Enabling Computation of Correlation Bounds for Finite-Dimensional Quantum Systems via Symmetrization

Armin Tavakoli,[1,*] Denis Rosset,[2,*] and Marc-Olivier Renou[1]
[1]*Department of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*
[2]*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada, N2L 2Y5*

(Received 29 August 2018; revised manuscript received 11 December 2018; published 20 February 2019)

We present a technique for reducing the computational requirements by several orders of magnitude in the evaluation of semidefinite relaxations for bounding the set of quantum correlations arising from finite-dimensional Hilbert spaces. The technique, which we make publicly available through a user-friendly software package, relies on the exploitation of symmetries present in the optimization problem to reduce the number of variables and the block sizes in semidefinite relaxations. It is widely applicable in problems encountered in quantum information theory and enables computations that were previously too demanding. We demonstrate its advantages and general applicability in several physical problems. In particular, we use it to robustly certify the nonprojectiveness of high-dimensional measurements in a black-box scenario based on self-tests of d-dimensional symmetric informationally complete positive-operator-valued measurements.

DOI: 10.1103/PhysRevLett.122.070501

Introduction.—Finite-dimensional quantum systems are common in quantum information theory. They are standard in the broad scope of quantum communication complexity problems (CCPs) [1] in which quantum correlations are studied under limited communication resources. Furthermore, they are widely used in semi-device-independent quantum information protocols [2] in which systems are fully uncharacterized up to their Hilbert space dimension. Also, studying correlations obtainable from finite-dimensional systems is critical for device-independent dimension witnessing [3,4].

In view of their diverse relevance, it is important to bound quantum correlations arising from dimension-bounded Hilbert spaces. To this end, semidefinite programs (SDPs) [5] constitute a powerful tool. Lower bounds on quantum correlations are straightforwardly obtained using alternating convex searchers (SDPs in see-saw) [6,7]. However, obtaining upper bounds valid for *any* quantum states and measurements is more demanding. A powerful approach to this problem is to relax some well-chosen constraints of quantum theory so that the resulting super-quantum correlations easily can be computed with SDPs, thus returning upper bounds on quantum correlations. Such approaches are commonplace in various problems in quantum information theory [8–10]. A hierarchy of semidefinite relaxations for upper-bounding quantum correlations on dimension-bounded Hilbert spaces was introduced by Navascués and Vértesi (NV) [10,11]. This is an effective tool for problems involving a small number of states and measurements, and low Hilbert space dimensions. However beyond simple scenarios, the computational requirements of evaluating the relaxations quickly become too demanding.

It is increasingly relevant to overcome the practical limitations of the NV hierarchy, i.e., to provide efficient computational tools for bounding quantum correlations in problems beyond small sizes and low Hilbert space dimensions. This is motivated by both theoretical and experimental advances. Dimension witnessing has been experimentally realized far beyond the lowest Hilbert space dimensions [12,13]. Furthermore, increasing the dimension can activate unexpectedly strong quantum correlations [14], a phenomenon that has been experimentally demonstrated [15]. Also, quantum correlations obtained from a sizable number of states and measurements are interesting for studying mutually unbiased bases [16]. Moreover, large problem sizes naturally appear in multipartite CCPs involving single particles [17–19]. Similarly sized problems also appear in multipartite CCPs for the characterization of entangled states and measurements [20]. In addition, efficiently evaluating the NV hierarchy many times can improve randomness extraction from experimental data [21].

In this work we develop techniques for efficiently bounding quantum correlations under dimension constraints. The technique is powered by the exploitation of *symmetries*, i.e., relabelings of optimization variables that leave a figure of merit invariant. The use of symmetries for reducing the complexity of SDPs was first introduced in Ref. [22] and was shown to lead to remarkable efficiency gains. These efficiency gains have also been harvested in several specific quantum information problems relying on SDPs. These include finding bounds on classical [23] and quantum [24,25] Bell correlations, quantifying entanglement [9,26], and finding symmetric Bell inequalities [27].

Note that symmetries in Bell scenarios also have been studied without application to SDPs [28–31]. In dimension-bounded scenarios, symmetries have been considered for CCPs tailored for studying the existence of mutually unbiased bases [16].

We describe a powerful, generally applicable, and easy-to-use technique for symmetrized semidefinite relaxations for dimension-bounded quantum correlations. We show how to automatize searches for symmetries in general Bell scenarios and CCPs, and how these can be exploited to reduce computational requirements in all parts of the NV hierarchy. This amounts to reducing the number of variables in an optimization, and reducing block sizes beyond previous approaches. We make these techniques readily available via a user-friendly software package supporting general correlation scenarios. Subsequently, we give examples of problems that can be solved faster (several orders of magnitude), and other previously unattainable problems that can now be computed. We focus on the usefulness of symmetrization for the problem of certifying that an uncharacterized device implements a nonprojective measurement using only the observed correlations. To this end, we introduce a family of CCPs, prove that they enable self-tests of d-dimensional symmetric informationally complete (SIC) positive-operator-valued measurements (POVMs), then use symmetrized semidefinite relaxations to bound the correlations attainable under projective measurements. This allows us to go beyond previously studied qubit systems [32–36] and robustly certify the nonprojectiveness of SIC-POVMs subject to imperfections.

Bounding finite-dimensional quantum correlations.— We begin by summarizing the NV hierarchy [10,11] for optimizing dimensionally constrained quantum correlations. For simplicity, we first describe CCPs, and later consider Bell scenarios.

Consider a CCP in which a party, Alice, holds a random input x and another party, Bob, holds a random input y. Alice encodes her input into a quantum state ρ_x of dimension d and sends it to Bob. Bob performs a measurement $\{M_y^b\}_b$ with outcome b. The resulting probability distribution is used to evaluate a functional $F(P) = \sum_{x,y,b} c_{x,y}^b P(b|x,y)$, where $c_{x,y}^b$ are real coefficients. The problem of interest is to compute the maximal quantum value of F when the probabilities are given by the Born rule $P(b|x,y) = \mathrm{tr}(\rho_x M_y^b)$, where the measurement operators are taken to be projectors. The NV hierarchy presents the following semidefinite relaxations. Sample a random set of states and measurements $\{\rho_x\}$ and $\{M_y^b\}$ of dimension d, which we collect in the set of operator variables $\{X_i\}$. Then, generate all strings, $\{s_j(X)\}_j$, of products of at most L of these operators. The choice of L determines the degree of relaxation, i.e., the level of the hierarchy. Construct a moment matrix

$$\Gamma_{j,k} = \langle s_j(X)^\dagger s_k(X) \rangle, \tag{1}$$

where, for the present CCP, the expectation value of an operator product S is $\langle S \rangle = \mathrm{tr}S$. Repeat this process many times, each time obtaining a new moment matrix. Terminate the process when the sampled moment matrix is linearly dependent on the collection of those previously generated. Hence, $\{\Gamma^{(1)}, \ldots, \Gamma^{(m)}\}$ identifies a basis for the feasible affine subspace $\mathcal{F}$ of such matrices under the given dimensional constraint. The semidefinite relaxation amounts to finding an affine combination $\Gamma = \sum_{\ell=1}^m c_\ell \Gamma^{(\ell)} \in \mathcal{F}$, with $\Gamma \geq 0$, that maximizes the functional F (which can be expressed as a linear combination of entries of Γ). Hence, the relaxation reads

$$\max_{\vec{c} \in \mathbb{R}^m} F(\Gamma) \quad \text{s.t.} \quad \Gamma \geq 0, \quad \sum_{\ell=1}^m c_\ell = 1. \tag{2}$$

In summary, the problem consists in first sampling a basis enforcing the dimensional constraint and then evaluating a SDP. Crucially, the complexity of solving the SDP hinges on the number of basis elements, m, needed to complete the basis and the size of the final SDP matrix, n. For a single iteration of primal-dual interior point solvers, the required memory scales as $\mathcal{O}(m^2 + mn^2)$ while the CPU time scales as $\mathcal{O}(m^3 + n^3 + mn^3 + m^2n^2)$ [37]. Without exploitation of the problem structure, medium-sized physical scenarios, as well as small-sized scenarios with high relaxation degree, practically remain out of reach for current desktop computers. We have performed all computations using a machine of 32 GB RAM and i5-6500 3.2 GHz CP.

Symmetric relaxations.—The key to reducing the computational requirements for the NV hierarchy is twofold: First reducing the number of elements needed to form the basis in the sampling step, i.e., decreasing the dimension of $\mathcal{F}$, and then shrinking the size of the positivity constraints in the subsequent SDP by block-diagonalizing Γ. Here, we show how such a reduction can be systematically achieved by identifying and exploiting the set of symmetries of the problem.

Recall that $\{X_i\}$ collects all the operators (states, measurements etc.) present in the formulation of the problem, where $i \in \mathcal{I}$ is an index. Consider a permutation of elements of $\mathcal{I}$, i.e., a bijective function $\pi\colon \mathcal{I} \to \mathcal{I}$. We write $\pi(X_i) = X_{\pi(i)}$ and define the action of the permutation on the strings $s = X_i X_j \ldots$ of products of operators X_i appearing in the NV hierarchy as $\pi(X_i X_j \ldots) = X_{\pi(i)} X_{\pi(j)} \ldots$. We call π an *ambient symmetry* if it is a transformation of the scenario which preserves its structure, as expressed by implicit or explicit constraints on the operators $\{X_i\}$. The set of those symmetries form the *ambient group* $\mathcal{A} = \{\pi\}$. In the Supplemental Material [38] (SM, including Refs. [39–54]), we describe the ambient groups for general Bell scenarios and CCPs. Given a moment matrix Γ and $\pi \in \mathcal{A}$, we consider the relabeled matrix $\pi(\Gamma)$ where $(\pi(\Gamma))_{j,k} = \Gamma_{\pi^{-1}(j),\pi^{-1}(k)}$, according to the convention of Eq. (1). By construction, π preserves the constraints of the problem: for a feasible moment matrix $\Gamma \in \mathcal{F}$ we have $\pi(\Gamma) \in \mathcal{F}$ for any $\pi \in \mathcal{A}$. Moreover, the feasible set $\mathcal{F}$ is convex, so any convex combination of those $\pi(\Gamma)$ is feasible as well.

However, not all elements of $\mathcal{A}$ leave the objective $F(\Gamma)$ invariant. We write $\mathcal{G} = \{\pi \in \mathcal{A}: F(\pi(\Gamma)) = F(\Gamma)\}$ the *symmetry group* of the optimization problem. One can straightforwardly find the elements of $\mathcal{G}$ by enumerating the elements of $\mathcal{A}$ and filtering those that leave $F(\pi(\Gamma)) = F(\Gamma)$ invariant. Then, following a standard procedure [16,22,24,27] we can average any optimal solution Γ under the Reynolds operator, defined as

$$\Gamma' \equiv \mathcal{R}(\Gamma) = \frac{1}{|\mathcal{G}|}\sum_{\pi\in\mathcal{G}}\pi(\Gamma), \tag{3}$$

where $|\mathcal{G}|$ is the size of $\mathcal{G}$ and obtain an optimal solution of the problem, which now satisfies $\pi(\Gamma') = \Gamma'$ for all $\pi \in \mathcal{G}$. Since the set Γ' is characterized by the relation $\mathcal{R}(\Gamma') = \Gamma'$, instead of searching the optimal Γ in the full feasible set, it is sufficient to only consider the symmetric subspace $\mathcal{R}(\mathcal{F})$ given by the image of the feasible set under $\mathcal{R}$. As discussed above, the basis of $\mathcal{F}$ is found by sampling. To sample $\mathcal{R}(\mathcal{F})$ instead, we simply apply $\mathcal{R}$ on each sample during the construction of the basis, thus obtaining $\{\Gamma'^{(1)}, \ldots, \Gamma'^{(m')}\}$. As a result, the size of the basis, m', decreases due to the smaller dimension of $\mathcal{R}(\mathcal{F})$. In the SM, we discuss methods for speeding up the computation of $\mathcal{R}$.

Moreover, a second major reduction is obtained: As the symmetrized moment matrices Γ' commute with a representation of the group $\mathcal{G}$, there exists [22] a unitary matrix that block diagonalizes the moment matrix. This reduces the size of the positivity constraint on the final SDP matrix. A complete symmetry exploitation is obtained when the decomposition of the representation of $\mathcal{G}$ into irreducible components with multiplicities is known. We achieve this via an efficient general block diagonalization method detailed in the SM. Moreover, we make available a user-friendly MATLAB package [55] for symmetrization of semidefinite relaxations in the NV hierarchy applicable to general correlation scenarios encountered in quantum information. The package automates both a search for the symmetries of a problem (if these are unknown) and the construction of symmetry-adapted relaxation.

Robust certification of nonprojective measurements based on SIC-POVMs.—We now exemplify the usefulness of symmetrization in a physical application. We certify, solely from observed data, that an uncharacterized device ("black-box") implements a nonprojective measurement. Nonprojective measurements have diverse applications in quantum theory [32,56–62]. This has motivated interest in their black-box certification [32–36]. Using semidefinite relaxations (whose complexity scales quickly with dimension) as a primary tool, these works limit themselves to qubits. We use symmetrization to overcome this limitation and certify the nonprojectiveness of higher-dimensional measurements of physical interest. Since such certificates are typically only useful for nonprojective measurements that are close (e.g., in fidelity) to a particular targeted nonprojective measurement (corresponding to the optimal quantum correlations) [33], it is important to ensure that the targeted measurement is well motivated.

One of the most celebrated nonprojective measurements is the SIC-POVM. These are sets of d^2 subnormalized rank-one projectors $\{(1/d)|\psi_x\rangle\langle\psi_x|\}_{x=1}^{d^2}$ with $|\langle\psi_x|\psi_{x'}\rangle|^2 = 1/(d+1)$ when $x \neq x'$. Higher-dimensional SIC-POVMs have been of substantial interest for both fundamental (see, e.g., Ref. [63] for a review) and practical considerations [64–68] in quantum information theory. We introduce a family of CCPs and prove that optimal quantum correlations imply a d-dimensional SIC-POVM. However, due to unavoidable experimental imperfections, such optimal correlations will never occur in practice. Therefore, we use symmetrization to certify the nonprojectiveness of measurements close to SIC-POVMs, that achieve nearly optimal correlations. Moreover, as noted in Ref. [33], the dimension-bounded scenario is well-suited for black-box studies of nonprojective measurements since said property is only well-defined on Hilbert spaces of fixed dimension.

Consider a CCP in which Alice encodes her input x into a d-dimensional system sent to Bob, who associates his input y to a measurement producing an outcome b. A general witness can be written

$$W = \sum_{x,y,b}\alpha_{xyb}P(b|x,y), \tag{4}$$

where α_{xyb} are real coefficients. By tuning the coefficients, one can construct CCPs in which the optimal correlations W^Q are uniquely realized with a particular nonprojective measurement. This is known as a self-test [69]. Consequently, there must exist some $W^P < W^Q$ which bounds the correlations under all projective measurements. Thus, observing $W > W^P$ certifies that Bob implements a nonprojective measurement.

We construct a family of CCPs (inspired by Refs. [33,70]) tailored to self-test d-dimensional SIC-POVMs. Alice and Bob each receive inputs $x \in [N]$ and $(y, y') \in [N]$ with $y < y'$, respectively, for some $N > d$ and $[N] = \{1, \ldots, N\}$. Bob outputs $b \in \{0, 1\}$. Bob also possesses another measurement setting labeled *povm* which returns an outcome $o \in [N]$. The witness of interest is

$$W_d = \sum_{x<x'}P(b=0|x,(x,x')) + P(b=1|x',(x,x')) + \sum_{x=1}^{N}P(o=x|x,povm). \tag{5}$$

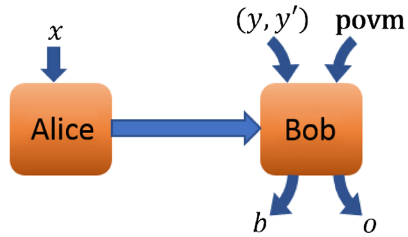

FIG. 1. Illustration of the CCP [Eq. (5)]. Bob has $\binom{N}{2}$ settings labeled by (y, y') and one additional setting labeled *povm*. Alice and Bob aim to satisfy the following relations: $o = x$ for the setting *povm*, and $b = 0$ when $x = y$ and $b = 1$ when $x = y'$, respectively, for the settings (y, y').

The scenario is illustrated in Figure 1.

Theorem 1: For $N = d^2$, the maximal quantum value of the witness is

$$W_d^Q = \frac{1}{2}\sqrt{d^5(d-1)^2(d+1)} + \binom{d^2}{2} + d. \qquad (6)$$

This value self-tests that Alice prepares a SIC ensemble and that Bob's setting *povm* corresponds to a SIC-POVM (Note that SIC-POVMs are not proven to exist in all dimensions).

The proof is given in the SM. To enable the certification of a nonprojective measurement producing nearly optimal correlations, we must obtain a bound W_d^P on W_d respected by all projective measurements. To this end, we use symmetrized semidefinite relaxations.

The symmetries of the witness [Eq. (5)] correspond to coordinated permutations of the inputs of Alice and inputs and outputs of Bob. We permute x among its N possible values. This requires us to compensate the permutation by also applying it to o. Furthermore, to preserve the probabilities appearing in the first summand of Eq. (5), we must apply a permutation to the indices (y, y') and the outcome b. Moreover, since we are interested in bounding W_d under projective measurements, said property must be explicitly imposed on Bob's setting *povm*. This means that at most d of the POVM elements $\{M_{povm}^x\}_{x=1}^{d^2}$ are nonzero, corresponding to rank-one projectors. This must be accounted for in the symmetries of the problem. In the SM we discuss the symmetries in detail.

TABLE I. Upper bounds (UBs) and lower bounds (LBs) on quantum correlations under projective measurements with $N = d^2$. The lower bounds are obtained via SDPs in an alternate convex search and the upper bounds via symmetrized semidefinite relaxations.

d	2	3	4	5	6
LB: W_d^P	12.8484	70.0961	231.2685	578.7002	1219.0129
UB: W_d^P	12.8484	70.1133	231.2685	578.7987	1219.2041
W_d^Q	12.8990	70.1769	231.3313	578.8613	1219.2667

Using the general recipe, we have implemented the symmetrized NV hierarchy. We use the relaxation degree corresponding to monomials $\{\mathbb{1}, \rho, M, M_{povm}, \rho\rho\}$ and also all the monomials $\rho_x M_{(x,x')}^b$ appearing in the first summand of Eq. (5). In Table I we present the upper bounds W_d^P. We have also obtained lower bounds for W_d under projective measurements by considering SDPs in an alternate convex search, enforcing only d nonzero elements of trace one. These lower bounds were verified to be achieved with projective measurements up to machine precision. The results show that the obtained upper bounds are either optimal or close to optimal, depending on d. In analogy with previous works [32–36], we find that the gap between optimal quantum correlations and those obtained under projective measurements is small.

Consider the role of symmetrization in obtaining the above results. In Table II we present the number of samples needed to complete the basis in the NV hierarchy, the size of the final SDP matrix, and the time required to evaluate the SDPs. We compare these parameters for a

TABLE II. Comparison between computational parameters for the task of bounding W_d under projective measurements using a standard implementation, symmetrization to reduce the number of samples [using only Eq. (3)], and symmetrization to also perform block diagonalization (BD). The notation $D[a, b]$ means that there are D blocks with the smallest being of size a and the largest of size b.

	d	2	3	4	5	6
Non-sym	No. of samples	221	>12 000	...	...	...
	Block sizes	1[43]	1[229]	1[741]	1[1831]	1[3823]
	SDP [s]	2.0	...	...	...	...
Sym no BD	No. of samples	65	134		137	
	Block sizes	1[43]	1[229]	1[741]	1[1831]	1[3823]
	SDP [s]	0.5	19	500	...	...
Sym + BD	No. of samples	65	134		137	
	Block sizes	4[6,16]	7[3,16]		8[3,16]	
	SDP [s]	0.3	0.6		1.2	

standard implementation, a symmetrized implementation only reducing the number of samples, and a the full symmetrization developed to also exploit block diagonalization of the SDP matrix. Without symmetries, we are unable to go beyond qubit systems ($d = 2$), since already for $d = 3$ we have over 12 000 samples. Interestingly, this rapid increase in complexity can be completely overcome via symmetrization: The number of samples becomes constant when $d = 4$, 5, 6. In addition, the size of the SDP matrix increases polynomially in d, causing symmetrization that only addresses the number of samples to still be too demanding already when $d > 4$. However, using the block-diagonalization methods detailed in the SM, we can reduce the size of the SDP matrix to be constant for $d = 4$, 5, 6. This allows us to straightforwardly solve the semidefinite relaxations in less than two seconds.

Further applications.—The general symmetrization technique applies to many problems in quantum information theory. In the SM, we consider four different examples. For each, we demonstrate the remarkable computational advantages of symmetrization, both in terms of reducing the number of basis elements and in terms of block diagonalization. This enables us to obtain improved bounds on previously studied physical quantities. The problems we consider are (high-dimensional and many-input) random access codes [71,72], I_{3322}-like Bell inequalities [11,73], a sequential communication in multipartite CCPs (in the spirit of Refs. [17,18]), and CCPs exhibiting dimensional discontinuities [14,15]. In the latter, we also exemplify the advantages in automatizing the search for the symmetries in problems in which these are not easily spotted by inspection.

Moreover, we previously observed that the complexity of the evaluation for bounding W_d^P can be reduced to be constant for $d = 4$, 5, 6 via symmetries. This suggests that similar reductions may occur for other CCPs as well. In the SM we have focused on the CCPs known as random access codes and proven that symmetries enable us to evaluate the NV hierarchy with constant complexity for any Hilbert space dimension. In this sense, the computational advantages over standard implementations, as well as over symmetrization that does not utilize block diagonalization, increase with d.

Conclusions.—We presented a technique for efficiently evaluating semidefinite relaxations of finite-dimensional quantum correlations using symmetries present in the problem. We applied it to robustly certify higher-dimensional nonprojective measurements by considering CCPs that self-test d-dimensional SIC-POVMs. The scheme could be implemented in photonics experiments using, e.g., encodings in path [64,68], path and polarization [65], and orbital angular momentum [66,67]. Measuring a value of W_d above the upper bounds (UBs) stated in Table I completes the certification. A broadly relevant open problem in this topic [32–36] is making the certification more tolerant to experimental imperfections (i.e., larger gaps between W_d^P (UB) and W_d^Q in Table I).

We conclude with two more open problems. Can the sampling approach be adapted to semidefinite relaxations in Bell inequalities without dimensional bounds? How does the symmetrization technique adapt to physical problems that do not concern quantum resources; e.g., cardinality of hidden variables [74] and the dimension of post-quantum resources?

We are thankful for useful discussions with Jean-Daniel Bancal. This work was supported by the Swiss National Science Foundation (Starting Grant DIAQ, NCCR-QSIT). Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. This publication was made possible through the support of a grant from the John Templeton Foundation.

Note added.—Recently, we became aware of a work-in-preparation by E. Aguilar and P. Mironowicz to generalize the results of Ref. [16].

[*] A. T. and D. R. contributed equally for this project.

[1] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Nonlocality and communication complexity, Rev. Mod. Phys. **82**, 665 (2010).
[2] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).
[3] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-Independent Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. **105**, 230501 (2010).
[4] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, Testing the Dimension of Hilbert Spaces, Phys. Rev. Lett. **100**, 210503 (2008).
[5] L. Vandenberghe and S. Boyd, Semidefinite programming, SIAM Rev. **38**, 49 (1996).
[6] R. E. Wendell and A. P. Hurter, Jr., Minimization of a non-separable objective function subject to disjoint constraints, Oper. Res. **24**, 643 (1976).
[7] K. F. Pál and T. Vértesi, Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems, Phys. Rev. A **82**, 022116 (2010).
[8] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, Phys. Rev. Lett. **98**, 010401 (2007).
[9] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Device-Independent Entanglement Quantification and Related Applications, Phys. Rev. Lett. **111**, 030501 (2013).
[10] M. Navascués and T. Vértesi, Bounding the Set of Finite Dimensional Quantum Correlations, Phys. Rev. Lett. **115**, 020501 (2015).

[11] M. Navascués, A. Feix, M. Araújo, and A. Vértesi, Characterizing finite-dimensional quantum behavior, Phys. Rev. A **92**, 042117 (2015).

[12] V. D'Ambrosio, F. Bisesto, F. Sciarrino, J. F. Barra, G. Lima, and A. Cabello, Device-Independent Certification of High-Dimensional Quantum Systems, Phys. Rev. Lett. **112**, 140503 (2014).

[13] E. A. Aguilar, M. Farkas, D. Martínez, M. Alvarado, J. Cariñe, G. B. Xavier, J. F. Barra, G. Cañas, M. Pawłowski, and G. Lima, Certifying an Irreducible 1024-Dimensional Photonic State Using Refined Dimension Witnesses, Phys. Rev. Lett. **120**, 230503 (2018).

[14] A. Tavakoli, M. Pawłowski, M. Żukowski, and M. Bourennane, Dimensional discontinuity in quantum communication complexity at dimension seven, Phys. Rev. A **95**, 020302(R) (2017).

[15] D. Martínez, A. Tavakoli, M. Casanova, G. Cañas, B. Marques, and G. Lima, High-Dimensional Quantum Communication Complexity beyond Strategies Based on Bells Theorem, Phys. Rev. Lett. **121**, 150504 (2018).

[16] E. A. Aguilar, J. J. Borkała, P. Mironowicz, and M. Pawłowski, Connections Between Mutually Unbiased Bases and Quantum Random Access Codes, Phys. Rev. Lett. **121**, 050501 (2018).

[17] E. F. Galvão, Feasible quantum communication complexity protocol, Phys. Rev. A **65**, 012318 (2001).

[18] P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Żukowski, and H. Weinfurter, Experimental quantum communication complexity, Phys. Rev. A **72**, 050305(R) (2005).

[19] M. Smania, A. M. Elhassan, A. Tavakoli, and M. Bourennane, Experimental quantum multiparty communication protocols, npj Quantum Inf. **2**, 16010 (2016).

[20] A. Tavakoli, A. A. Abbott, M.-O. Renou, N. Gisin, and N. Brunner, Semi-device-independent characterization of multipartite entanglement of states and measurements, Phys. Rev. A **98**, 052333 (2018).

[21] P. Mironowicz, A. Tavakoli, A. Hameedi, B. Marques, P. Pawłowski, and M. Bourennane, Increased certification of semi-device independent random numbers using many inputs and more postprocessing, New J. Phys. **18**, 065004 (2016).

[22] K. Gatermann and P. A. Parrilo, Symmetry groups, semidefinite programs, and sums of squares, J. Pure Appl. Algebra **192**, 95 (2004).

[23] M. Fadel and J. Tura, Bounding the Set of Classical Correlations of a Many-Body System, Phys. Rev. Lett. **119**, 230402 (2017).

[24] D. Rosset, Characterization of correlations in quantum networks, Ph.D. thesis, 2015.

[25] C. Bamps and S. Pironio, Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing, Phys. Rev. A **91**, 052111 (2015).

[26] Y. Cai, J.-D. Bancal, J. Romero, and V. Scarani, A new device-independent dimension witness and its experimental implementation, J. Phys. A **49**, 305301 (2016).

[27] J.-D. Bancal, N. Gisin, and S. Pironio, Looking for symmetric Bell inequalities, J. Phys. A **43**, 385303 (2010).

[28] C. Śliwa, Symmetries of the Bell correlation inequalities, Phys. Lett. A **317**, 165 (2003).

[29] D. Collins and N. Gisin, A relevant two qubit Bell inequality inequivalent to the CHSH inequality, J. Phys. A **37**, 1775 (2004).

[30] M.-O. Renou, D. Rosset, A. Martin, and N. Gisin, On the inequivalence of the CH and CHSH inequalities due to finite statistics, J. Phys. A **50**, 255301 (2017).

[31] D. Rosset, J.-D. Bancal, and N. Gisin, Classifying 50 years of Bell inequalities, J. Phys. A **47**, 424022 (2014).

[32] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A **93**, 040102(R) (2016).

[33] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, Self-testing non-projective quantum measurements, arXiv:1811.12712.

[34] E. S. Gómez *et al.*, Device-Independent Certification of a Nonprojective Qubit Measurement, Phys. Rev. Lett. **117**, 260401 (2016).

[35] P. Mironowicz and M. Pawłowski, Experimentally feasible semi-device-independent certification of 4 outcome POVMs, arXiv:1811.12872.

[36] M. Smania, P. Mironowicz, M. Nawareg, M. Pawlowski, A. Cabello, and M. Bourennane, Experimental device-independent certification of a symmetric, informationally complete, positive operator-valued measure, arXiv:1811.12851.

[37] M. Yamashita *et al.*, Personal communication from the SDPA collaboration.

[38] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.122.070501 for general symmetrization techniques, explicit examples and the proof of Theorem 1.

[39] S. Burgdorf and I. Klep, The truncated tracial moment problem, J. Oper. Theory, **68**, 141 (2012).

[40] D. Rosset *et al.* (to be published).

[41] C. Brukner, M. Żukowski, and A. Zeilinger, Quantum Communication Complexity Protocol with Two Entangled Qutrits, Phys. Rev. Lett. **89**, 197901 (2002).

[42] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Bell Inequalities for Arbitrarily High-Dimensional Systems, Phys. Rev. Lett. **88**, 040404 (2002).

[43] J. J. Benedetto and M. Fickus, Finite normalized tight frames, Adv. Comput. Math. **18**, 357 (2003).

[44] H. Derksen and G. Kemper, *Computational Invariant Theory* (Springer-Verlag, Berlin, Heidelberg, 2002), Vol. 130.

[45] D. F. Holt, B. Eick, and E. A. O'Brien, *Handbook of Computational Group Theory* (CRC Press, 2005).

[46] J. S. Leon, On an algorithm for finding a base and strong generating set for a group given by generating permutations, Math. Comput. **35**, 941 (1980).

[47] J.-P. Serre, *Linear Representations of Finite Groups, Graduate texts in Mathematics* (Springer, 1977).

[48] J. C. Gilbert and J. Cédric, *Plea for a Semidefinite Optimization Solver in Complex Numbers–The Full Report* (LAAS, INRIA Paris, 2017).

[49] The MOSEK optimization toolbox for MATLAB manual, Published by MOSEK ApS, Denmark. Available at http://docs.mosek.com/7.0/toolbox/index.html.

[50] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, England, 2004).

[51] I. Armeanu, About ambivalent groups, Ann. Math. Blaise Pascal **3**, 17 (1996).

[52] T. Maehara and K. Murota, A numerical algorithm for block-diagonal decomposition of matrix *-algebras with general irreducible components, Jpn. J. Indust. Appl. Math. **27**, 263 (2010).

[53] G. W. Anderson, A. Guionnet, and O. Zeitouni, *An Introduction to Random Matrices* (Cambridge University Press, Cambridge, England, 2009).

[54] K. Murota, Y. Kanno, M. Kojima, and S. Kojima, A numerical algorithm for blockdiagonal decomposition of matrix $f * g$-algebras with application to semidefinite programming, Jpn. J. Indust. Appl. Math. **27**, 125 (2010).

[55] The MATLAB package is available at https://denisrosset.github.io/qdimsum/.

[56] D. Dieks, Overlap and distinguishability of quantum states, Phys. Lett. A **126**, 303 (1988).

[57] A. Peres, How to differentiate between non-orthogonal states, Phys. Lett. A **128**, 19 (1988).

[58] R. Derka, V. Buzek, and A. K. Ekert, Universal Algorithm for Optimal Estimation of Quantum States from Finite Ensembles via Realizable Generalized Measurement, Phys. Rev. Lett. **80**, 1571 (1998).

[59] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. (N.Y.) **45**, 2171 (2004).

[60] J. Shang, A. Asadian, H. Zhu, and O. Gühne, Enhanced entanglement criterion via symmetric informationally complete measurements, Phys. Rev. A **98**, 022309 (2018).

[61] S. Gómez, A. Mattar, E. S. Gómez, D. Cavalcanti, O. Jiménez Farías, A. Acín, and G. Lima, Experimental nonlocality-based randomness generation with non-projective measurements, Phys. Rev. A **97**, 040102(R) (2018).

[62] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, Phys. Rev. Applied **7**, 054018 (2017).

[63] C. A. Fuchs, M. C. Hoang, and B. C. Stacey, The SIC question: History and state of play, Axioms **6**, 21 (2017).

[64] G. N. M. Tabia, Experimental scheme for qubit and qutrit symmetric informationally complete positive operator-valued measurements using multiport devices, Phys. Rev. A **86**, 062107 (2012).

[65] Z. E. D. Medendorp, F. A. Torres-Ruiz, L. K. Shalm, G. N. M. Tabia, C. A. Fuchs, and A. M. Steinberg, Experimental characterization of qutrits using symmetric informationally complete positive operator-valued measurements, Phys. Rev. A **83**, 051801(R) (2011).

[66] N. Bent, H. Qassim, A. A. Tahir, D. Sych, G. Leuchs, L. L. Sánchez-Soto, E. Karimi, and 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).

[67] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons, Quantum **2**, 111 (2018).

[68] W. M. Pimenta, B. Marques, T. O. Maciel, R. O. Vianna, A. Delgado, C. Saavedra, and 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).

[69] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Self-testing quantum states and measurements in the prepare-and-measure scenario, Phys. Rev. A **98**, 062307 (2018).

[70] N. Brunner, M. Navascués, and T. Vértesi, Dimension Witnesses and Quantum State Discrimination, Phys. Rev. Lett. **110**, 150501 (2013).

[71] A. Ambainis, A. Nayak, A. Ta-Shama, and U. Varizani, Dense quantum coding and quantum finite automata, J. ACM, **49**, 496 (2002).

[72] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes Using Single d-Level Systems, Phys. Rev. Lett. **114**, 170502 (2015).

[73] M. Froissart, Constructive generalization of Bells inequalities, Il Nuovo Cimento B **64**, 241 (1981).

[74] D. Rosset, N. Gisin, and E. Wolfe, Universal bound on the cardinality of local hidden variables in networks, Quantum Inf. Comput. **18**, 0910 (2018).