

Bounding the Set of Finite Dimensional Quantum Correlations

Miguel Navascués¹ and Tamás Vértesi^{2,3}

¹*Department of Physics, Bilkent University, Ankara 06800, Turkey*

²*Institute for Nuclear Research, Hungarian Academy of Sciences, P.O. Box 51, H-4001 Debrecen, Hungary*

³*Département de Physique Théorique, Université de Genève, 1211 Genève, Switzerland*

(Received 17 December 2014; published 7 July 2015)

We describe a simple method to derive high performance semidefinite programming relaxations for optimizations over complex and real operator algebras in finite dimensional Hilbert spaces. The method is very flexible, easy to program, and allows the user to assess the behavior of finite dimensional quantum systems in a number of interesting setups. We use this method to bound the strength of quantum nonlocality in Bell scenarios where the dimension of the parties is bounded from above. We derive new results in quantum communication complexity and prove the soundness of the prepare-and-measure dimension witnesses introduced in Gallego *et al.*, Phys. Rev. Lett. 105, 230501 (2010). Finally, we propose a new dimension witness that can distinguish between classical, real, and complex two-level systems.

DOI: [10.1103/PhysRevLett.115.020501](https://doi.org/10.1103/PhysRevLett.115.020501)

PACS numbers: 03.67.Mn, 03.65.Ud, 03.67.Hk

The realization that certain experimental setups can only store a finite amount of information, related to the dimensionality of the underlying quantum system [1], is one of the most surprising features of quantum theory.

Building upon this observation, quantum communication complexity studies the possibility to conduct a distributed computation when we limit the dimension of the quantum systems we allow to exchange [2,3]. Consider the following scenario: two parties, call them Alice and Bob, receive the inputs x, y , respectively. They wish to compute the Boolean function $f(x, y) \in \{0, 1\}$, for which purpose Alice is allowed to transmit Bob a D -level quantum system. The question is: given a prior distribution of the inputs $p(x, y)$, what is the maximum probability that Bob guesses the value of $f(x, y)$? More often than not, the possibility of exchanging D -dimensional quantum systems gives Alice and Bob an advantage with respect to exchanging classical variables with D possible values [4].

An upper bound on the dimension of the systems transmitted is also the basis of semidevice independent quantum key distribution (QKD) and randomness expansion [5,6]. Here the experimental setup only differs from the above one in that Alice and Bob choose the inputs x, y locally. Apart from the dimensionality D of the sent states, no assumption is made on their actual wave function, or on the nature of Bob's interaction with the quantum system, which produces an outcome b . The aim of semidevice independent QKD and semidevice independent randomness expansion is to process the variables (x, y, b) in order to distill a secret key between these two parties or generate a genuinely random string of bits, respectively. In both cases, security proofs rely on upper bounds on the maximum value of specific linear functionals of the correlations $P(b|x, y)$ achievable with D -level quantum systems.

Such upper bounds can also be used to determine the number of quantum levels that new quantum technologies can effectively manipulate, and hence assess their potential for quantum computation, or as quantum memories. Indeed, by conducting an experiment where the value of these functionals exceeds the D -dimensional limit, we can certify that the experimental setup has access to a quantum system of dimension at least $D + 1$. Lower bounds on the dimensionality of an experimental setup can be derived from prepare and measure dimension witnesses [7], such as the ones used in quantum communication complexity and semidevice independent QKD, or even better, through the degree of the violation of a Bell inequality [8–11]. This last technique has the advantage that classical degrees of freedom have no contribution on the certified dimensionality.

The above motivates the need of bounding the statistics arising from quantum systems of a given dimension. A high performance method to bound D -dimensional quantum correlations would allow us, given a functional, to upper bound its maximum value for systems of dimension D , with applications in quantum communication complexity, semidevice independent quantum information science, and experimental tests of quantum dimensionality. Unfortunately, all methods proposed so far are either very computationally demanding [8,12], cannot be shown to converge [13,14], or only apply to particular functionals of the measured probabilities [9–11,15,16].

In this Letter, we propose a simple scheme to generate semidefinite programming (SDP) [17] relaxations of dimensionally constrained problems in quantum information theory. Such relaxations, whose working principles stem from noncommutative polynomial optimization theory [18], beat all previous methods in almost all conceivable scenarios. For the sake of clarity, we have chosen to illustrate how the scheme works by applying it to

specific setups of interest in quantum information theory. For many of the problems considered, the application of any other existing numerical algorithm was not feasible due to memory or time limitations: our numerical tests must hence be regarded as new theoretical results derived with the aid of our proof system. A general approach to the noncommutative polynomial optimization problem under dimension constraints, together with an analysis of the convergence (in the sense of completeness) of the hierarchies of relaxations introduced here, will appear elsewhere [19].

Let us start by considering the problem of introducing dimension constraints in quantum nonlocality. Suppose that we wish to maximize a Bell functional $B(P) = \sum_{x,y} \sum_{a,b} B_{a,b}^{x,y} P(a,b|x,y)$ under the constraint that each party has access to a D -level quantum system. That is, we want to solve the problem

$$\begin{aligned} & \max \sum_{x,y,a,b} B_{a,b}^{x,y} P(a,b|x,y), \\ \text{s.t. } & P(a,b|x,y) = \langle \psi | E_a^x \otimes F_b^y | \psi \rangle, \end{aligned} \quad (1)$$

where $\{E_a^x, F_b^y\}$ are projection operators acting in \mathbb{C}^D , with $\sum_a E_a^x = \sum_b F_b^y = \mathbb{1}_D$, and $|\psi\rangle \in \mathbb{C}^{D^2}$.

One way to attack this problem is to simply ignore the dimension restrictions and apply the Navascués-Pironio-Acín (NPA) hierarchy of semidefinite programs for the characterization of quantum correlations [20,21].

The NPA hierarchy works by reformulating problems such as (1) as linear optimizations over the underlying system's moments $c_{\mathbb{1}} \equiv \langle \psi | \mathbb{1} | \psi \rangle, \dots, c_{F_b^y} \equiv \langle \psi | (E_a^x \otimes F_b^y) | \psi \rangle, \dots, c_{E_a^x E_{a'}^x F_b^y} \equiv \langle \psi | (E_a^x E_{a'}^x \otimes F_b^y) | \psi \rangle, \dots$

Let us group all of them in a single *moment vector* $c \equiv (c_{\mathbb{1}}, c_{F_b^y}, \dots)$, whose components are labeled by strings of operators.

It can be shown that, if we arrange the moments of order smaller than or equal to $2n$ of a quantum system as the entries of a matrix in a certain way, the resulting n th-order *moment matrix* $\Gamma_n(c)$ must be positive semidefinite [20,21]. See the Supplemental Material [22] for a precise definition of the moment matrix. The operating principle behind the NPA hierarchy is to approximate the set of feasible moments by a vector of complex numbers c , with $c_{\mathbb{1}} = 1, \Gamma_n(c) \geq 0$.

Calling m the number of moments of length smaller than or equal to $2n$, the n th order NPA relaxation to problem (1) is

$$\begin{aligned} & \max \sum_{x,y,a,b} B_{a,b}^{x,y} c_{E_a^x F_b^y} \\ \text{s.t. } & c \in \mathbb{C}^m, c_{\mathbb{1}} = 1, \Gamma_n(c) \geq 0. \end{aligned} \quad (2)$$

This happens to be a semidefinite program (SDP), a class of optimization problems for which plenty of efficient numerical tools are available [17].

Although a sound relaxation of problem (1), the NPA hierarchy is not sensitive to the dimensionality parameter D , and so it cannot be used to derive dimension witnesses. The key to go beyond the NPA approximation is to acknowledge that \mathbb{C}^m does not capture all linear restrictions present in moment vectors arising from quantum systems of dimension D . We will incorporate dimension constraints to the SDP problem (2) by characterizing exactly the span of such a set of vectors. That is, we will identify a *minimal* basis of vectors $\{c_j\}_{j=1}^N$ such that any truncated feasible moment vector c of order $2n$ arising from a D -dimensional quantum system can be expressed as $c = \sum_{j=1}^N \lambda_j c_j$, for some coefficients λ_j .

For convenience, we start by making an assumption on the *ranks* of the optimal projectors $\{E_a^x, F_b^y\}$. Calling $\mathcal{S}_{D,\bar{r}}^n$ the set of all feasible moment vectors of order $2n$ with $\text{rank}(E_a^x) = r_a^{x,x}, \text{rank}(F_b^y) = r_b^{y,y}$, the problem we wish to solve is

$$\begin{aligned} & \max \sum_{x,y,a,b} B_{a,b}^{x,y} c_{E_a^x F_b^y} \\ \text{s.t. } & c \in \mathcal{S}_{D,\bar{r}}^n, c_{\mathbb{1}} = 1, \Gamma_n(c) \geq 0. \end{aligned} \quad (3)$$

Clearly, in order to conduct this optimization, we must first identify the space $\mathcal{S}_{D,\bar{r}}^n$ of feasible moment vectors of order $2n$.

To that end, we generate randomly quantum states $|\psi^j\rangle \langle \psi^j| \in B(\mathbb{C}^{D^2})$ and projection operators $\{E_a^{x,j}, F_b^{y,j}\} \subset B(\mathbb{C}^D)$, with $\text{rank}(E_a^{x,j}) = r_a^{x,a}, \text{rank}(F_b^{y,j}) = r_b^{y,b}$. For each tuple $(|\psi^j\rangle \langle \psi^j|, E_a^{x,j}, F_b^{y,j})$ of feasible state and projectors, we build the corresponding $2n$ th order moment vector

$$c_u^j = \langle \psi^j | u(\tilde{E}_a^{x,j}, \tilde{F}_b^{y,j}) | \psi^j \rangle, \quad (4)$$

where $\tilde{E}_a^{x,j} = E_a^{x,j} \otimes \mathbb{1}_D, \tilde{F}_b^{y,j} = \mathbb{1}_D \otimes F_b^{y,j}$, and u ranges over all strings of operators of length smaller than or equal to $2n$. We thus get a sequence of random feasible moment vectors c^1, c^2, \dots . Since on one hand we are only interested in linear combinations of real entries of the system's moment vector (namely, $c_{\tilde{E}_a^x \tilde{F}_b^y}$) and, on the other hand, given a feasible tuple $(\psi^j, E_a^{x,j}, F_b^{y,j})$, its complex conjugate $(\psi^j, E_a^{x,j}, F_b^{y,j})^*$ is also feasible, it is enough to consider the real part of the above sequence, i.e., $\text{Re}(c^1), \text{Re}(c^2), \dots$

One can apply the Gram-Schmidt process to this sequence of real moment vectors in order to obtain an orthogonal basis $\tilde{c}_1, \tilde{c}_2, \dots$ for the space spanned by such vectors. We will notice that, for some number $N, \tilde{c}_{N+1} = 0$, up to numerical precision. This is the point to terminate the Gram-Schmidt process and define the normalized vectors $\{c_j \equiv (\tilde{c}_j / \sqrt{\tilde{c}_j^2}) : j = 1, \dots, N\}$. It is easy to see that, even though the basis $\{c_j\}_{j=1}^N$ was obtained randomly, the space

it represents is always the same, namely, the intersection of $\mathcal{S}_{D,\bar{r}}^n$ with \mathbb{R}^m .

Note that, alternatively, we could have reformulated the objective function as a linear combination of the entries of the moment matrix Γ_n , characterized the span of feasible n th-order moment matrices Γ_n , and carried out an optimization over all positive semidefinite matrices in such a space with $(\Gamma_n)_{1,0} = 1$. This is actually how we wrote the codes for the forthcoming numerical examples.

A brief note on strict feasibility is in order. One can show that, even if we eliminate one projection operator from each measurement as in Refs. [20,21] to remove operator dependencies, for high enough relaxation orders n there are no strictly feasible points for problem (3) [19]. In other words: there is no $s \times s$ positive definite matrix $\Gamma_n(c)$, with $c \in \mathcal{S}_{D,\bar{r}}^n$. This poses a problem for the implementation of Eq. (3), since many SDP solvers require strict feasibility to operate. An easy way to circumvent this issue is to compute the matrix $G \equiv (1/N) \sum_{i=1}^N \text{Re}[\Gamma(c^i)]$ and find an isometry $V: \text{supp}(G) \rightarrow \mathbb{R}^s$. Then, the positive semidefinite condition over $\Gamma_n(c)$ can be replaced by $V\Gamma_n(c)V^\dagger \geq 0$, which, by construction, admits a strictly feasible point.

We have just described how to perform in practice the n th order SDP relaxation of problem (3), which, in turn, is a relaxation of a rank-constrained version of problem (1). Taking the maximum over all possible rank combinations \bar{r} , we obtain an upper bound on the solution of (1).

At this point, the reader will probably wonder whether this method is actually useful for the kind of problems we usually encounter in quantum information theory. Hence, we conducted a number of optimizations over the set of D -dimensional quantum correlations in order to assess its performance. Such numerical computations, as well as all subsequent ones presented in this Letter, were carried out with the MATLAB packages YALMIP [23] and the SDP solvers SEDUMI [24] and MOSEK [25]. First we considered the I_{3322} inequality, a three-setting bipartite two-outcome Bell inequality from the I_{NN22} family, defined in Ref. [26]. Recently, it has been proven that qubit systems are not enough to attain the quantum maximum ~ 0.2509 [12,13]. Rather, the best value in $\mathbb{C}^2 \times \mathbb{C}^2$ systems is 0.25. Using Eq. (3), we certified up to 8 significant digits that the maximum is 0.25 in dimensions $\mathbb{C}^3 \times \mathbb{C}^3$ as well. The computations, which were performed on a normal desktop PC using the solver SEDUMI on third order NPA relaxation, took about 5 min for a fixed rank combination of measurements. Note that the hierarchy of Moroder *et al.* [13], by allowing the user to limit the negativity [27] of the bipartite quantum state, also gives a (not necessarily tight) lower bound on the dimension of the quantum state for a fixed Bell violation. Indeed, in the case of the I_{3322} inequality, this method works for $\mathbb{C}^2 \times \mathbb{C}^2$ systems by returning a violation of 0.25; however, it turns out not to converge for $\mathbb{C}^3 \times \mathbb{C}^3$ systems (see Fig. 1 of Ref. [13]).

We then switched to the four-setting Bell inequality defined in Ref. [12] by Eq. (19). Its maximal violation in $\mathbb{C}^2 \times \mathbb{C}^2$ systems has been upper bounded by 5.8515 [12]. However, this upper bound turns out to be not tight: using our new tool one can certify a value of 5.8310, which can be matched by seesaw variational methods [28,29]. By raising the dimension to $\mathbb{C}^3 \times \mathbb{C}^3$, one obtains the same number again, which must be compared to the maximum value of 5.9907, achievable in $\mathbb{C}^4 \times \mathbb{C}^4$ systems. In contrast to our certified value 5.8310 for qutrits, the corresponding value arising from Moroder *et al.* hierarchy [13] (on their level 2) is 5.9045.

Note that relaxation (3) is only valid under the assumption that both parties are conducting projective measurements. More general measurements are modeled in quantum theory via positive operator valued measures (POVMs), i.e., by a collection of operators $\{M_a^x\} \subset B(\mathbb{C}^D)$ with $M_a^x \geq 0$, $\sum_a M_a^x = \mathbb{1}_D$. It so happens that, for two-outcome measurements, the extreme points of the POVM set are given by projective operators. Relaxation (3) is hence sound in all such scenarios.

In order to study more complex measurement setups, we can exploit the fact that any d -outcome POVM in dimension D can be viewed as a projective measurement in an extended Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^D$ [30]. In this dilation picture, Alice and Bob's state is $|0\rangle\langle 0|_{A'} \otimes |0\rangle\langle 0|_{B'} \otimes |\psi\rangle\langle \psi|_{AB}$, with $\dim(A') = \dim(B') = d$, $\dim(A) = \dim(B) = D$, while Alice's local measurement projectors are given by $E_a^x = U^x(|a\rangle\langle a| \otimes \mathbb{1}_D)(U^x)^\dagger$, where $U^x \in B(A' \otimes A)$ is an arbitrary unitary operator (and similarly for Bob). A feasible moment vector for this system would thus be generated by sampling random unitaries U_x, V_y and states $|\psi\rangle$. In this scheme it may be convenient to introduce two different "identity operators" in our moment matrices. One of them would be the genuine identity $\mathbb{1}_{A'B'} \otimes \mathbb{1}_{AB}$ on Alice and Bob's target and ancillary states. The other one would be the projector $|0\rangle\langle 0|_{A'B'}^{\otimes 2} \otimes \mathbb{1}_{AB}$ onto Alice and Bob's target space AB .

To test the efficiency of the above method, we picked the Pironio-Bell inequality [8,31], which is the simplest tight Bell inequality beyond two-outcome inequalities. Here, Alice has three binary-outcome measurement settings, whereas Bob's first setting has binary outcomes and his second setting has ternary outcomes. By allowing general POVM measurements on Bob's second setting, we recover the two-qubit quantum maximum $(\sqrt{2} - 1)/2 \approx 0.2071$ up to 8-digit precision on level 3 of the hierarchy. Note that the overall quantum maximum is a larger value of 0.2532 which can be attained with two-qutrit systems [8].

Limiting quantum nonlocality under dimension constraints is not the only interesting problem in quantum information that can be solved with the above scheme. Consider, for instance, the problem of bounding the efficiency of quantum communication complexity. This scenario can be modeled by assuming that Bob performs a

binary measurement F_b^y over the state ρ_x sent by Alice. The outcome $b \in \{0, 1\}$ will be Bob's guess on the value of the Boolean function $f(x, y)$, which he will output with probability $P(b|x, y) = \text{tr}(\rho_x F_b^y)$. Finding the maximum probability of success hence translates into the problem

$$\begin{aligned} \max \quad & \sum_{x,y} p(x, y) \text{tr}(\rho_x F_{f(x,y)}^y), \\ \text{s.t.} \quad & \text{tr}(\rho_x) = 1, \rho_x^2 = \rho_x, (F_b^y)^2 = F_b^y, \\ & \rho_x, F_b^y \in B(\mathbb{C}^D). \end{aligned} \quad (5)$$

Here we have exploited the fact that the extreme points of the distributions $P(b|x, y)$ are generated by pure states and projective measurements. Note that the maximal value of prepare and measure dimension witnesses, as defined in Ref. [7], can also be expressed as a linear optimization over the set of feasible probabilities $P(b|x, y)$. There are many ways to reformulate problem (5): e.g., by modeling the preparation device via measurements on one side of a maximally entangled state, as in Ref. [14]. Each of them leads to a different hierarchy of SDP relaxations. Here we study the most obvious choice: namely, we regard our reference state as the unnormalized maximally mixed state in dimension D , and ρ_x , as rank-1 projectors. Hence we obtain our random basis by choosing randomly the projectors $\rho_x^j, F_b^{y,j} \in B(\mathbb{C}^D)$, with $\text{rank}(\rho_x^j) = 1, \text{rank}(F_b^{y,j}) = r_b^y$ and using them to construct the moment vectors $c_u^j = \text{tr}\{u(\rho_x^j, F_b^{y,j})\}$.

Denoting by $\mathcal{T}_{D,\vec{r}}$ the span of the real part of all such vectors, the resulting program is

$$\begin{aligned} \max \quad & \sum_{x,y} p(x, y) c_{\rho_x F_{f(x,y)}^y} \\ \text{s.t.} \quad & c \in \mathcal{T}_{D,\vec{r}}, c_0 = D, \Gamma_n(c) \geq 0. \end{aligned} \quad (6)$$

Let us explore how relaxations of the problem above performs in practice. In a quantum random access code (QRAC) [32], the inputs \vec{x}, y can take values in $\{0, 1\}^k$ and $\{1, \dots, k\}$, respectively, and the function to compute is $f(\vec{x}, y) = x_y$. If the inputs are distributed independently and uniformly and Alice is allowed to transmit Bob a D -level quantum system, the average success probability of the optimal $k \rightarrow \log_2(D)$ QRAC is usually denoted as $P_{\max}[k \rightarrow \log_2(D)]$ [33].

It was previously known that $P_{\max}(2 \rightarrow 1) = 1/2 + \sqrt{2}/4$ [32]. Actually, this is the value given by

program (6) at order $n = 2$, up to computer precision. Likewise, for $D = 3$, i.e., when we allow Alice to transmit a qutrit, program (6) at the same order gives $P_{\max} \leq 0.904\,508\,50$, which is equal up to numerical precision to the lower bound obtained via seesaw methods [28,29]. The only other feasible method to attack this problem is the Mironowicz-Li-Pawlowski (MLP) SDP hierarchy [14], whose 2nd order relaxation gives an upper bound of 0.926 835 5.

The 2nd order relaxation of Eq. (6) also performs well when we increase D and k . Table I shows bounds on the average success probability for QRAC $3 \rightarrow \log_2(D)$ for different values of D , computed via program (6) in a normal desktop (using the solver mosek [25]). It is worth noting that, except for the cases $D = 5, 6$, with gaps between the upper (UB) and lower bounds (LB) of the order of 10^{-6} and 10^{-3} , respectively, the values obtained via seesaw and Eq. (6) are equal up to numerical precision. For comparison, we also include the upper bounds (UB') derived via the second-order relaxation of the MLP method [14]. Except for $D = 2, 4$, where the outputs of both methods coincide, the new tool gives predictions $\sim 10^{-2}$ more accurate than the MLP method.

We also used program (6) to recompute the optimal quantum value of the dimension witnesses I_N defined in Ref. [7], Table I. We found that the second relaxation produced upper bounds on the maximal value of I_N that matched the lower bounds obtained via seesaw for $N = 3, 4$ and $D = 2, 3$. To appreciate the importance of these calculations, note that the conclusions of the experimental papers [34,35] relied on the conjecture that the inequality $I_4 \leq 7.9689$ cannot be violated by quantum systems of dimension $D = 3$.

So far, we have been interested in bounding the behavior of complex quantum mechanical systems, but nothing prevents us from applying the same ideas to characterize the properties of *real* quantum mechanical systems as well. Consider the dimension witness V_4 , defined in Ref. [15], and take $D = 2$. Running the SDP for the case of complex qubits, we recover the upper bound $Q_{2C} = 2\sqrt{6}$. This bound is tight and can be saturated via SIC POVMs [15]. In the real qubit case, though, we obtain the upper bound $Q_{2R} = 2(\sqrt{2} + 1)$, also tight. We obtained both results in a few seconds on a normal desktop PC by using a relaxation level intermediate between two and three.

Conclusion.—We have described a simple method to derive SDP relaxations for optimizations over operator

TABLE I. Lower and upper bounds on $P_{\max}[3 \rightarrow \log_2(D)]$.

D	2	3	4	5	6	7
LB	0.788 675	0.832 273	0.908 248	0.924 431	0.951 184	0.969 841
UB	0.788 675	0.832 273	0.908 248	0.924 445	0.954 123	0.969 841
UB'	0.788 675	0.853 553	0.908 248	0.934 264	0.957 785	0.979 567

algebras under dimension constraints. This method allows us to attack a number of relevant problems in quantum information theory, such as the characterization of quantum nonlocality under dimension constraints or the determination of the quantum communication complexity of arbitrary Boolean functions. As we saw, the method even distinguishes between real and complex algebras, and hence it can be used to certify that a given experimental setup has control over a complex D -dimensional space.

Note that one can also use the nondeterministic algorithms sketched above to identify the space spanned by tensor products $c^{\otimes k}$ of k identical moment vectors. By imposing the existence of a symmetric separable decomposition (rather than just positive semidefiniteness) over the corresponding “ k -partite” moment matrices Γ_n^k , we hence obtain a nontrivial relaxation for the convex hull of k -degree polynomials of the system’s moments. It would be interesting to explore whether this scheme leads to good outer approximations of the (nonconvex) set of D -dimensional quantum correlations.

We thank A. Winter for useful discussions. M. N. acknowledges the European Commission (EC) STREP “RAQUEL,” as well as the MINECO Projects No. FIS2008-01236 and No. FIS2013-40627-P, with the support of FEDER funds. T. V. acknowledges financial support from a János Bolyai Grant of the Hungarian Academy of Sciences, the Hungarian National Research Fund OTKA (K111734), and SEFRI (COST action MP1006).

-
- [1] A. S. Holevo, *Probl. Peredachi Inf.* **9**, 3 (1973) [*Probl. Inf. Transm.* **9**, 177 (1973)].
- [2] A. C.-C. Yao, *Proceedings of the 34th IEEE FOCS* (IEEE Computer Society Press, Los Alamitos, CA, 1993), p. 352.
- [3] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, *Rev. Mod. Phys.* **82**, 665 (2010).
- [4] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis, *Proceedings of the 36th annual ACM symposium on Theory of Computing* (ACM, New York, 2004).
- [5] M. Pawłowski and N. Brunner, *Phys. Rev. A* **84**, 010302(R) (2011).
- [6] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, *Phys. Rev. A* **85**, 052308 (2012).
- [7] R. Gallego, N. Brunner, C. Hadley, and A. Acín, *Phys. Rev. Lett.* **105**, 230501 (2010).
- [8] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, *Phys. Rev. Lett.* **100**, 210503 (2008).
- [9] K. F. Pál and T. Vértesi, *Phys. Rev. A* **77**, 042105 (2008).
- [10] S. Wehner, M. Christandl, and A. C. Doherty, *Phys. Rev. A* **78**, 062112 (2008).
- [11] J. Briët, H. Buhrman, and B. Toner, *Commun. Math. Phys.* **305**, 827 (2011).
- [12] M. Navascués, G. de la Torre, and T. Vértesi, *Phys. Rev. X* **4**, 011011 (2014).
- [13] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, *Phys. Rev. Lett.* **111**, 030501 (2013).
- [14] P. Mironowicz, H.-W. Li, and M. Pawłowski, *Phys. Rev. A* **90**, 022322 (2014).
- [15] N. Brunner, M. Navascués, and T. Vértesi, *Phys. Rev. Lett.* **110**, 150501 (2013).
- [16] J. Bowles, M. T. Quintino, and N. Brunner, *Phys. Rev. Lett.* **112**, 140407 (2014).
- [17] L. Vandenberghe and S. Boyd, *SIAM Rev.* **38**, 49 (1996).
- [18] S. Pironio, M. Navascués, and A. Acín, *SIAM J. Optim.* **20**, 2157 (2010).
- [19] M. Navascués and T. Vértesi (to be published).
- [20] M. Navascués, S. Pironio, and A. Acín, *Phys. Rev. Lett.* **98**, 010401 (2007).
- [21] M. Navascués, S. Pironio, and A. Acín, *New J. Phys.* **10**, 073013 (2008).
- [22] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.115.020501> for a definition of moment matrices and a proof of their positive semidefiniteness.
- [23] J. Löfberg, *Proceedings of the CACSD Conference* (Taipei, Taiwan, 2004).
- [24] J. F. Sturm, *Optimization Methods and Software* **11**, 625 (1999). Special issue on Interior Point Methods (CD supplement with software).
- [25] The mosek optimization toolbox for MATLAB manual. Version 7.0 (Revision 140). Published by MOSEK ApS, Denmark. <http://docs.mosek.com/7.0/toolbox/index.html>.
- [26] D. Collins and N. Gisin, *J. Phys. A* **37**, 1775 (2004).
- [27] G. Vidal and R. F. Werner, *Phys. Rev. A* **65**, 032314 (2002).
- [28] R. F. Werner and M. M. Wolf, *Quantum Inf. Comput.* **1**, 1 (2001).
- [29] K. F. Pál and T. Vértesi, *Phys. Rev. A* **82**, 022116 (2010).
- [30] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Series on Information and the Natural Sciences (Cambridge University Press, Cambridge, England, 2000).
- [31] S. Pironio, *J. Phys. A* **47**, 424020 (2014).
- [32] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, *J. ACM* **49**, 496 (2002).
- [33] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, *Phys. Rev. A* **85**, 052308 (2012).
- [34] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, *Nat. Phys.* **8**, 588 (2012).
- [35] J. Ahrens, P. Badziąg, A. Cabello, and M. Bourennane, *Nat. Phys.* **8**, 592 (2012).