by the dimension $d \geq 2$) (*61*). None of these results can be used to certify MUBs in dimension $d \geq 4$.

Since mutual unbiasedness and symmetric informational completeness are natural and broadly important concepts in quantum theory, they are prime candidates of interest for such certification in general Hilbert space dimensions. This challenge is increasingly relevant because of the broader experimental advances toward high-dimensional systems along the frontier of quantum information theory. This is also reflected in the fact that recent experimental implementations of MUBs and SICs can go well beyond the few lowest Hilbert space dimensions (*38*, *41*, *62*).

Focusing on mutual unbiasedness and symmetric informational completeness, we solve the above challenges. To this end, we first construct Bell inequalities that are maximally violated using a maximally entangled state of local dimension d and, respectively, a pair of d-dimensional MUBs and a d-dimensional SIC. In the case of MUBs, we show that the maximal quantum violation of the proposed Bell inequality device independently certifies that the measurements satisfy an operational definition of mutual unbiasedness as well as that the shared state is essentially a maximally entangled state of local dimension d. Similarly, in the case of SICs, we find that the maximal quantum violation device independently certifies that the measurements satisfy an analogous operational definition of symmetric informational completeness. Moreover, we also show that our Bell inequalities are useful in two practically relevant tasks. For the case of MUBs, we consider a scheme for device-independent quantum key distribution and prove a key rate of $\log d$ bits, which is optimal for any protocol that extracts key from a d-outcome measurement. For SICs, we construct a scheme for device-independent random number generation. For two-dimensional SICs, we obtain the largest amount of randomness possible for any protocol based on qubits. For three-dimensional SICs, we obtain more randomness than can be obtained in any protocol based on projective measurements and quantum systems of dimension up to seven. For low dimensions, we numerically show that both protocols are robust to noise, which is imperative to any experiment. The implementation of these two protocols involves performing a Bell-type experiment, estimating the outcome statistics and computing the resulting Bell inequality violation. The efficiency and security of the protocol is then deduced only from the observed Bell inequality violation, i.e., it does not require a complete characterization of the devices. Device-independent protocols can, in principle, be implemented on any experimental platform suitable for Bell nonlocality experiments, such as entangled spins (*63*), entangled photons (*64*, *65*), and entangled atoms (*66*).

RESULTS

Bell inequalities for MUBs

The task of finding Bell inequalities that are maximally violated by MUBs for $d \geq 3$ has been attempted several times (*67*–*70*) but with limited success. The only convincing candidate is the inequality corresponding to $d = 3$ studied in (*67*), and even then, there is only numerical evidence (no analytical proof is known). Some progress has been made in (*60*), which considers the case of prime d and proposes a family of Bell inequalities maximally violated by a specific set of d MUBs in dimension d. These inequalities, however, have two drawbacks: (i) There is no generalization to the case of nonprime d, and (ii) even for the case of prime d, we have no characterization of the quantum realizations that achieve the maximal violation.

In this work, we present a family of Bell inequalities in which the maximal quantum violation is achieved with a maximally entangled state and any pair of d-dimensional MUBs. These Bell inequalities have been constructed so that their maximal quantum violation can be computed analytically, which then enables us to obtain a detailed characterization of the optimal realizations. As a result we find a previously unidentified, intermediate form of device-independent certification.

We formally define a pair of MUBs as two orthonormal bases on a d-dimensional Hilbert space $\mathbb{C}^d$, namely, $\{|e_j\rangle\}_{j=1}^d$ and $\{|f_k\rangle\}_{k=1}^d$, with the property that

$$|\langle e_j|f_k\rangle|^2 = \frac{1}{d} \tag{1}$$

for all j and k. The constant on the right-hand side is merely a consequence of the two bases being normalized. To this end, consider a bipartite Bell scenario parameterized by an integer $d \geq 2$. Alice randomly receives one of d^2 possible inputs labeled by $x \equiv x_1x_2 \in [d]^2$ (where $[s] \equiv \{1, \ldots, s\}$) and produces a ternary output labeled by $a \in \{1,2,\perp\}$. Bob receives a random binary input labeled by $y \in \{1,2\}$ and produces a d-valued output labeled by $b \in [d]$. The joint probability distribution in the Bell scenario is denoted by $p(a, b|x, y)$, and the scenario is illustrated in Fig. 1.

To make our choice of Bell functional transparent, we will phrase it as a game in which Alice and Bob collectively win or lose points. If Alice outputs $a = \perp$, then no points will be won or lost. If she outputs $a \in \{1,2\}$, then points will be won or lost if $b = x_y$. More specifically, Alice and Bob win a point if $a = y$ and lose a point if $a = \bar{y}$, where the bar sign flips the value of $y \in \{1,2\}$. This leads to the score

$$\mathcal{R}_d^{\mathrm{MUB}} \equiv \sum_{x,y} p(a = y, b = x_y|x,y) - p(a = \bar{y}, b = x_y|x,y) \tag{2}$$

where the sum goes over $x = x_1x_2 \in [d]^2$ and $y \in \{1,2\}$.

At this point, the outcome $a = \perp$ might seem artificial, so let us show why it plays a crucial role in the construction of the game. To this end, we use intuition based on the hypothetical case in which Alice and Bob share a maximally entangled state

$$|\psi_d^{\max}\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k,k\rangle \tag{3}$$

The reason that we consider the maximally entangled state is that we aim to tailor the Bell inequalities so that this state is optimal. Then, we would like to ensure that Alice, via her measurement and for her outcomes $a \in \{1,2\}$, remotely prepares Bob in a pure state. This would allow Bob to create stronger correlations as compared to the case of Alice remotely preparing his system is a mixed state. Hence, this corresponds to Alice's outcomes $a \in \{1,2\}$ being represented by rank-one projectors. Since the subsystems of $|\psi_d^{\max}\rangle$ are maximally mixed, it follows that $(a = 1|x) = p(a = 2|x) = 1/d \ \forall x$. Thus, we want to motivate Alice to use a strategy in which she outputs $a = \perp$ with probability $p(a = \perp|x) = 1 - 2/d$. Our tool for this purpose is to introduce a penalty. Specifically, whenever Alice decides to output $a \in \{1,2\}$, she is penalized by losing γ_d points. Thus, the total score (the Bell functional) reads

$$\mathcal{S}_d^{\mathrm{MUB}} \equiv \mathcal{R}_d^{\mathrm{MUB}} - \gamma_d \sum_x (p(a = 1|x) + p(a = 2|x)) \tag{4}$$

Now, outputting $a \in \{1,2\}$ not only contributes toward $\mathcal{R}_d^{\mathrm{MUB}}$ but also causes a penalty γ_d. Therefore, we expect to see a trade-off between γ_d and the rate at which Alice outputs $a = \perp$. We must suitably choose γ_d such that Alice's best strategy is to output $a = \perp$ with (on average over x) the desired probability $p(a = \perp|x) = 1 - 2/d$. This accounts for the intuition that leads us to the following Bell inequalities for MUBs.

Theorem II.1 (Bell inequalities for MUBs). The Bell functional $\mathcal{S}_d^{\mathrm{MUB}}$ in Eq. 4 with

$$\gamma_d = \frac{1}{2}\sqrt{\frac{d-1}{d}} \tag{5}$$

obeys the tight local bound

$$\mathcal{S}_d^{\mathrm{MUB}} \overset{\mathrm{LHV}}{\leq} 2(d-1)\left(1 - \frac{1}{2}\sqrt{\frac{d-1}{d}}\right) \tag{6}$$

and the quantum bound

$$\mathcal{S}_d^{\mathrm{MUB}} \overset{\mathrm{Q}}{\leq} \sqrt{d(d-1)} \tag{7}$$

Moreover, the quantum bound can be saturated by sharing a maximally entangled state of local dimension d and Bob performing measurements in any two MUBs.

Proof. A complete proof is presented in the Supplementary Materials (section S1A). The essential ingredient to obtain the bound in Eq. 7 is the Cauchy-Schwarz inequality. Furthermore, for local models, by inspecting the symmetries of the Bell functional $\mathcal{S}_d^{\mathrm{MUB}}$, one finds that the local bound can be attained by Bob always outputting $b = 1$. This greatly simplifies the evaluation of the bound in Eq. 6.

To see that the bound in Eq. 7 can be saturated in quantum theory, let us evaluate the Bell functional for a particular quantum realization. Let $|\psi\rangle$ be the shared state, $\{P_{x_1}\}_{x_1=1}^d$ and $\{Q_{x_2}\}_{x_2=1}^d$ be the measurement operators of Bob corresponding to $y = 1$ and $y = 2$, respectively, and A_x be the observable of Alice defined as the difference between Alice's outcome-one and outcome-two measurement operators, i.e., $A_x = A_x^1 - A_x^2$. Then, the Bell functional reads

$$\mathcal{S}_d^{\mathrm{MUB}} = \sum_x \langle\psi| A_x \otimes (P_{x_1} - Q_{x_2}) - \gamma_d (A_x^1 + A_x^2) \otimes \mathbb{1} |\psi\rangle \tag{8}$$

Now, we choose the maximally entangled state of local dimension d, i.e., $|\psi\rangle = |\psi_d^{\max}\rangle$, and define Bob's measurements as rank-one projectors $P_{x1} = |\phi_{x1}\rangle\langle\phi_{x1}|$ and $Q_{x2} = |\varphi_{x2}\rangle\langle\varphi_{x2}|$, which correspond to MUBs, i.e., $|\langle\phi_{x1}|\varphi_{x2}\rangle|^2 = 1/d$. Last, we choose Alice's observables as $A_x = \sqrt{d/(d-1)}\,(P_{x_1} - Q_{x_2})^{\mathrm{T}}$, where the prefactor ensures the correct normalization and $^{\mathrm{T}}$ denotes the transpose in the standard basis. Note that A_x is a rank-two operator; the corresponding measurement operator A_x^1 (A_x^2) is a rank-one projector onto the eigenvector of A_x associated to the positive (negative) eigenvalue. Since the subsystems of $|\psi_d^{\max}\rangle$ are maximally mixed, this implies $\langle\psi_d^{\max}|(A_x^1 + A_x^2) \otimes 1 |\psi_d^{\max}\rangle = 2/d$. Inserting all this

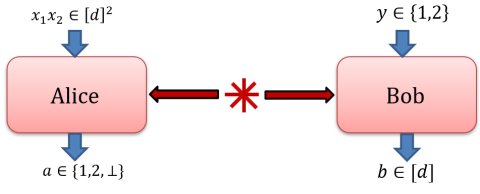

Fig. 1. Bell scenario for two MUBs of dimension *d*. Alice receives one of d^2 inputs and produces a ternary output, while Bob receives a binary input and produces a d-valued output.

into the above quantum model and exploiting the fact that for any linear operator O, we have $O \otimes \mathbb{1} \,|\, \psi_d^{\max}\rangle = \mathbb{1} \otimes O^{\mathrm{T}} \,|\, \psi_d^{\max}\rangle$, we straightforwardly saturate the bound in Eq. 7.

We remark that for the case of $d = 2$ one could also choose $\gamma_2 = 0$ and retain the property that qubit MUBs are optimal. In this case, the marginal term is not necessary because in the optimal realization, Alice never outputs $\perp$. Then, the quantum bound becomes $2\sqrt{2}$, and the local bound becomes 2. The resulting Bell inequality resembles the Clauser-Horne-Shimony-Holt (CHSH) inequality (*71*) not only because it gives the same local and quantum values but also because the optimal realizations coincide. More specifically, the measurements of Bob are precisely the optimal CHSH measurements, whereas the four measurements of Alice correspond to two pairs of optimal CHSH measurements.

Device-independent certification of mutual unbiasedness

Theorem II establishes that a pair of MUBs of any dimension can generate a maximal quantum violation in a Bell inequality test. We now turn to the converse matter, namely, that of device-independent certification. Specifically, given that we observe the maximal quantum violation, i.e., equality in Eq. 7, what can be said about the shared state and the measurements? Since the measurement operators can only be characterized on the support of the state, to simplify the notation, let us assume that the marginal states of Alice and Bob are full rank. (Note that this is not a physical assumption but a mathematical convention that simplifies the notation in the rest of this work. Whenever the marginal state is not full rank, the local Hilbert space naturally decomposes as a direct sum of two terms, where the state is only supported on one of them. The measurement operators can only be characterized on the support of the state, and that is precisely what we achieve. This convention allows us to only write out the part that can be characterized and leave out the rest.)

Theorem II.2 (Device-independent certification). The maximal quantum value of the Bell functional $\mathcal{S}_d^{\mathrm{MUB}}$ in Eq. 4 implies that (i) there exist local isometries that allow Alice and Bob to extract a maximally entangled state of local dimension d, and (i) if the marginal state of Bob is full rank, the two d-outcome measurements that he performs satisfy the relations

$$P_a \;=\; d\,P_a\,Q_b\,P_a \text{ and } Q_b \;=\; d\,Q_b\,P_a\,Q_b \tag{9}$$

for all a and b.

Proof. The proof is detailed in the Supplementary Materials (section S1A). Here, we briefly summarize the part concerning Bob's measurements. Since the Cauchy-Schwarz inequality is the main tool for proving the quantum bound in Eq. 7, saturating it implies that the Cauchy-Schwarz inequality is also saturated. This allows us to deduce that the measurements of Bob are projective, and moreover, we obtain the following optimality condition

$$A_x \otimes \mathbb{1} \,|\, \psi\rangle = \mathbb{1} \otimes \sqrt{\frac{d}{d-1}}(P_{x_1} - Q_{x_2}) \,|\, \psi\rangle \tag{10}$$

for all $x_1, x_2 \in [d]$ where the factor $\sqrt{d/(d-1)}$ can be regarded as a normalization. Since we do not attempt to certify the measurements of Alice, we can, without loss of generality, assume that they are projective. This implies that the spectrum of A_x only contains $\{+1, -1, 0\}$ and therefore $(A_x)^3 = A_x$. This allows us to obtain a relation that only contains Bob's operators. Tracing out Alice's system and subsequently eliminating the marginal state of Bob (it is assumed to be full rank) leads to

$$P_{x_1} - Q_{x_2} \;=\; \frac{d}{d-1}(P_{x_1} - Q_{x_2})^3 \tag{11}$$

Expanding this relation and then using projectivity and the completeness of measurements, one recovers the result in Eq. 9.

We have shown that observing the maximal quantum value of $\mathcal{S}_d^{\mathrm{MUB}}$ implies that the measurements of Bob satisfy the relations given in Eq. 9. It is natural to ask whether a stronger conclusion can be derived, but the answer turns out to be negative. In the Supplementary Materials (section S1B), we show that any pair of d-outcome measurements (acting on a finite-dimensional Hilbert space) satisfying the relations in Eq. 9 is capable of generating the maximal Bell inequality violation. For $d = 2,3$, the relations given in Eq. 9 imply that the unknown measurements correspond to a direct sum of MUBs (see section S2C) and since, in these dimensions, there exists only a single pair of MUBs (up to unitaries and complex conjugation), our results imply a self-testing statement of the usual kind. However, since, in higher dimensions, not all pairs of MUBs are equivalent (*72*), our certification statement is less informative than the usual formulation of self-testing. In other words, our inequalities allow us to self-test the quantum state, but we cannot completely determine the measurements [see (*73*, *74*) for related results]. Note that we could also conduct a device-independent characterization of the measurements of Alice. Equation 61 from the Supplementary Materials enables us to relate the measurements of Alice to the measurements of Bob, which we have already characterized. However, since we do not expect the observables of Alice to satisfy any simple algebraic relations and since they are not directly relevant for the scope of this work (namely, MUBs and SICs), we do not pursue this direction.

The certification provided in Theorem II.2 turns out to be sufficient to determine all the probabilities $p(a, b \mid x, y)$ that arise in the Bell experiment (see section S1C), which means that the maximal quantum value of $\mathcal{S}_d^{\mathrm{MUB}}$ is achieved by a single probability distribution. Because of the existence of inequivalent pairs of MUBs in certain dimensions (e.g., for $d = 4$), this constitutes the first example of an extremal point of the quantum set, which admits inequivalent quantum realizations. Recall that the notion of equivalence that we use is precisely the one that appears in the context of self-testing, i.e., we allow for additional degrees of freedom, local isometries, and a transposition.

It is important to understand the relation between the condition given in Eq. 9 and the concept of MUBs. Naturally, if $\{P_a\}_{a=1}^d$ and $\{Q_b\}_{b=1}^d$ are d-dimensional MUBs, then the relations (Eq. 9) are satisfied. However, there exist solutions to Eq. 9 that are neither MUBs nor direct sums thereof. While, as mentioned above, for $d = 2,3$, one can show that any measurements satisfying the relations (Eq. 9) must correspond to a direct sum of MUBs, this is not true in general. For $d = 4,5$, we have found explicit examples of measurement operators satisfying Eq. 9, which cannot be written as a direct sum of MUBs. They cannot even be transformed into a pair of MUBs via a completely positive unital map (see section S2 for details). These results beg the crucial question: How should one interpret the condition given in Eq. 9?

To answer this question, we resort to an operational formulation of what it means for two measurements to be mutually unbiased. An operational approach must rely on observable quantities (i.e., probabilities), as opposed to algebraic relations between vectors or

operators. This notion, which we refer to as mutually unbiased measurements (MUMs), was recently formalized by Tasca *et al.* (*75*). Note that in what follows, we use the term "eigenvector" to refer to eigenvectors corresponding to nonzero eigenvalues.

Definition II.3 (MUMs). We say that two n-outcome measurements $\{P_a\}_{a=1}^n$ and $\{Q_b\}_{b=1}^n$ are mutually unbiased if they are projective and the following implications hold

$$\begin{aligned} \langle\psi|P_a|\psi\rangle = 1 \;\Rightarrow\; \langle\psi|Q_b|\psi\rangle = \frac{1}{n} \\ \langle\psi|Q_b|\psi\rangle = 1 \;\Rightarrow\; \langle\psi|P_a|\psi\rangle = \frac{1}{n} \end{aligned} \tag{12}$$

for all a and b. That is, two projective measurements are mutually unbiased if the eigenvectors of one measurement give rise to a uniform outcome distribution for the other measurement.

Note that this definition precisely captures the intuition behind MUBs without the need to specify the dimension of the underlying Hilbert space. MUMs admit a simple algebraic characterization.

Theorem II.4. Two n-outcome measurements $\{P_a\}_{a=1}^n$ and $\{Q_b\}_{b=1}^n$ are mutually unbiased if and only if

$$\mathrm{P}_a \;=\; n P_a Q_b P_a \; and \; Q_b \;=\; n Q_b P_a Q_b \tag{13}$$

for all a and b.

Proof. Let us first assume that the algebraic relations hold. By summing over the middle index, one finds that both measurements are projective. Moreover, if $|\psi\rangle$ is an eigenvector of P_a, then $\langle\psi|Q_b|\psi\rangle = \langle\psi|P_aQ_bP_a|\psi\rangle = \frac{1}{n}\langle\psi|P_a|\psi\rangle = \frac{1}{n}$

By symmetry, the analogous property holds if $|\psi\rangle$ is an eigenvector of Q_b. Conversely, let us show that MUMs must satisfy the above algebraic relations. Since $\Sigma_a P_a = \mathbb{1}$, we can choose an orthonormal basis of the Hilbert space composed only of the eigenvectors of the measurement operators. Let $\{|e_j^a\rangle\}_{a,j}$ be an orthonormal basis, where $a \in [n]$ tells us which projector the eigenvector corresponds to and j labels the eigenvectors within a fixed projector (if P_a has finite rank, then $j \in [\mathrm{tr}\, P_a]$; otherwise, $j \in \mathbb{N}$). By construction, for such a basis, we have

$P_a|e_j^{a'}\rangle = \delta_{aa'}|e_j^a\rangle$. To show that $P_a = nP_aQ_bP_a$, it suffices to show that the two operators have the same coefficients in this basis. Since

$$\left\langle e_j^{a'}|nP_aQ_bP_a|e_k^{a''}\right\rangle = n\delta_{aa'}\delta_{aa''}\left\langle e_j^a|Q_b|e_k^a\right\rangle \tag{14}$$

$$\left\langle e_j^{a'}|P_a|e_k^{a''}\right\rangle = \delta_{aa'}\delta_{aa''}\delta_{jk} \tag{15}$$

it suffices to show that $n\langle e_j^a|Q_b|e_k^a\rangle = \delta_{jk}$. For $j = k$, this is a direct consequence of the definition in Eq. 12. To prove the other case, define $|\phi_\theta\rangle = (|e_j^a\rangle + e^{i\theta}|e_k^a\rangle)/\sqrt{2}$, for $\theta \in [0,2\pi)$. Since $P_a\,|\,\phi_\theta\rangle = |\,\phi_\theta\rangle$, we have $\langle\phi_\theta|Q_b|\phi_\theta\rangle = 1/n$. Writing this equality out gives

$$\frac{1}{n} \;=\; \frac{1}{2}\left(\frac{2}{n} + e^{i\theta}\langle e_j^a|Q_b|e_k^a\rangle + e^{-i\theta}\langle e_k^a|Q_b|e_j^a\rangle\right) \tag{16}$$

Choosing $\theta = 0$ implies that the real part of $\langle e_j^a|Q_b|e_k^a\rangle$ vanishes, while $\theta = \pi/2$ implies that the imaginary part vanishes. Proving the relation $Q_b = nQ_bP_aQ_b$ proceeds in an analogous fashion.

Theorem II.4 implies that the maximal violation of the Bell inequality for MUBs certifies precisely the fact the Bob's measurements are mutually unbiased. To provide further evidence that MUMs constitute the correct device-independent generalization of MUBs, we give two specific situations in which the two objects behave in the same manner.

Maassen and Uffink (*16*) considered a scenario in which two measurements (with a finite number of outcomes) are performed on an unknown state. Their famous uncertainty relation provides a state-independent lower bound on the sum of the Shannon entropies of the resulting distributions. While the original result only applies to rank-one projective measurements, a generalization to nonprojective measurements reads (*76*)

$$H(P) + H(Q) \geq -\log c \tag{17}$$

where H denotes the Shannon entropy and $c = \max_{a,b} \| \sqrt{P_a}\sqrt{Q_b} \|^2$, where $\| \cdot \|$ is the operator norm. If we restrict ourselves to rank-one projective measurements on a Hilbert space of dimension d, then one finds that the largest uncertainty, corresponding to $c = 1/d$, is obtained only by MUBs. It turns out that precisely the same value is achieved by any pair of MUMs with d outcomes regardless of the dimension of the Hilbert space

$$\begin{aligned} c \;&=\; \max_{a,b} \|\sqrt{P_a}\sqrt{Q_b}\|^2 \;=\; \max_{a,b} \|P_aQ_b\|^2 \\ &= \max_{a,b} \|P_aQ_bP_a\| = \max_a \|P_a/d\| = \frac{1}{d} \end{aligned} \tag{18}$$

A closely related concept is that of measurement incompatibility, which captures the phenomenon that two measurements cannot be performed simultaneously on a single copy of a system. The extent to which two measurements are incompatible can be quantified, e.g., by so-called incompatibility robustness measures (*77*). In the Supplementary Materials (section S2D), we show that according to these measures, MUMs are exactly as incompatible as MUBs. Moreover, we can show that for the so-called generalized incompatibility robustness (*78*), MUMs are among the most incompatible pairs of d-outcome measurements.

Application: Device-independent quantum key distribution

The fact that the maximal quantum violation of the Bell inequalities introduced above requires a maximally entangled state and MUMs and, moreover, that it is achieved by a unique probability distribution suggests that these inequalities might be useful for device-independent quantum information processing. In the task of quantum key distribution (*3*, *17*, *18*), Alice and Bob aim to establish a shared dataset (a key) that is secure against a malicious eavesdropper. Such a task requires the use of incompatible measurements, and MUBs in dimension $d = 2$ constitute the most popular choice. Since, in the ideal case, the measurement outcomes of Alice and Bob that contribute to the key should be perfectly correlated, most protocols are based on maximally entangled states. In the device-independent approach to quantum key distribution, the amount of key and its security is deduced from the observed Bell inequality violation.

We present a proof-of-principle application to device-independent quantum key distribution based on the quantum nonlocality witnessed through the Bell functional in Eq. 4. In the ideal case, Alice and Bob follow the strategy that gives them the maximal violation, i.e., they share a maximally entangled state of local dimension d and Bob measures two MUBs. To generate the key, we provide Alice with

an extra setting that produces outcomes that are perfectly correlated with the outcomes of the first setting of Bob. This will be the only pair of settings from which the raw key will be extracted, and let us denote them by $x = x^*$ and $y = y^* = 1$. In most rounds of the experiment, Alice and Bob choose these settings and therefore contribute toward the raw key. However, to ensure security, a small number of rounds is used to evaluate the Bell functional. In these rounds, which are chosen at random, Alice and Bob randomly choose their measurement settings. Once the experiment is complete, the resulting value of the Bell functional is used to infer the amount of secure raw key shared between Alice and Bob. The raw key can then be turned into the final key by standard classical postprocessing. For simplicity, we consider only individual attacks, and moreover, we focus on the limit of asymptotically many rounds in which fluctuations due to finite statistics can be neglected.

The key rate, K, can be lower bounded by (*79*)

$$K \geq -\log\left(P_g^{\beta}\right) - H(B_{y^*}|A_{x^*}) \tag{19}$$

where P_g^{β} denotes the highest probability that the eavesdropper can correctly guess Bob's outcome when his setting is y^* given that the Bell inequality value β was observed, and $H(\cdot\,|\,\cdot)$ denotes the conditional Shannon entropy. The guessing probability P_g^{β} is defined as

$$P_g^{\beta} \equiv \sup\left\{ \sum_{c=1}^{d} \langle \psi_{ABE} | \mathbb{1} \otimes P_c \otimes E_c | \psi_{ABE} \rangle \right\} \tag{20}$$

where $\{E_c\}_{c=1}^{d}$ is the measurement used by the eavesdropper to produce her guess, the expression inside the curly braces is the probability that her outcome is the same as Bob's for a particular realization, and the supremum is taken over all quantum realizations (the tripartite state and measurements of all three parties) compatible with the observed Bell inequality value β.

Let us first focus on the key rate in a noise-free scenario, i.e., in a scenario in which $\mathcal{S}_d^{\mathrm{MUB}}$ attains its maximal value. Then, one straightforwardly arrives at the following result.

Theorem II.5 (Device-independent key rate). In the noiseless case, the quantum key distribution protocol based on $\mathcal{S}_d^{\mathrm{MUB}}$ achieves the key rate of

$$K = \log d \tag{21}$$

for any integer $d \geq 2$.

Proof. In the noiseless case, Alice and Bob observe exactly the correlations predicted by the ideal setup. In this case, the outcomes for settings (x^*, y^*) are perfectly correlated, which implies that $H(B_{y^*}|A_{x^*}) = 0$. Therefore, the only nontrivial task is to bound the guessing probability.

Since the actions of the eavesdropper commute with the actions of Alice and Bob, we can assume that she performs her measurement first. If the probability of the eavesdropper observing outcome $c \in [d]$, which we denote by $p(c)$, is nonzero, then the (normalized) state of Alice and Bob conditioned on the eavesdropper observing that outcome is given by

$$\rho_{AB}^{(c)} = \frac{1}{p(c)} \mathrm{tr}_C\left[(\mathbb{1} \otimes \mathbb{1} \otimes E_c)\,|\,\psi_{ABE}\rangle\langle\psi_{ABE}\,|\right] \tag{22}$$

Now, Alice and Bob share one of the postmeasurement states $\rho_{AB}^{(c)}$, and when they perform their Bell inequality test, they will obtain different distributions depending on c, which we write as $p_c(a, b \mid x, y)$. However, since the statistics achieve the maximal quantum value of $\mathcal{S}_d^{\mathrm{MUB}}$ and we have previously shown that the maximal quantum value is achieved by a single probability point, all the probability distributions $p_c(a, b \mid x, y)$ must be the same. Moreover, we have shown that for this probability point, the marginal distribution of outcomes on Bob's side is uniform over $[d]$ for both inputs. This implies that

$$P_g = \sum_{c=1}^{d} p(c)\, p_c(b = c \,|\, y = 1) = \frac{1}{d} \tag{23}$$

because $p_c(b = c \,|\, y = 1) = p(b = c \,|\, y = 1) = \frac{1}{d}$ for all c.

We remark that the argument above is a direct consequence of a more general result that states that if a bipartite probability distribution is a nonlocal extremal point of the quantum set, then no external party can be correlated with the outcomes (*80*). The obtained key rate is the largest possible for general setups in which the key is generated from a d-outcome measurement. In addition, the key rate is optimal for all protocols based on a pair of entangled d-dimensional systems subject to projective measurements. This follows from the fact that projective measurements in $\mathbb{C}^d$ cannot have more than d outcomes. It has recently been shown that the same amount of randomness can be generated using a modified version of the Collins-Gisin-Linden-Massar-Popescu inequalities (*61*), but note that the measurements used there do not correspond to MUBs (except for the special case of $d = 2$).

Let us now depart from the noise-free case and estimate the key rate in the presence of noise. To ensure that both the guessing probability and the conditional Shannon entropy can be computed in terms of a single noise parameter, we have to introduce an explicit noise model. We use the standard approach in which the measurements remain unchanged, while the maximally entangled state is replaced with an isotropic state given by

$$\rho_v = v \left|\psi_d^{\max}\right\rangle\left\langle\psi_d^{\max}\right| + \frac{1 - v}{d^2}\mathbb{1} \tag{24}$$

where $v \in [0,1]$ is the visibility of the state. Using this state and the ideal measurements for Alice and Bob, the relation between v and $\mathcal{S}_d^{\mathrm{MUB}}$ can be easily derived from Eq. 8, namely

$$v = \frac{1}{2}\left(1 + \frac{\mathcal{S}_d^{\mathrm{MUB}}}{\sqrt{d(d-1)}}\right) \tag{25}$$

Using this formula, we also obtain the value of $H(B_{y^*} \mid A_{x^*})$ as a function of the Bell violation. The remaining part of Eq. 19 is the guessing probability (Eq. 20). In the case of $d = 3$, we proceed to bound this quantity through semidefinite programming.

Concretely, we implement the three-party semidefinite relaxation (*81*) of the set of quantum correlations at local level 1 (we attribute one operator to each outcome of Bob and the eavesdropper but only take into account the first two outcomes of Alice). This results in a moment matrix of size 532×532 with 15,617 variables. The guessing probability is directly given by the sum of three elements of the moment matrix. It can then be maximized under the constraints that the value of the Bell functional $\mathcal{S}_3^{\mathrm{MUB}}$ is fixed and the moment matrix is positive semidefinite. However, we notice that this problem is invariant under the following relabeling: $b \to \pi(b)$ for $y = 1$, $c \to \pi(c)$, and $x_1 \to \pi(x_1)$, where $\pi \in S_3$ is a permutation of three elements.

Therefore, it is possible to simplify this semidefinite program by requiring the matrix to be invariant under the group action of S_3 on the moment matrix (i.e., it is a Reynolds matrix) (*43*, *82*, *83*). This reduces the number of free variables in the moment matrix to 2823. With the Self-Dual Minimization (SeDuMi) (*84*) solver, this lowers the precision (1.1×10^{-6} instead of 8.4×10^{-8}) but speeds up the computation (155 s instead of 8928 s) and requires less memory (0.1 gigabytes instead of 5.5 gigabytes). For the maximal value of $\mathcal{S}_d^{\mathrm{MUB}}$, we recover the noise-free result of $K = \log 3$ up to the fifth digit. In addition, we have a key rate of at least one bit when $\mathcal{S}_d^{\mathrm{MUB}} \gtrsim 2.432$ and a nonzero key rate when $\mathcal{S}_d^{\mathrm{MUB}} \gtrsim 2.375$. The latter is close to the local bound, which is $\mathcal{S}_d^{\mathrm{MUB}} \approx 2.367$. The resulting lower bound on the key rate as a function of the Bell inequality violation is plotted in Fig. 2.

Nonlocality for symmetric informational completeness

We now shift our focus from MUBs to SICs. We construct Bell inequalities whose maximal quantum violations are achieved with SICs. We formally define a SIC as a set of d^2 unit vectors in $\mathbb{C}^d$, namely, $\{|r_j\rangle\}_{j=1}^{d^2}$, with the property that

$$|\langle r_j|r_k\rangle|^2 = \frac{1}{d+1} \tag{26}$$

for all $j \neq k$, where the constant on the right-hand side is fixed by normalization. The reason for there being precisely d^2 elements in a SIC is that this is the largest number of unit vectors in $\mathbb{C}^d$ that could possibly admit the uniform overlap property (Eq. 26). Moreover, we formally distinguish between a SIC as the presented set of rank-one projectors and a SIC-POVM (positive operator-valued measure), which is the generalized quantum measurement with d^2 possible outcomes corresponding to the subnormalized projectors $\left\{\frac{1}{d}|r_k\rangle\langle r_k|\right\}_{k=1}^{d^2}$.

Since the treatment of SICs in Bell nonlocality turns out to be more challenging than for the case of MUBs, we first establish the relevance of SICs in a simplified Bell scenario subject to additional constraints. This serves as a stepping stone to a subsequent relaxation, which gives a standard (unconstrained) Bell inequality for SICs. We then focus on the device-independent certification power of these inequalities, which leads us to an operational notion of symmetric informational completeness. Last, we extend the Bell inequalities so that their maximal quantum violations are achieved with both projectors forming SICs and a single generalized measurement corresponding to a SIC-POVM.

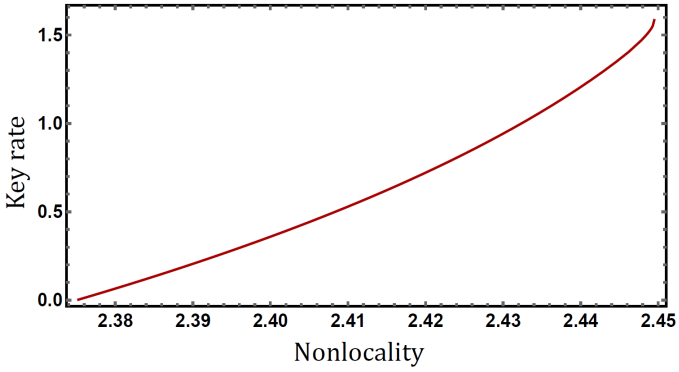

Fig. 2. Lower bound on the key rate *K* in the asymptotic limit versus the value of the Bell functional $\mathcal{S}_3^{\mathrm{MUB}}$.

Stepping stone: Quantum correlations for SICs

Consider a Bell scenario, parameterized by an integer $d \geq 2$, involving two parties Alice and Bob who share a physical system. Alice receives an input labeled by a tuple (x_1, x_2) representing one of $\binom{d^2}{2}$ possible inputs, which we collectively refer to as $x = x_1x_2$. The tuple is randomly taken from the set $\mathrm{Pairs}(d^2) \equiv \{x \mid x_1, x_2 \in [d^2] \text{ and } x_1 < x_2\}$. Alice performs a measurement on her part of the shared system and produces a ternary output labeled by $a \in \{1,2,\perp\}$. Bob receives an input labeled by $y \in [d^2]$, and the associated measurement produces a binary outcome labeled by $b \in \{1,\perp\}$. The joint probability distribution is denoted by $p(a, b \mid x, y)$, and the Bell scenario is illustrated in Fig. 3.

Similar to the case of MUBs, to make our choice of Bell functional transparent, we phrase it as a game played by Alice and Bob. We imagine that their inputs are supplied by a referee, who promises to provide $x = x_1x_2$ and y such that either $y = x_1$ or $y = x_2$. Similar to the previous game, Alice can output $a = \perp$ to ensure that no points are won or lost. However, in this game also, Bob can ensure that no points are won or lost by outputting $b = \perp$. If neither of them outputs $\perp$, then a point is either won or lost. Specifically, when $a = 1$, a point is won if $y = x_1$ (and lost otherwise), whereas if $a = 2$, then a point is won if $y = x_2$ (and lost otherwise). Let us remark that in this game, Bob's only role is to decide whether, in a given round, points can be won/lost or not. For this game, the total number of points (the Bell functional) reads

$$\begin{aligned}\mathcal{R}_d^{\mathrm{SIC}} \equiv \sum_{x_1<x_2} \big(&p(1,1|x,x_1) - p(1,1|x,x_2) \\ &+ p(2,1|x,x_2) - p(2,1|x,x_1)\big)\end{aligned} \tag{27}$$

where the sum is taken over all $x \in \mathrm{Pairs}(d^2)$.

Let us now impose additional constraints on the marginal distributions of the outputs. More specifically, we require that

$$\begin{aligned}&\forall x: p(a=1|x) + p(a=2|x) = \frac{2}{d} \\ &\forall y: p(b=1|y) = \frac{1}{d}\end{aligned} \tag{28}$$

The intuition behind these constraints is analogous to that discussed for the case of MUBs. Namely, we imagine that Alice and Bob perform measurements on a maximally entangled state of local dimension d. Then, we wish to fix the marginals such that the measurements of Alice (Bob) for the outcomes $a \in \{1,2\}$ ($b = 1$) remotely prepare Bob's (Alice's) subsystem in a pure state. This corresponds to the marginals $p(a = 1 \mid x) = p(a = 2 \mid x) = p(b = 1 \mid x) = 1/d$, which is reflected in the marginal constraints in Eq. 28. We remark

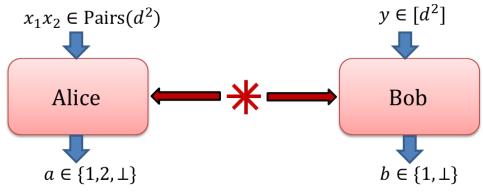

Fig. 3. Bell scenario for SICs of dimension *d*. Alice receives one of $\binom{d^2}{2}$ inputs and returns a ternary outcome, while Bob receives one of d^2 inputs and returns a binary outcome.

that imposing these constraints simplifies both the intuitive understanding of the game and the derivation of the results below. However, it merely serves as a stepping stone to a more general subsequent treatment in which the constraints (Eq. 28) will be removed.

To write the value of the Bell functional of a quantum realization, let us introduce two simplifications. The measurement operators of Alice are denoted by $\{A_x^a\}$, and as before, it is convenient to work with the observables defined as $A_x = A_x^1 - A_x^2$. The measurements of Bob are denoted by $\{B_y^b\}$, but since they only have two outcomes, all the expressions can be written in terms of a single operator from each input y. In our case, it is convenient to use the outcome-one operator, and for convenience, we will skip the superscript, i.e., we will write $B_y \equiv B_y^1$ for all y. Then, the Bell functional evaluated on a specific quantum realization reads

$$\mathcal{R}_d^{\mathrm{SIC}} = \sum_{x_1<x_2} \langle \psi | A_x \otimes (B_{x_1} - B_{x_2}) | \psi \rangle \tag{29}$$

Note that the Bell functional, in particular, when written in a quantum model, is much reminiscent of the expression $\mathcal{R}_d^{\mathrm{MUB}}$ (Eq. 2) encountered for MUBs, with the key difference that the roles of the inputs and outputs of Bob are swapped. Let us consider a quantum strategy in which Alice and Bob share a maximally entangled state $|\psi_d^{\max}\rangle$. Moreover, Bob's measurements are defined as $B_y = |\phi_y\rangle\langle\phi_y|$, where $\{|\phi_y\rangle\}_{y=1}^{d^2}$ is a set of unit vectors forming a SIC (assuming it exists in dimension d), i.e., $|\langle\phi_y|\phi_{y'}\rangle|^2 = 1/(d+1)$ for all $y \neq y'$. In addition, we define Alice's observables as $A_x = \sqrt{(d+1)/d}\,(B_{x_1} - B_{x_2})^{\mathrm{T}}$, where the prefactor ensures normalization. First, since the subsystems of Alice and Bob are maximally mixed and the outcomes $a \in \{1,2\}$ and $b = 1$ each correspond to rank-one projectors, the marginal constraints in Eq. 28 are satisfied. Using the fact that for any linear operator O we have $O \otimes \mathbb{1} |\psi_d^{\max}\rangle = \mathbb{1} \otimes O^{\mathrm{T}} |\psi_d^{\max}\rangle$, we find that

$$\begin{aligned}\mathcal{R}_d^{\mathrm{SIC}} &= \sqrt{\frac{d+1}{d}} \sum_{x_1<x_2} \langle \psi_d^{\max} | \mathbb{1} \otimes (|\phi_{x_1}\rangle\langle\phi_{x_1}| - |\phi_{x_2}\rangle\langle\phi_{x_2}|)^2 | \psi_d^{\max} \rangle \\ &= \sqrt{\frac{d+1}{d}} \sum_{x_1<x_2} \left(\frac{2}{d} - \frac{2}{d(d+1)} \right) = d(d-1)\sqrt{d(d+1)}\end{aligned} \tag{30}$$

This strategy relying on a maximally entangled state and a SIC achieves the maximal quantum value of $\mathcal{R}_d^{\mathrm{SIC}}$ under the constraints of Eq. 28. In the Supplementary Materials (section S3A), we prove that under these constraints, the tight quantum and no-signaling bounds on $\mathcal{R}_d^{\mathrm{SIC}}$ read

$$\mathcal{R}_d^{\mathrm{SIC}} \overset{\mathrm{Q}}{\leq} d(d-1)\sqrt{d(d+1)} \tag{31}$$

$$\mathcal{R}_d^{\mathrm{SIC}} \overset{\mathrm{NS}}{\leq} d(d^2-1) \tag{32}$$

We remark that SICs are not known to exist in all Hilbert space dimensions. However, their existence in all dimensions is strongly conjectured, and explicit SICs have been found in all dimensions up to 193 (*53*–*55*).

Bell inequalities for SICs

The marginal constraints in Eq. 28 allowed us to prove that the quantum realization based on SICs achieves the maximal quantum value of $\mathcal{R}_d^{\mathrm{SIC}}$. Our goal now is to remove these constraints to obtain a standard Bell functional. Analogously to the case of MUBs, we add marginal terms to the original functional $\mathcal{R}_d^{\mathrm{SIC}}$.

To this end, we introduce penalties for both Alice and Bob. Specifically, if Alice outputs $a \in \{1,2\}$, then they lose α_d points, whereas if Bob outputs $b = 1$, then they lose β_d points. The total number of points in the modified game constitutes our final Bell functional

$$\mathcal{S}_d^{\mathrm{SIC}} \equiv \mathcal{R}_d^{\mathrm{SIC}} - \alpha_d \sum_{x_1<x_2} (p(a=1|x) + p(a=2|x)) - \beta_d \sum_y p(b=1|y) \tag{33}$$

Hence, our aim is to suitably choose the penalties α_d and β_d so that the maximal quantum value of $\mathcal{S}_d^{\mathrm{SIC}}$ is achieved with a strategy that closely mimics the marginal constraints (Eq. 28) and thus maintains the optimality of Bob performing a SIC.

Theorem II.6 (Bell inequalities for SICs). The Bell functional $\mathcal{S}_d^{\mathrm{SIC}}$ in Eq. 33 with

$$\begin{aligned}\alpha_d &= \frac{1-\delta_{d,2}}{2}\sqrt{\frac{d}{d+1}} \\ \beta_d &= \frac{d-2}{2}\sqrt{d(d+1)}\end{aligned} \tag{34}$$

obeys the tight local bound

$$\mathcal{S}_d^{\mathrm{SIC}} \overset{\mathrm{LHV}}{\leq} \begin{cases} 4 & \text{for } d = 2 \\ d^2(d-1) - d(d^2-d-1)\sqrt{\frac{d}{d+1}} & \text{for } d \geq 3 \end{cases} \tag{35}$$

and the quantum bound

$$\mathcal{S}_d^{\mathrm{SIC}} \overset{\mathrm{Q}}{\leq} \frac{d+2\delta_{d,2}}{2}\sqrt{d(d+1)} \tag{36}$$

Moreover, the quantum bound is tight and can be saturated by sharing a maximally entangled state of local dimension d and choosing Bob's outcome-one projectors to form a SIC.

Proof. The proof is presented in the Supplementary Materials (section S3B). To obtain the quantum bound in Eq. 36, the key ingredients are the Cauchy-Schwarz inequality and semidefinite relaxations of polynomial optimization problems. To derive the local bound in Eq. 35, the key observation is that the symmetries of the Bell functional allow us to notably simplify the problem.

The fact that the quantum bound is saturated by a maximally entangled state and Bob performing a SIC can be seen immediately from the previous discussion that led to Eq. 30. With that strategy, we find $\mathcal{R}_d^{\mathrm{SIC}} = d(d-1)\sqrt{d(d+1)}$. Since it also respects $(a=1|x) + p(a=2|x) = 2/d\ \forall x$, as well as $p(b=1|y) = 1/d\ \forall y$, a direct insertion into Eq. 33 saturates the bound in Eq. 36. Note that in the limit of $d \to \infty$ both the local bound and the quantum bound grow quadratically in d.

We remark that for the special case of $d = 2$, no penalties are needed to maintain the optimality of SICs (which is why the Kronecker delta appears in Eq. 34). The derived Bell inequality for a qubit SIC (which corresponds to a tetrahedron configuration on the Bloch sphere) can be compared to the so-called elegant Bell inequality (*85*) whose maximal violation is also achieved using the tetrahedron configuration. While we require six settings of Alice and four settings of Bob, the elegant Bell inequality requires only four

settings of Alice and three settings of Bob. However, the additional complexity in our setup carries an advantage when considering the critical visibility of the shared state, i.e., the smallest value of v in Eq. 24 (defining an isotropic state) for which the Bell inequality is violated. The critical visibility for violating the elegant Bell inequality is 86.6%, whereas for our Bell inequality, it is lowered to 81.6%. We remark that on the Bloch sphere, the antipodal points corresponding to the four measurements of Alice and the six measurements of Bob form a cube and a cuboctahedron, respectively, which constitutes an instance of the type of Bell inequalities proposed in (*86*).

Device-independent certification

Theorem II.6 shows that for any dimension $d \geq 2$, we can construct a Bell inequality that is maximally violated by a SIC in that dimension (provided that a SIC exists). Let us now consider the converse question, namely, that of device-independent certification. In analogy with the case of MUBs (Eq. 9), we find a simple description of Bob's measurements.

Theorem II.7 (Device-independent certification). The maximal quantum value of the Bell functional $\mathcal{S}_d^{\mathrm{SIC}}$, provided that the marginal state of Bob is full rank, implies that his measurement operators $\{B_y\}_{y=1}^{d^2}$ are projective and satisfy

$$\sum_y B_y = d\mathbb{1} \tag{37}$$

and

$$\mathrm{B}_y = (d+1)\, B_y B_{y'} B_y \tag{38}$$

for all $y \neq y'$.

A complete proof, which is similar in spirit to the proof of Theorem II.2, can be found in the Supplementary Materials (section S3C). For the special case of $d = 2$, the conclusion can be made even more accurate: The maximal quantum violation of $\mathcal{S}_2^{\mathrm{SIC}}$ implies that Bob's outcome-one projectors are rank-one projectors acting on a qubit whose Bloch vectors form a regular tetrahedron (up to the three standard equivalences used in self-testing).

Similar to the case of MUBs, we face the key question of interpreting the condition in Eq. 38 and its relation to SICs. Again, in analogy with the case of MUBs, we note that the concept of a SIC references the dimension of the Hilbert space, which should not appear explicitly in a device-independent scenario. Hence, we consider an operational approach to SICs, which must rely on observable quantities (i.e., probabilities). This leads us to the following natural definition of a set of projectors being operationally symmetric informationally complete (OP-SIC).

Definition II.8 (Operational SIC). We say that a set of projectors $\{B_a\}_{a=1}^{n^2}$ is OP-SIC if

$$\sum_a B_a = n\mathbb{1} \tag{39}$$

and

$$\langle\psi|B_a|\psi\rangle = 1 \;\Rightarrow\; \langle\psi|B_b|\psi\rangle = \frac{1}{n+1} \tag{40}$$

for all $a \neq b$.

This definition trivially encompasses SICs as special instances of OP-SICs. An argument analogous to the proof of Theorem II.4 shows that this definition is in fact equivalent to the relations given in Eqs. 37 and 38. Hence, in analogy with the case of MUBs, the property of Bob's measurements certified by the maximal violation of our Bell inequality is precisely the notion of OP-SICs.

Adding a SIC-POVM

The Bell inequalities proposed above (Bell functional $\mathcal{S}_d^{\mathrm{SIC}}$) are tailored to sets of rank-one projectors forming a SIC. However, it is also interesting to consider a closely related entity, namely, a SIC-POVM, which is obtained simply by normalizing these projectors, so that they can be collectively interpreted as arising from a single measurement. That is, a SIC-POVM on $\mathbb{C}^d$ is a measurement $\{E_a\}_{a=1}^{d^2}$ in which every measurement operator can be written as $E_a = \frac{1}{d}|\phi_a\rangle\langle\phi_a|$, where the set of rank-one projectors $\{|\phi_a\rangle\langle\phi_a|\}_a$ forms a SIC. Because of the simple relation between SICs and SIC-POVMs, we can extend the Bell inequalities for SICs proposed above such that they are optimally implemented with both a SIC (as before) and a SIC-POVM.

It is clear that to make SIC-POVMs relevant to the Bell experiment, it must involve at least one setting that corresponds to a d^2-outcome measurement. For the Bell scenario previously considered for SICs (see Fig. 3), no such measurement is present. Therefore, we supplement the original Bell scenario by introducing a single additional measurement setting of Alice, labeled by **povm**, which has d^2 outcomes labeled by $a' \in [d^2]$. The modified Bell scenario is illustrated in Fig. 4. We construct the Bell functional $\mathcal{T}_d^{\mathrm{SIC}}$ for this scenario by modifying the previously considered Bell functional $\mathcal{S}_d^{\mathrm{SIC}}$

$$\mathcal{T}_d^{\mathrm{SIC}} = \mathcal{S}_d^{\mathrm{SIC}} - \sum_{y=1}^{d^2} p(a' = y, b = \perp | \mathbf{povm}, y) \tag{41}$$

Hence, whenever Bob outputs "$\perp$" and the outcome associated to the setting **povm** coincides with the input of Bob, a point is lost. Evidently, the largest quantum value of $\mathcal{T}_d^{\mathrm{SIC}}$ is no greater than the largest quantum value of $\mathcal{S}_d^{\mathrm{SIC}}$. For the former to equal the latter, we require that (i) $\mathcal{S}_d^{\mathrm{SIC}}$ reaches its maximal quantum value (which is given in Eq. 36) and (ii) that $(a' = y, b = \perp | \mathbf{povm}, y) = 0\ \forall y$. We have already seen that by sharing a maximally entangled state and Bob's outcome-one projectors $\{B_y\}_y$ forming a SIC, the condition (i) can be satisfied. By normalization, we have that Bob's outcome-$\perp$ projectors are $B_y^{\perp} = \mathbb{1} - B_y$. Again, noting that for any linear operator O we have $O \otimes \mathbb{1}\,|\,\psi_d^{\max}\rangle = \mathbb{1} \otimes O^{\mathrm{T}}\,|\,\psi_d^{\max}\rangle$, observe that if Bob applies $B_y^{\perp}$, then Alice's local state is orthogonal to B_y. Hence, if Alice chooses her POVM $\{E_{a'}\}$, corresponding to the setting **povm**, as the SIC-POVM defined by $E_{a'} = \frac{1}{d}B_{a'}^{\mathrm{T}}$, the probability of finding $a' = y$ vanishes. This satisfies condition (ii). Hence, we conclude that in a general quantum model

$$\mathcal{T}_d^{\mathrm{SIC}} \overset{\mathrm{Q}}{\leq} \frac{d+2\delta_{d,2}}{2}\sqrt{d(d+1)} \tag{42}$$

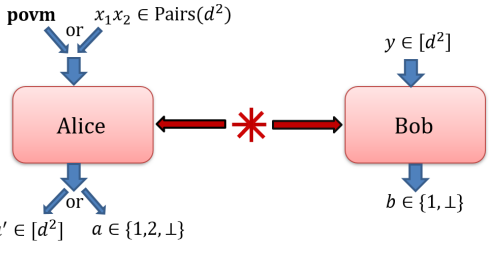

Fig. 4. Bell scenario for SICs and SIC-POVMs of dimension *d*. This scenario modifies the original Bell scenario for SICs (see Fig. 3) by supplying Alice with an extra setting labeled by **povm**, which has d^2 possible outcomes.

and that the bound can be saturated by supplementing the previous optimal realization with a SIC-POVM on Alice's side.

Application: Device-independent quantum random number generation

The fact that the Bell functionals $\mathcal{S}_d^{\mathrm{SIC}}$ and $\mathcal{T}_d^{\mathrm{SIC}}$ achieve their maximal quantum values with a SIC and a SIC-POVM, respectively, opens up the possibility for device-independent quantum information protocols for tasks in which SICs and SIC-POVMs are desirable. We focus on one such application, namely, that of device-independent quantum random number generation (*87*). This is the task of certifying that the data generated by a party cannot be predicted by a malicious eavesdropper. In the device-independent setting, both the amount of randomness and its security are derived from the violation of a Bell inequality.

Nonprojective measurements, such as SIC-POVMs, are useful for this task. The reason is that a Bell experiment implemented with entangled systems of local dimension d and standard projective measurements cannot have more than d outcomes. Consequently, one cannot hope to certify more than $\log d$ bits of local randomness. However, Bell experiment relying on d-dimensional entanglement implemented with (extremal) nonprojective measurements can have up to d^2 outcomes (*88*). This opens the possibility of generating up to 2 $\log d$ bits of local randomness without increasing the dimension of the shared entangled state. Notably, for the case of $d = 2$, such optimal quantum random number generation has been shown using a qubit SIC-POVM (*42*).

Here, we use our Bell inequalities for SIC-POVMs to significantly outperform standard protocols relying on projective measurements on d-dimensional entangled states. To this end, we briefly summarize the scenario for randomness generation. Alice and Bob perform many rounds of the Bell experiment illustrated in Figure 4. Alice will attempt to generate local randomness from the outcomes of her setting labeled by **povm**. In most rounds of the Bell experiment, Alice performs **povm** and records the outcome a'. In a smaller number of rounds, she randomly chooses her measurement setting, and the data are used toward estimating the value of the Bell functional $\mathcal{T}_d^{\mathrm{SIC}}$ defined in Eq. 41. A malicious eavesdropper may attempt to guess Alice's relevant outcome a'. To this end, the eavesdropper may entangle her system with that of Alice and Bob and perform a well-chosen POVM $\{E_c\}_c$ to enhance her guess. In analogy to Eq. 20, the eavesdropper's guessing probability reads

$$P_g^{\beta} \equiv \sup\left\{ \sum_{c=1}^{d^2} \langle \psi_{\mathrm{ABE}} | A_{\mathrm{povm}}^{c} \otimes \mathbb{1} \otimes E_c | \psi_{\mathrm{ABE}} \rangle \right\} \tag{43}$$

where $\{E_c\}_{c=1}^{d^2}$ is the measurement used by the eavesdropper to produce her guess, the expression inside the curly braces is the probability that her outcome is the same as Alice's outcome for the setting **povm** for a particular realization, and the supremum is taken over all quantum realizations (the tripartite state and measurements of all three parties) compatible with the observed Bell inequality violation $\beta = \mathcal{T}_d^{\mathrm{SIC}}$.

We quantify the randomness generated by Alice using the conditional min-entropy $H_{\min}(A_{\mathbf{povm}}|E) = -\log(P_g^{\beta})$. To obtain a device-independent lower bound on the randomness, we must evaluate an upper bound on P_g^{β} for a given observed value of the Bell functional. We saw in the "Application: Device-independent quantum key distribution" section that if the eavesdropper is only trying to guess the outcome of a single measurement setting, we can, without loss of generality, assume that they are only classically correlated with the systems of Alice and Bob. As before, we restrict ourselves to the asymptotic limit of many rounds, in which fluctuations due to finite statistics can be neglected.

To bound the randomness for some given value of $\mathcal{T}_d^{\mathrm{SIC}}$, we use the hierarchy of quantum correlations (*81*). We restrict ourselves to the cases of $d = 2$ and $d = 3$. For the case of $d = 2$, we construct a moment matrix with the operators $\{(\mathbb{1}, A_x) \otimes (\mathbb{1}, B_y) \otimes (\mathbb{1}, E)\} \cup \{A_{\mathrm{povm}} \otimes (\mathbb{1}, B_y, E)\}$, neglecting the $\perp$ outcome. The matrix is of size 361×361 with 10,116 variables. Again, we can make use of symmetry to simplify the semidefinite program. In this case, the following permutation leaves the problem invariant: $x_1 \to \pi(x_1)$, $x_2 \to \pi(x_2)$, $a \to f_\pi(a, x_1, x_2)$, $a' \to \pi(a')$, $y \to \pi(y)$, and $c \to \pi(c)$, where

$$f_\pi(a, x_1, x_2) = \begin{cases} a & \pi(x_1) < \pi(x_2) \\ 2 & \pi(x_1) \geq \pi(x_2) \text{ and } a = 1 \\ 1 & \pi(x_1) \geq \pi(x_2) \text{ and } a = 2 \\ \perp & \pi(x_1) \geq \pi(x_2) \text{ and } a = \perp \end{cases} \tag{44}$$

and $\pi \in S_4$. Using this symmetry reduces the number of free variables to 477. The trade-off between the amount of certified randomness and the nonlocality is illustrated in Fig. 5. We find that for sufficiently large values of $\mathcal{T}_2^{\mathrm{SIC}}$ (roughly $\mathcal{T}_2^{\mathrm{SIC}} \geq 4.8718$), we outperform the one-bit limitation associated to projective measurements on entangled qubits. Notably, for even larger values of $\mathcal{T}_2^{\mathrm{SIC}}$, we also outperform the restriction of $\log 3$ bits associated to projective measurements on entangled systems of local dimension three. For the optimal value of $\mathcal{T}_2^{\mathrm{SIC}}$ we find $H_{\min}(A_{\mathbf{povm}} \mid E) \gtrsim 1.999$, which is compatible up to numerical precision with the largest possible amount of randomness obtainable from qubit systems under general measurements, namely, two bits. This two-bit limit stems from the fact that every qubit measurement with more than four outcomes can be stochastically simulated with measurements of at most four outcomes (*88*).

For the case of $d = 3$, we bound the guessing probability following the method of (*87*). This has the advantage of requiring only a bipartite, and hence smaller, moment matrix than the tripartite formulation. However, the amount of symmetry leaving the problem invariant is reduced because the objective function only involves one outcome. Concretely, we construct a moment matrix of size 820×820 with 263,549 variables. We then write the guessing probability

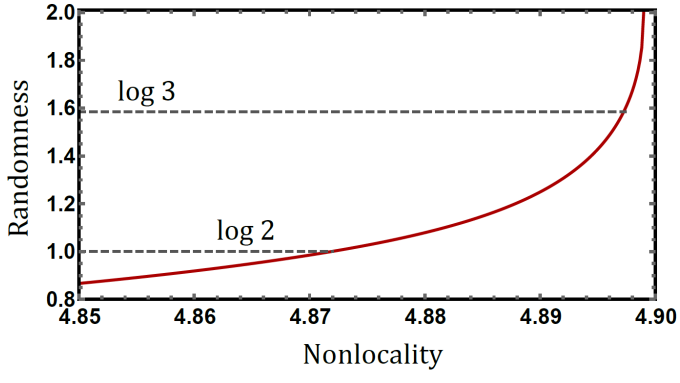

Fig. 5. Lower bound on the amount of device-independent randomness versus the value of $\mathcal{T}_2^{\mathrm{SIC}}$.

as $P(a' = 1 \,|\, \mathbf{povm})$ and identify the following group of permutations, leaving the problem invariant: $x_1 \to \pi(x_1)$, $x_2 \to \pi(x_2)$, $a \to f_\pi(a, x_1, x_2)$, $a' \to \pi(a')$, and $y \to \pi(y)$, where $\pi \in S_9$ leaves element 1 invariant and permutes elements 2, …,9 in all possible ways. Taking this symmetry into account reduces the number of free variables to 460. To further simplify the problem, we make use of RepLAB, a recently developed tool that decomposes representations of finite groups into irreducible representations (*89*, *90*). This allows us to write the moment matrix in a preferred basis in which it is block diagonal. The semidefinite constraint can then be imposed on each block independently, with the largest block size 28 × 28 instead of 820 × 820. Solving one semidefinite program with SeDuMi (*84*) then takes 0.7 s with <0.1 gigabytes of memory instead of 162 s/0.2 gigabytes without block diagonalization and fails because of lack of memory without any symmetrization (>400 gigabytes required).

Using entangled states of dimension 3 and corresponding SIC-POVMs, one can attain the full range of values for $\mathcal{T}_3^{\mathrm{SIC}}$. The guessing probability is independent of the outcome guessed by the eavesdropper, and we can verify that the bound that we obtain is convex, hence guaranteeing that no mixture of strategy by the eavesdropper must be considered (*87*). The randomness is then given in Fig. 6, which indicates that by increasing the value of $\mathcal{T}_3^{\mathrm{SIC}}$, we can obtain more randomness than the best possible schemes relying on standard projective measurements and entangled systems of dimensions 3,4,5,6, and 7. In particular, in the case of $\mathcal{T}_3^{\mathrm{SIC}}$ being maximal, we find that $H_{\min}(A_{\mathbf{povm}} \,|\, E) \approx 3.03$ bits. This is larger than what can be obtained by performing projective measurements on eight dimensional systems (since log 8 = 3 bits). It is, however, worth noting that this last value is obtained at the boundary of the set of quantum correlations where the precision of the solver is significantly reduced (in particular, the DIMACS errors at this point are of the order of 10^{-4}). It is not straightforward to estimate the extent to which this reduced precision may influence the guessing probability, so it would be interesting to reproduce this computation with a more precise solver such as SDPA (*91*).

DISCUSSION

MUBs and SICs are conceptually elegant, fundamentally important, and practically useful features of quantum theory. We investigated their role in quantum nonlocality. For both MUBs and SICs (of any Hilbert space dimension), we presented families of Bell inequalities for which they produce the maximal quantum violations. Moreover, we showed that these maximal quantum violations certify natural operational notions of mutual unbiasedness and symmetric informational completeness. Then, we considered applications of both families of Bell inequalities in practically relevant tasks. The Bell inequalities for MUBs turn out to be useful for the task of device-independent quantum key distribution and give the optimal key rate for measurements with d outcomes. Moreover, for the case of qutrit systems, we investigated the noise robustness of the protocol. For the Bell inequalities for SICs, we considered device-independent random number generation for qubits and qutrits based on SIC-POVMs. We showed (up to numerical precision) optimal randomness generation for qubit systems. For qutrit systems, we showed that more randomness can be generated than in any scheme using standard projective measurements and entanglement of up to dimension 7. These results were obtained using the RepLAB package, which helped to significantly reduce the complexity of the corresponding semidefinite programs by taking advantage of their symmetry.

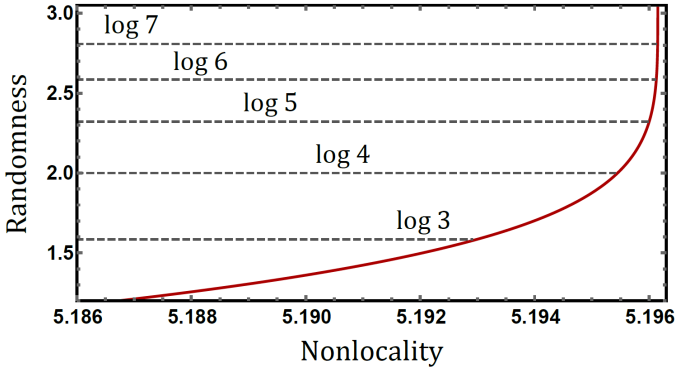

Fig. 6. Lower bound on the amount of device-independent randomness versus the value of $\mathcal{T}_3^{\mathrm{SIC}}$.

This work opens many new research directions, so let us mention just a few of them. We showed that a maximal quantum violation of the Bell inequality for MUBs self-tests a maximally entangled state of local dimension d. In the case of the Bell inequality for SICs, we have managed to certify the measurements of Bob, but we do not have a self-testing result for the state. If a self-test of the state is possible, what are the implications for the device-independent certification of the SIC-POVM setting? This may prove helpful toward solving another interesting question, namely, that of proving optimal local randomness generation (i.e., 2 log d bits) for any d based on the Bell inequality for SIC-POVMs. Another avenue of exploration regards the concept of MUMs. In this work, we have shown some of their basic properties with regard to MUBs and examples of how they are relevant in quantum information theory. However, a more systematic exploration of MUMs would be desirable. Similarly, a general exploration of OP-SICs in quantum information theory, as well as their relation to SICs, would be of similar interest. Last, we note that our noise-robust results for quantum key distribution and quantum random number generation may be relevant for experimental implementations.

MATERIALS AND METHODS

The method used for the construction of Bell inequalities for MUBs and SICs is based on tailoring these respective geometries to the framework of nonlocal games. Furthermore, to device-independently certify such structures, we relied on establishing operational generalizations of MUBs and SICs that rest solely on algebraic relationships whose validity is independent of Hilbert space dimension. We applied the Bell inequalities for MUBs and SICs, respectively, to the task of device-independent quantum key distribution and random number generation. To make possible the analysis of the key rate and the randomness rate in the presence of noise, we used semidefinite programming (*92*), which is an essential tool in established methods to bound the quantum set of correlations (*81*). To make the semidefinite programs efficiently computable, we used so-called symmetrization methods [see, e.g., (*93*)].

SUPPLEMENTARY MATERIALS

Supplementary material for this article is available at http://advances.sciencemag.org/cgi/content/full/7/7/eabc3847/DC1

REFERENCES AND NOTES

1. S. Kochen, E. P. Specker, The problem of hidden variables in quantum mechanics. *J. Math. Mech.* **17**, 59–87 (1967).
2. J. S. Bell, On the Einstein Podolsky Rosen paradox. *Physics* **1**, 195–200 (1964).
3. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
4. M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2010).
5. P. Busch, P. J. Lahti, J.-P. Pellonpää, K. Ylinen, *Quantum Measurement* (Springer, 2016).
6. J. Schwinger, Unitary operator bases. *Proc. Natl. Acad. Sci. U.S.A.* **46**, 570–579 (1960).
7. G. Zauner, "Quantendesigns, Grundzüge einer nichtkommutativen Designtheorie," thesis, University of Vienna (1999).
8. J. M. Renes, R. Blume-Kohout, A. J. Scott, C. M. Caves, Symmetric informationally complete quantum measurements. *J. Math. Phys.* **45**, 2171 (2004).
9. W. K. Wootters, Quantum measurements and finite geometry. *Found. Phys.* **36**, 112–126 (2006).
10. M. Grassl, On SIC-POVMs and MUBs in dimension 6. arXiv: 0406175 [quant-ph] (2004).
11. R. Beneduci, T. J. Bullock, P. Busch, C. Carmeli, T. Heinosaari, A. Toigo, Operational link between mutually unbiased bases and symmetric informationally complete positive operator-valued measures. *Phys. Rev. A* **88**, 032312 (2013).
12. I. Bengtsson, From SICs and MUBs to Eddington. *J. Phys. Conf. Ser.* **254**, 012007 (2010).
13. I. Bengtsson, K. Blanchfield, A. Cabello, A Kochen-Specker inequality from a SIC. *Phys. Lett. A* **376**, 374–376 (2012).
14. A. E. Rastegin, Uncertainty relations for MUBs and SIC-POVMs in terms of generalized entropies. *Eur. Phys. J. D* **67**, 269 (2013).
15. T. Durt, B.-G. Englert, I. Bengtsson, K. Życzkowski, On mutually unbiased bases. *Int. J. Quantum Inf.* **8**, 535–640 (2010).
16. H. Maassen, J. B. M. Uffink, Generalized entropic uncertainty relations. *Phys. Rev. Lett.* **60**, 1103 (1988).
17. C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, 1984), vol. 175, p. 8.
18. A. K. Ekert, Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
19. D. Bruß, Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**, 3018 (1998).
20. N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
21. V. Scarani, A. Acín, G. Ribordy, N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92**, 057901 (2004).
22. M. Hillery, V. Bužek, A. Berthiaume, Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
23. I.-C. Yu, F.-L. Lin, C.-Y. Huang, Quantum secret sharing with multilevel mutually (un) biased bases. *Phys. Rev. A* **78**, 012344 (2008).
24. A. Tavakoli, I. Herbauts, M. Żukowski, M. Bourennane, Secret sharing with a single d-level quantum system. *Phys. Rev. A* **92**, 030302(R) (2015).
25. W. K. Wootters, B. D. Fields, Optimal state-determination by mutually unbiased measurements. *Ann. Phys.* **191**, 363–381 (1989).
26. R. B. A. Adamson, A. M. Steinberg, Improving quantum state estimation with mutually unbiased bases. *Phys. Rev. Lett.* **105**, 030406 (2010).
27. A. Ambainis, A. Nayak, A. Ta-Shma, U. Vazirani, Dense quantum coding and a lower bound for 1-way quantum automata, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC'99)* (Association for Computing Machinery, 1999), pp. 376–383.
28. A. Tavakoli, A. Hameedi, B. Marques, M. Bourennane, Quantum random access codes using single *d*-level systems. *Phys. Rev. Lett.* **114**, 170502 (2015).
29. E. A. Aguilar, J. J. Borkała, P. Mironowicz, M. Pawłowski, Connections between mutually unbiased bases and quantum random access codes. *Phys. Rev. Lett.* **121**, 050501 (2018).
30. A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, N. Brunner, Self-testing quantum states and measurements in the prepare-and-measure scenario. *Phys. Rev. A* **98**, 062307 (2018).
31. M. Farkas, J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario. *Phys. Rev. A* **99**, 032316 (2019).
32. D. Gottesman, Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A* **54**, 1862 (1996).
33. A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.* **78**, 405 (1997).
34. C. Spengler, M. Huber, S. Brierley, T. Adaktylos, B. C. Hiesmayr, Entanglement detection via mutually unbiased bases. *Phys. Rev. A* **86**, 022311 (2012).
35. C. M. Caves, C. A. Fuchs, R. Schack, Unknown quantum states: The quantum de Finetti representation. *J. Math. Phys.* **43**, 4537–4559 (2002).
36. Z. E. D. Medendorp, F. A. Torres-Ruiz, L. K. Shalm, G. N. M. Tabia, C. A. Fuchs, A. M. Steinberg, Experimental characterization of qutrits using symmetric informationally complete positive operator-valued measurements. *Phys. Rev. A* **83**, 051801(R) (2011).
37. W. M. Pimenta, B. Marques, T. O. Maciel, R. O. Vianna, A. Delgado, C. Saavedra, S. Pádua, Minimum tomography of two entangled qutrits using local measurements of one-qutrit symmetric informationally complete positive operator-valued measure. *Phys. Rev. A* **88**, 012112 (2013).
38. N. Bent, H. Qassim, A. A. Tahir, D. Sych, G. Leuchs, L. L. Sánchez-Soto, E. Karimi, R. W. Boyd, Experimental realization of quantum tomography of photonic qudits via symmetric informationally complete positive operator-valued measures. *Phys. Rev. X* **5**, 041006 (2015).
39. J. M. Renes, Equiangular spherical codes in quantum cryptography. *Quant. Inf. Comput.* **5**, 080–091 (2005).
40. B.-G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Řeháček, J. Anders, Efficient and robust quantum key distribution with minimal state tomography. arXiv:0412075 [quant-ph] (2004).
41. F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, E. Karimi, Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum* **2**, 111 (2018).
42. A. Acín, S. Pironio, T. Vértesi, P. Wittek, Optimal randomness certification from one entangled bit. *Phys. Rev. A* **93**, 040102(R) (2016).
43. A. Tavakoli, D. Rosset, M.-O. Renou, Enabling computation of correlation bounds for finite-dimensional quantum systems via symmetrization. *Phys. Rev. Lett.* **122**, 070501 (2019).
44. P. Mironowicz, M. Pawłowski, Experimentally feasible semi-device-independent certification of four-outcome positive-operator-valued measurements. *Phys. Rev. A* **100**, 030301(R) (2019).
45. A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, M. Bourennane, Self-testing nonprojective quantum measurements in prepare-and-measure experiments. *Sci. Adv.* **6**, eaaw6664 (2020).
46. M. Smania, P. Mironowicz, M. Nawareg, M. Pawłowski, A. Cabello, M. Bourennane, Experimental certification of an informationally complete quantum measurement in a device-independent protocol. *Optica* **7**, 123–128 (2020).
47. J. Shang, A. Asadian, H. Zhu, O. Gühne, Enhanced entanglement criterion via symmetric informationally complete measurements. *Phys. Rev. A* **98**, 022309 (2018).
48. J. Bae, B. C. Hiesmayr, D. McNulty, Linking entanglement detection and state tomography via quantum 2-designs. *New J. Phys.* **21**, 013012 (2019).
49. C. A. Fuchs, R. Schack, Quantum-Bayesian coherence. *Rev. Mod. Phys.* **85**, 1693 (2013).
50. D. M. Appleby, C. A. Fuchs, H. Zhu, Group theoretic, lie algebraic and Jordan algebraic formulations of the sic existence problem. *Quant. Inf. Comput.* **15**, 61–94 (2015).
51. M. Appleby, S. Flammia, G. McConnell, J. Yard, SICs and algebraic number theory. *Found. Phys.* **47**, 1042–1059 (2017).
52. A. J. Scott, M. Grassl, SIC-POVMs: A new computer study. *J. Math. Phys.* **51**, 042203 (2010).
53. A. J. Scott, SICs: Extending the list of solutions. arXiv:1703.03993 [quant-ph] (2017).
54. C. A. Fuchs, M. C. Hoang, B. C. Stacey, The SIC question: History and state of play. *Axioms* **6**, 21 (2017).
55. J. B. DeBrota, C. A. Fuchs, B. C. Stacey, The varieties of minimal tomographically complete measurements. arXiv:1812.08762 [quant-ph] (2018).
56. N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, Bell nonlocality. *Rev. Mod. Phys.* **86**, 419 (2014).
57. I. Šupić, J. Bowles, Self-testing of quantum systems: A review. *Quantum* **4**, 337 (2020).
58. D. Ostrev, The structure of nearly-optimal quantum strategies for the CHSH(n) XOR games. *Quant. Inf. Comput.* **16**, 1191–1211 (2016).
59. A. Coladangelo, K. T. Goh, V. Scarani, All pure bipartite entangled states can be self-tested. *Nat. Commun.* **8**, 15485 (2017).
60. J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, R. Augusiak, Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. *Quantum* **3**, 198 (2019).
61. S. Sarkar, D. Saha, J. Kaniewski, R. Augusiak, Self-testing quantum systems of arbitrary local dimension with minimal number of measurements. arXiv:1909.12722 [quant-ph] (2019).
62. M. J. Kewming, S. Shrapnel, A. G. White, J. Romero, Hiding ignorance using high dimensions. *Phys. Rev. Lett.* **124**, 250401 (2020).
63. B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015).
64. L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, S. W. Nam, Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
65. M. Giustina, M. A. . M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri,

M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, A. Zeilinger, Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
66. W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, H. Weinfurter, Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.* **119**, 010402 (2017).
67. S.-W. Ji, J. Lee, J. Lim, K. Nagata, H.-W. Lee, Multi-setting Bell inequality for qudits. *Phys. Rev. A* **78**, 052103 (2008).
68. Y.-C. Liang, C.-W. Lim, D.-L. Deng, Reexamination of a multisetting Bell inequality for qudits. *Phys. Rev. A* **80**, 052116 (2009).
69. J. Lim, J. Ryu, S. Yoo, C. Lee, J. Bang, J. Lee, Genuinely high-dimensional nonlocality optimized by complementary measurements. *New J. Phys.* **12**, 103012 (2010).
70. H. Bechmann-Pasquinucci, N. Gisin, Bell inequality for quNits with binary measurements. *Quant. Inf. Comput.* **3**, 157–164 (2003).
71. J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880 (1969).
72. S. Brierley, S. Weigert, I. Bengtsson, All mutually unbiased bases in dimensions two to five. *Quant. Inf. Comput.* **10**, 0803–0820 (2010).
73. C. Jebarathinam, J.-C. Hung, S.-L. Chen, Y.-C. Liang, Maximal violation of a broad class of Bell inequalities and its implication on self-testing. *Phys. Rev. Res.* **1**, 033073 (2019).
74. J. Kaniewski, A weak form of self-testing. *Phys. Rev. Res.* **2**, 033420 (2020).
75. D. S. Tasca, P. Sánchez, S. P. Walborn, Ł. Rudnicki, Mutual unbiasedness in coarse-grained continuous variables. *Phys. Rev. Lett.* **120**, 040403 (2018).
76. M. Krishna, K. R. Parthasarathy, An entropic uncertainty principle for quantum measurements. *Indian J. Stat.* **64**, 842–851 (2002).
77. T. Heinosaari, T. Miyadera, M. Ziman, An invitation to quantum incompatibility. *J. Phys. A Math. Theor.* **49**, 123001 (2016).
78. E. Haapasalo, Robustness of incompatibility for quantum devices. *J. Phys. A Math. Theor.* **48**, 255303 (2015).
79. L. Masanes, S. Pironio, A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.* **2**, 238 (2011).
80. T. Franz, F. Furrer, R. F. Werner, Extremal quantum correlations and cryptographic security. *Phys. Rev. Lett.* **106**, 250502 (2011).
81. M. Navascués, S. Pironio, A. Acín, Bounding the set of quantum correlations. *Phys. Rev. Lett.* **98**, 010401 (2007).
82. D. Rosset, SymDPoly: Symmetry-adapted moment relaxations for noncommutative polynomial optimization. arXiv:1808.09598 [quant-ph] (2018).
83. Y. Cai, J.-D. Bancal, J. Romero, V. Scarani, A new device-independent dimension witness and its experimental implementation. *J. Phys. A Math. Theor.* **49**, 305301 (2016).
84. J. F. Sturm, Using SeDuMi 1.02, A Matlab toolbox for optimization over symmetric cones. *Optim. Methods Softw.* **11**, 625–653 (1999).
85. N. Gisin, Bell inequalities: Many questions, a few answers. arXiv:0702021 [quant-ph] (2007).
86. A. Tavakoli, N. Gisin, Platonic solids and fundamental tests of quantum mechanics. *Quantum* **4**, 293 (2020).
87. S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
88. G. M. D'Ariano, P. L. Presti, P. Perinotti, Classical randomness in quantum measurements. *J. Phys. A Math. Gen.* **38**, 5979 (2005).
89. https://replab.github.io.
90. D. Rosset, F. Montealegre-Mora, J.-D. Bancal, RepLAB: A computational/numerical approach to representation theory. arXiv:1911.09154 [quant-ph] (2019).
91. http://sdpa.sourceforge.net.
92. S. Boyd, L. Vandenberghe, *Convex Optimization* (Cambridge Univ. Press, 2004).
93. K. Gaterman, P. A. Parrilo, Symmetry groups, semidefinite programs, and sums of squares. *J. Pure Appl. Algebra* **192**, 95–128 (2004).
94. M. Navascués, S. Pironio, A. Acín, SDP relaxations for non-commutative polynomial optimization, in *Handbook on Semidefinite, Conic and Polynomial Optimization*, M. F. Anjos, J. B. Lasserre, Eds. (Springer, 2012), International Series in Operations Research & Management Science, vol. 166, pp. 601–634.
95. M.-D. Choi, Completely positive linear maps on complex matrices. *Linear Algebra Appl.* **10**, 285–290 (1975).
96. A. Jamiołkowski, Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.* **3**, 275–278 (1972).
97. S. Designolle, M. Farkas, J. Kaniewski, Incompatibility robustness of quantum measurements: A unified framework. *New J. Phys.* **21**, 113053 (2019).
98. J. Kaniewski, M. Tomamichel, S. Wehner, Entropic uncertainty from effective anticommutators. *Phys. Rev. A* **90**, 012332 (2014).

Acknowledgments: We would like to thank T. de Lima Silva and N. Gisin for fruitful discussions. We thank M. Araújo for helpful comments. **Funding:** This work was supported by the Swiss National Science Foundation (starting grant DIAQ, NCCRQSIT). A.T. acknowledges support from the Swiss National Science Foundation (Early PostDoc Mobility fellowship P2GEP2 194800). The project "Robust certification of quantum devices" is carried out within the HOMING programme of the Foundation for Polish Science cofinanced by the European Union under the European Regional Development Fund. M.F. acknowledges support from the Polish NCN grant Sonata UMO-2014/14/E/ST2/00020, the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme ERC AdG CERQUTE (grant agreement no. 834266), the State Research Agency (AEI) TRANQI (PID2019-106888GB-I00/10.13039/501100011033), the Government of Spain (FIS2020-TRANQI; Severo Ochoa CEX2019-000910-S), Fundació Cellex, Fundació Mir-Puig, and Generalitat de Catalunya (CERCA, AGAUR). **Author contributions:** A.T. and J.K. proposed the basic concept. A.T., M.F., J.-D.B., and J.K. developed the theory and the proofs. D.R. developed a software that was used to facilitate particular computations. A.T., M.F., J.-D.B., and J.K. discussed the results and participated in the writing of the manuscript. **Competing interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. Additional data related to this paper may be requested from the authors.

Submitted 22 April 2020
Accepted 4 December 2020
Published 10 February 2021
10.1126/sciadv.abc3847

Citation: A. Tavakoli, M. Farkas, D. Rosset, J.-D. Bancal, J. Kaniewski, Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments. *Sci. Adv.* **7**, eabc3847 (2021).