# Semidefinite programming relaxations for quantum correlations

Armin Tavakoli

*Physics Department and NanoLund, Lund University, Box 118, 22100 Lund, Sweden*

Alejandro Pozas-Kerstjens

*Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland and Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM), Calle Nicolás Cabrera 13–15, 28049 Madrid, Spain*

Peter Brown

*Télécom Paris—LTCI, Inria, Institut Polytechnique de Paris, 91120 Palaiseau, France*

Mateus Araújo

*Departamento de Física Teórica, Atómica y Óptica, Universidad de Valladolid, 47011 Valladolid, Spain*

(published 4 December 2024)

Semidefinite programs are convex optimization problems involving a linear objective function and a domain of positive-semidefinite matrices. Over the past two decades, they have become an indispensable tool in quantum information science. Many otherwise intractable fundamental and applied problems can be successfully approached by means of relaxation to a semidefinite program. This methodology is reviewed here in the context of quantum correlations. The manner in which the core idea of semidefinite relaxations can be adapted is discussed for a variety of research topics in quantum correlations, including nonlocality, quantum communication, quantum networks, entanglement, and quantum cryptography.

DOI: 10.1103/RevModPhys.96.045006

**CONTENTS**



 

## I. INTRODUCTION

Understanding and explaining the correlations observed in nature is a central task for any scientific theory. For quantum mechanics the study of correlations plays a crucial role in both its concepts and its applications. It broadly concerns the foundations of quantum theory, quantum information science, and currently also the emerging quantum technologies. Although quantum correlations is an umbrella term under which many different physical scenarios are accommodated, it establishes a common focus on the investigation of probability distributions describing physical events. The various expansive topics focusing on quantum correlations have warranted review articles of their own and we refer to them for specific discussions: see Genovese (2005), Brunner *et al.* (2014), and Tavakoli, Pozas-Kerstjens *et al.* (2022) for nonlocality; Gühne and Tóth (2009), Horodecki *et al.* (2009), and Friis *et al.* (2019) for entanglement; Budroni *et al.* (2022) for contextuality; Brassard (2003), Gisin and Thew (2007), and Buhrman *et al.* (2010) for quantum communication; and Gisin *et al.* (2002), Scarani *et al.* (2009), Pirandola *et al.* (2020), Xu *et al.* (2020), and Portmann and Renner (2022) for quantum cryptography.

Studies of quantum correlations take place in a given scenario or experiment where events can influence each other according to some causal structure, and the influences are potentially subject to various physical limitations. For example, this can be a Bell experiment where two parties act outside each other's light cones but are nevertheless connected through a preshared entangled state. Another example is a communication scenario where the channel connecting the sender to the receiver supports only a given number of bits per use. The fundamental challenge is to characterize the set of correlations predicted by quantum theory. This applies directly to a variety of basic questions, such as determining the largest violation of a Bell inequality or the largest quantum-over-classical advantage in a communication task. It also applies indirectly to several problems that rely on bounding such correlations, such as benchmarking a desirable property of quantum devices or computing the secret key rate in a quantum cryptographic scheme. However, the characterization of quantum correlations is typically difficult and can be solved exactly, by analytical means, in only a handful of special cases. Therefore, it is of pivotal interest to find other, more practically viable methods for characterizing quantum correlations.

Over the past two decades, semidefinite programs (SDPs) have emerged as an efficient and broadly useful tool for investigating quantum theory in general, and quantum correlations in particular. An SDP is an optimization task in which a linear objective function is maximized over a cone of positive-semidefinite (PSD) matrices subject to linear constraints. SDPs rose to prominence in convex optimization theory in the early 1990s through the development of efficient interior-point evaluation methods; see Vandenberghe and Boyd (1996) for a review. Today they are an indispensable tool for the field of quantum correlations. However, it is frequently the case that quantum correlation problems cannot be directly cast as SDPs, thus impeding a straightforward solution. Sometimes the reason is that the problem is simply not convex, such as bilinear optimization. Sometimes the reason is that, although the problem is convex, it cannot be represented exactly as an SDP, for example, optimization of von Neumann entropy.

Nevertheless, SDPs offer a powerful path out of such difficulties because they can be employed to approximate solutions that would otherwise remain obscure. Specifically, more sophisticated quantum correlation problems that are not immediately solvable by an SDP can still be approached through sequences of increasingly precise relaxations, each of which is itself an SDP; see Fig. 1. In this way one can obtain approximations that are accurate enough for practical purposes, and sometimes even exact. From the methodology perspective these SDP relaxation methods have attained a prominent role in quantum information science. Their success derives in part from the fact that today there are powerful, practical, and easily accessible algorithms for their evaluation, and partly from the fact that they offer a single methodology that pertains to most forms of quantum correlation, even though the physics underpinning experiments can be vastly different.

The purpose of this review is to examine SDP relaxation methods for quantum correlations. We discuss how this methodology can be adapted for a variety of conceptual and applied problems. In Sec. II we introduce the basics of semidefinite programming and some of the main correlation scenarios. In Sec. III we present a general framework for semidefinite relaxation hierarchies that can be applied to many of the later, physically motivated considerations. Sections IV and V discuss SDP relaxation methods in the context of entanglement theory and nonlocality, respectively, including device-independent applications. Section VI focuses on correlations from quantum communication and their applications. Section VII concerns SDP methods for evaluating the performance of protocols in random number generation and quantum key distribution. Section VIII focuses on networks

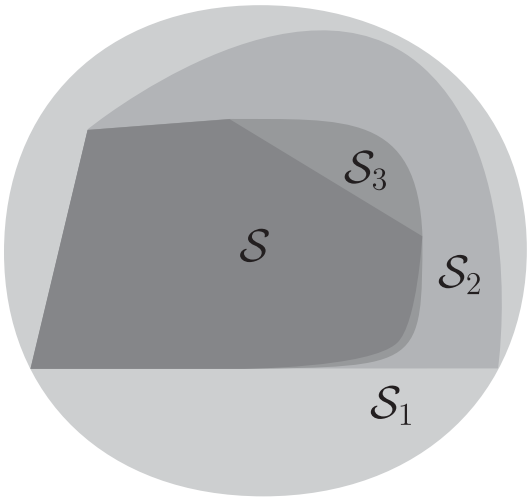


FIG. 1. Schematic representation of SDP relaxation methods. Instead of directly characterizing a complicated set $\mathcal{S}$, one approximates it with supersets $\mathcal{S}_i$, each of which can be characterized via SDP. Often there exist sequences $\{\mathcal{S}_i\}_i$ such that the next set is contained in the previous one, thus giving a more precise approximation of $\mathcal{S}$.

comprising independent sources of entanglement and discusses SDP methods for assessing their nonlocality. Section IX gives an overview of some related topics where SDP relaxations are prominent. Finally, Sec. X provides a concluding outlook. A guide to free and publicly available SDP solvers and relevant quantum information software packages is found in Appendix A.

## II. BACKGROUND

We begin with an introduction to semidefinite programming while referring the interested reader to relevant books and reviews (Wolkowicz, Saigal, and Vandenberghe, 2000; de Klerk, 2002; Boyd and Vandenberghe, 2004) for further discussions. In particular, owing to their focus on quantum correlations, we suggest Skrzypczyk and Cavalcanti (2023), who offered a didactic approach to SDP using basic quantum information tasks, and Mironowicz (2024), who explained the mathematical foundations of SDP.

### A. Primal and dual SDPs

A semidefinite program is an optimization problem in which a linear objective function is optimized over a convex domain consisting of the intersection of a cone of PSD matrices with hyperplanes and half-spaces. In general this can be written as

$$\begin{aligned} \max_X \quad & \langle C, X\rangle \\ \text{such that} \quad & \langle A_i, X\rangle = b_i \quad \forall\, i, \\ & X \succeq 0, \end{aligned} \tag{1}$$

where $C$, $X$, and $A_i$ are Hermitian matrices, $b$ is a real vector with components $b_i$, $\langle\cdot,\cdot\rangle$ denotes the inner product, and $X \succeq 0$ indicates that $X$ is PSD. In addition to the aforementioned linear equality constraints, SDPs can also include linear inequality constraints. These can always be converted into linear equality constraints, as shown in Eq. (1), by introducing additional parameters known as slack variables. While we have chosen to define SDPs as optimizations of the form presented in Eq. (1), many alternative definitions exist in the literature; see Watrous (2018) for a definition based on Hermitian-preserving maps.[1] Note, however, that all such definitions are equivalent, and, in particular, any SDP presented can be rewritten in the form of Eq. (1).

SDPs are generalizations of the more elementary linear programs (LPs) for which the PSD constraint is replaced by an elementwise positivity constraint. This is achieved by restricting the matrix $X$ to be diagonal. It is well known that LPs can be efficiently evaluated using interior-point methods (Karmarkar, 1984), and such methods also generalize to the case of SDPs (Kamath and Karmarkar, 1991, 1993; Alizadeh, 1992; Nesterov and Nemirovskii, 1994).

With every SDP of the form of Eq. (1), one can associate another SDP of the form

$$\begin{aligned} \min_y \quad & \langle b, y\rangle \\ \text{such that} \quad & \sum_i A_i y_i \succeq C, \end{aligned} \tag{2}$$

where the optimization is now over the real vector $y$ with components $y_i$. This is known as the dual SDP corresponding to the primal SDP in Eq. (1). Every feasible point of the dual SDP gives a value $\langle b, y\rangle$ that is an upper bound on the optimal value of the primal SDP. Thus, every feasible point of the primal SDP also gives a value $\langle C, X\rangle$ that is a lower bound on the optimal value of the dual SDP. This relation is known as weak duality.

A fundamental question is whether the bounds provided by weak duality can be turned into equality, i.e., when does the optimal value of the primal SDP in Eq. (1) coincide with the optimal value of the dual SDP in Eq. (2)? When they are equal we say that strong duality holds. Strong duality always holds for LPs but in general not for SDPs. However, a sufficient condition for strong duality is that the primal or dual SDP is strictly feasible (Slater, 1950): in the primal formulation (1) this means that there exists an $X^* \succ 0$ such that $\langle A_i, X^*\rangle = b_i$ for all $i$, and in the dual formulation (2) that there exists a $y^*$ such that $\sum_i A_i y_i^* \succ C$.

If one wants to solve an SDP numerically, one needs in addition for the optimal values of the primal and dual problems to be attained, i.e., that there exist finite $X$ and $y$ that produce the optimal values. A sufficient condition for their existence is that the SDP be strictly feasible and its feasible region be bounded, or that both the primal and dual problems be strictly feasible (Nesterov and Nemirovskii, 1994; Drusvyatskiy and Wolkowicz, 2017).

### B. Correlation scenarios and quantum theory

This section provides an introduction to some often studied quantum correlation scenarios. We first discuss scenarios

[1] A Hermitian-preserving map has a Hermitian Choi state representation.

based on entanglement and then address scenarios featuring communication. The presentation is geared toward highlighting the relevance of LPs and SDPs.

### 1. Entanglement-based scenarios

The standard scenario for investigating quantum correlations harvested from the shares of a bipartite state is illustrated in Fig. 2. A source emits a pair of particles in some state $\rho_{AB}$ that is shared between two parties Alice and Bob. Formally a state is a PSD operator $\rho_{AB} \succeq 0$ of unit trace $\mathrm{tr}(\rho_{AB}) = 1$. Alice and Bob can independently select classical inputs $x$ and $y$, respectively, from finite sets $X$ and $Y$ and can perform corresponding quantum measurements on their systems $A$ and $B$.

In general a quantum measurement with $N$ possible outcomes is represented by a positive operator-valued measure (POVM), i.e., a set of PSD operators $\{E_i\}_{i=1}^N$ that sums to identity: $E_i \succeq 0$ and $\sum_{i=1}^N E_i = \mathbb{1}$. These conditions ensure the positivity and normalization of probabilities, respectively. We write the measurements of Alice and Bob as POVMs $\{A_{a|x}\}$ and $\{B_{b|y}\}$, respectively, where $a$ and $b$ denote their respective outcomes. The probability distribution of their outcomes for a specific choice of inputs is given by Born's rule,

$$p(a,b|x,y) = \mathrm{tr}[(A_{a|x} \otimes B_{b|y})\rho_{AB}]. \tag{3}$$

This conditional probability distribution is interchangeably referred to as the distribution or the correlations. Such entanglement-based correlations are often studied in three different scenarios, namely, those of entanglement, steering and nonlocality.

*Entanglement*. A bipartite quantum state is called separable if it can be written as a probabilistic mixture of states individually prepared by Alice and Bob, namely (Nielsen and Chuang, 2010),

$$\rho_{AB} = \sum_\lambda p(\lambda)\phi_\lambda \otimes \varphi_\lambda, \tag{4}$$

where $p(\lambda)$ is a probability distribution and $\phi_\lambda$ and $\varphi_\lambda$ are arbitrary quantum states of Alice and Bob, respectively. Note that some bipartite states cannot be decomposed in this way and are called entangled. For a discussion of entanglement, see Horodecki *et al.* (2009).

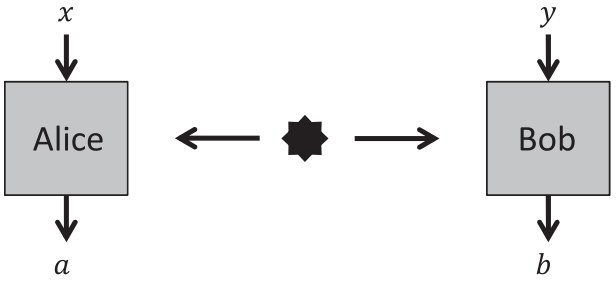


FIG. 2. The standard bipartite entanglement-based scenario. A source emits a pair of particles shared between the parties Alice and Bob. They each privately select inputs $x$ and $y$ and perform associated measurements that produce outcomes $a$ and $b$, respectively.

Assume that Alice and Bob, as in Fig. 2, perform known quantum measurements on some unknown shared state $\rho_{AB}$. Can we determine whether the state is separable or entangled? This is done by inspecting the correlations in Eq. (3). One approach is that both Alice and Bob perform a set of tomographically complete local measurements that are most prominently exemplified by a complete set of mutually unbiased bases (Ivanović, 1981; Wootters and Fields, 1989) or a symmetric, informationally complete POVM (Renes *et al.*, 2004). They can then reconstruct the density matrix $\rho_{AB}$ and try to decide its separability through some analytical criterion. However, the separability problem is known to be NP hard[2] (Gurvits, 2003; Gharibian, 2010), and a necessary and sufficient criterion is known only for qubit-qubit or qubit-qutrit systems. This is the well-known positive partial transpose (PPT) criterion (Horodecki, Horodecki, and Horodecki, 1996; Peres, 1996), which more generally is a necessary condition for separability in all dimensions: a bipartite system is entangled if $\rho_{AB}^{T_A} \not\succeq 0$, where $T_A$ denotes transposition on system $A$.[3] However, many entangled states go undetected by this criterion (Horodecki, Horodecki, and Horodecki, 1998).

The PPT criterion can be used to quantify the amount of entanglement in a quantum state, for example, by computing how much of the maximally mixed state needs to be mixed with $\rho_{AB}$ to make the resulting state PPT. Known as the random robustness of entanglement with respect to the PPT criterion, this can be computed[4] via a simple SDP (Vidal and Tarrach, 1999),

$$\begin{aligned} \max_t \quad & t \\ \text{such that} \quad & \rho_{AB}^{T_A} \succeq t\mathbb{1}. \end{aligned} \tag{5}$$

According to the previous discussion, if the optimal value of the SDP is negative, then it must be the case that the state $\rho_{AB}$ is entangled. Note that since having nonpositive partial transposition is not a necessary condition for a state to be entangled, this SDP is a relaxation of the separability problem, and the random robustness it computes is only a lower bound on the actual amount of entanglement in $\rho_{AB}$. This is a simple example of the fundamental idea behind the methods explored in this review: in order to tackle an intractable problem, one finds partial conditions for its solution that are tractable to compute and provide bounds on the quantity of interest. Ideally one should find a sequence of tighter and tighter partial conditions that in the infinite limit correspond exactly to the problem one is trying to solve. In Sec. IV.A we see how this can be done for the separability problem.

[2]More precisely, it is NP hard to decide whether a quantum state is $\epsilon$-close to the set of separable states when $\epsilon$ is an inverse polynomial of the dimension.

[3]If $\rho_{AB} = \sum_{ijkl} \rho_{ijkl}|ij\rangle\langle kl|$, then $\rho_{AB}^{T_A} = \sum_{ijkl} \rho_{ijkl}|kj\rangle\langle il|$.

[4]The random robustness is then given by $-td^2$.

It is also useful to consider the dual of the SDP in Eq. (5), namely,[5]

$$\begin{aligned} \min_{W} \quad & \mathrm{tr}(W\rho_{AB}) \\ \text{such that} \quad & \mathrm{tr}(W) = 1, \\ & W^{T_A} \succeq 0. \end{aligned} \tag{6}$$

Consider any feasible point $W$ of the dual SDP. It then follows from weak duality of SDPs that for any state $\rho_{AB}$ we have $\mathrm{tr}(W\rho_{AB})$ as an upper bound on the random robustness of entanglement. In particular, as $W$ is Hermitian and hence an observable, if we measure $W$ and find that $\mathrm{tr}(W\rho_{AB}) < 0$, this implies that the state $\rho_{AB}$ is entangled. Thus, the dual SDP provides us with an operational procedure to detect and quantify entanglement (Brandão, 2005). The operator $W$ is known as an entanglement witness (Lewenstein *et al.*, 2000; Terhal, 2000). In particular, one does not need to perform full tomography of the quantum state, which is often impractical, as the number of required measurements grows rapidly with the dimension of the state. To measure the entanglement witness, one would need to decompose it in the form $W = \sum_{a,b,x,y} c_{abxy} A_{a|x} \otimes B_{b|y}$ for some real coefficients $c_{abxy}$ and some POVMs for Alice and Bob. Such a decomposition requires in general many fewer measurements than tomography, so a witness allows to detect entanglement from partial knowledge of the quantum state.

We emphasize that entanglement witnesses do not come only from the partial transposition criterion. In principle, for any entangled state $\rho_{AB}$ one can construct a witness $W$ such that $\mathrm{tr}(W\rho_{AB}) < 0$, but for any separable state $\sigma_{AB}$ it holds that $\mathrm{tr}(W\sigma_{AB}) \geq 0$. The construction of the witness operator, however, is not straightforward. Witness methods can sometimes detect entangled states even using just two local measurement bases; see Tóth and Gühne (2005) and Bavaresco *et al.* (2018). A common approach is to construct entanglement witnesses through the estimation of the fidelity between the state prepared in the laboratory and a pure target state (Bourennane *et al.*, 2004). While this method is practical for particular types of entanglement [see Häffner *et al.* (2005), Leibfried *et al.* (2005), Lu *et al.* (2007), and Wang *et al.* (2016)], it fails to detect the entanglement of most states (Weilenmann *et al.*, 2020). Aside from using the density matrix or partial knowledge of it, determining whether a state is separable or entangled is difficult.

*Steering*. By performing measurements on her share of a suitable entangled state and keeping track of the outcome $a$, Alice can remotely prepare any ensemble of states for Bob (Gisin, 1984; Hughston, Jozsa, and Wootters, 1993). The discussion of how entanglement allows one system to influence (or steer) another system traces back to Schrödinger's remarks (Schrödinger, 1935) on the historical debate about "spooky action at a distance" (Einstein, Podolsky, and Rosen, 1935). We again consider the situation in Fig. 2, but this time we ask whether Bob can know that Alice is quantumly steering his system. The set of states remotely prepared by Alice for Bob, when her outcome is made publicly known along with the probabilities of her outcomes, is described by a set of subnormalized states of Bob $\varrho_{a|x} = \mathrm{tr}_A[(A_{a|x} \otimes \mathbb{1})\rho]$. This set is known as an assemblage (Pusey, 2013). The assemblage can be modeled without a quantum influence from Alice to Bob if there exists a local hidden state decomposition (Wiseman, Jones, and Doherty, 2007), namely,

$$\varrho_{a|x} = \sum_{\lambda} p(\lambda) p(a|x,\lambda) \sigma_{\lambda}, \tag{7}$$

for some probabilities $p(\lambda)$ and $p(a|x,\lambda)$ and quantum states $\sigma_{\lambda}$. One can interpret this as a source probabilistically generating the pair $(\lambda, \sigma_{\lambda})$, sending the former to Alice, who then classically decides her output, and delivering the latter to Bob. If no model of the form of Eq. (7) is possible, then we say that the assemblage demonstrates steering and that consequently $\rho_{AB}$ is steerable. For reviews on steering, see Cavalcanti and Skrzypczyk (2017) and Uola *et al.* (2020).

Determining the steerability of an assemblage is an SDP. To see this, note that, for a given number of inputs and outputs for Alice, there are finitely many functions $r$ mapping $x$ to $a$. Indexing them by $\lambda$, we can define deterministic distributions $D(a|x,\lambda) = \delta_{r_\lambda(x),a}$. A strictly feasible formulation of the SDP is

$$\begin{aligned} \max_{\{\tilde{\sigma}_\lambda\},t} \quad & t \\ \text{such that} \quad & \varrho_{a|x} = \sum_{\lambda} \tilde{\sigma}_\lambda D(a|x,\lambda) \quad \forall\, a,x, \\ & \tilde{\sigma}_\lambda \succeq t\mathbb{1} \quad \forall\, \lambda. \end{aligned} \tag{8}$$

A local hidden state model is possible if and only if the optimal value of Eq. (8) is non-negative. Note that normalization of the assemblage is implicitly imposed by the equality constraint.

Moreover, consider the SDP dual to Eq. (8),

$$\begin{aligned} \min_{\{W_{a,x}\}} \quad & \sum_{a,x} \mathrm{tr}(W_{a,x}\varrho_{a|x}) \\ \text{such that} \quad & \sum_{a,x,\lambda} \mathrm{tr}(W_{a,x}) D(a|x,\lambda) = 1, \\ & \sum_{a,x} W_{a,x} D(a|x,\lambda) \succeq 0 \quad \forall\, \lambda. \end{aligned} \tag{9}$$

The first constraint is a normalization for the dual variables $\{W_{a,x}\}$, and the second constraint ensures that all local hidden state models return non-negative values. Thus, if the assemblage demonstrates steering, the dual gives us an inequality

$$\sum_{a,x} \mathrm{tr}(W_{a,x}\varrho_{a|x}) \geq 0 \tag{10}$$

that is satisfied by all local hidden state models and violated, in particular, by the assemblage $\{\varrho_{a|x}\}$, but also by some other assemblages. Indeed, the inequality (10) can be viewed as the steering equivalent of an entanglement witness [recall Eq. (6)],

[5]Note that a direct application of the definition of dual would give $W^{T_A}$ as the optimization variable instead of $W$, so we changed it for convenience. Throughout the review we make such trivial simplifications without comment.

i.e., a steering witness. However, we note that steering is a stronger notion than entanglement because it is established only from inspecting the assemblage; i.e., Bob's measurements are assumed to be characterized, whereas Alice's measurements need not even follow Born's rule. Note that as in the case of entanglement witnesses one does not need to perform full tomography of Bob's states to test steering witnesses.

*Nonlocality.* Bell's theorem (Bell, 1964) proclaims that there exist quantum correlations (3) that cannot be modeled in any theory respecting local causality[6] (Bell, 1975). Such a theory, known as a local hidden variable (LHV) model, assigns the outcomes of Alice and Bob based on their respective inputs and some shared classical information $\lambda$. A local model for their correlation takes the form

$$p(a,b|x,y)=\sum_{\lambda}p(\lambda)p(a|x,\lambda)p(b|y,\lambda). \tag{11}$$

Correlations admitting such a decomposition are called local, whereas those that do not are called nonlocal. For discussions of nonlocality, see Brunner *et al.* (2014) and Scarani (2019).

The response functions $p(a|x,\lambda)$ and $p(b|y,\lambda)$ can be written as probabilistic combinations of deterministic distributions, but, in analogy with the case of the local hidden state model, any randomness can be absorbed into $p(\lambda)$. Thus, without loss of generality we can focus on deterministic response functions and their convex combinations enabled by the shared common cause. Geometrically the set of local correlations forms a convex polytope (Fine, 1982). Deciding whether a given distribution $p(a,b|x,y)$ is local can therefore be cast as an LP,

$$\begin{aligned}\max_{\{p(\lambda)\},t}\quad & t\\ \text{such that}\quad & \sum_{\lambda}p(\lambda)D(a|x,\lambda)D(b|y,\lambda)=p(a,b|x,y),\\ & p(\lambda)\geq t\quad\forall\,\lambda,\end{aligned} \tag{12}$$

where the cardinality of $\lambda$ is the total number of deterministic distributions. The correlations are local if and only if the optimal value of Eq. (12) is non-negative. As before, it is also interesting to consider the dual LP,

$$\begin{aligned}\min_{\{c_{abxy}\}}\quad & \sum_{a,b,x,y}c_{abxy}p(a,b|x,y)\\ \text{such that}\quad & \sum_{\lambda,a,b,x,y}c_{abxy}D(a|x,\lambda)D(b|y,\lambda)=1,\\ & \sum_{a,b,x,y}c_{abxy}D(a|x,\lambda)D(b|y,\lambda)\geq 0\quad\forall\,\lambda.\end{aligned} \tag{13}$$

This is reminiscent of the steering dual in Eq. (9). The first constraint normalizes the coefficients $\{c_{abxy}\}$, and the second constraint ensures that if $p(a,b|x,y)$ is local, then the value of the dual is non-negative. Hence, this implies the inequality

$$\sum_{a,b,x,y}c_{abxy}p(a,b|x,y)\geq 0, \tag{14}$$

which is satisfied by all local distributions and violated by some nonlocal distributions, in particular, the target distribution $p(a,b|x,y)$ whenever it is nonlocal. This can be seen as the nonlocality equivalent of an entanglement and steering witness, but inequalities like Eq. (14) are more well known under the name Bell inequalities. The violation of a Bell inequality in quantum theory is the strongest sense of entanglement certification, as it requires no assumptions on the measurements of Alice or Bob.

The most famous and widely used Bell inequality is the Clauser-Horne-Shimony-Holt (CHSH) inequality (Clauser *et al.*, 1969). It applies to the simplest scenario in which nonlocality is possible, namely, when Alice and Bob have two inputs each ($x,y\in\{0,1\}$) and two possible outcomes each ($a,b\in\{0,1\}$). The CHSH inequality reads[7]

$$S_{\mathrm{CHSH}}\equiv\sum_{a,b,x,y}(-1)^{a+b+xy}p(a,b|x,y)\leq 2. \tag{15}$$

Equation (15) is equivalent to the historical formulation of this inequality in terms of expectation values of observables, $\langle A_0B_0\rangle+\langle A_0B_1\rangle+\langle A_1B_0\rangle-\langle A_1B_1\rangle\leq 2$. For this reformulation, one simply writes $p(a,b|x,y)=(1+(-1)^a\langle A_x\rangle+(-1)^b\langle B_y\rangle+(-1)^{a+b}\langle A_xB_y\rangle)/4$ by inverting the definition of expectation value. A quantum model based on a singlet state and particular pairs of anticommuting qubit measurements can achieve the violation $S_{\mathrm{CHSH}}=2\sqrt{2}$. This is the maximum violation achievable with quantum systems (Tsirelson, 1980).

More generally one can employ a simple optimization heuristic known as seesaw (Werner and Wolf, 2001; Liang and Doherty, 2007; Pál and Vértesi, 2010) to search for the largest quantum violation of any given Bell inequality. Formally this is obtained by replacing $p(a,b|x,y)$ with Born's rule in the left-hand side of Eq. (14) and optimizing over the state and measurements. The main observation is that for a fixed state and fixed measurements on, say, Bob's side, the optimal value of the resulting object is a linear function of Alice's measurements and thus can be evaluated[8] as the SDP (Audenaert and De Moor, 2002)

$$\begin{aligned}\max_{\{A_{a|x}\}}\quad & \sum_{a,b,x,y}c_{abxy}\mathrm{tr}(A_{a|x}\otimes B_{b|y}\rho_{AB})\\ \text{such that}\quad & \sum_{a}A_{a|x}=\mathbb{1}\quad\forall\,x,\\ & A_{a|x}\succeq 0\quad\forall\,a,x.\end{aligned} \tag{16}$$

Given the optimized POVMs of Alice, an analogous SDP then evaluates the optimal value of the Bell parameter over Bob's POVMs. Given the optimized POVMs of Alice and Bob, the

[6]A discussion of the historical debate on the interpretation of Bell's theorem was given by Laudisa (2023).

[7]Note, in contrast to Eq. (14), that the right-hand side is nonzero and the inequality sign is flipped. This is only a matter of convention. The notation of Eq. (15) can be obtained from Eq. (14) by setting $c_{abxy}=1/2-(-1)^{a+b+xy}$.

[8]When the outcomes are binary, this is simply an eigenvalue problem and hence does not require an SDP formulation.

optimal state can then be obtained as an eigenvector with maximal eigenvalue of the operator[9]

$$\mathcal{S} = \sum_{a,b,x,y} c_{abxy} A_{a|x} \otimes B_{b|y}. \tag{17}$$

One then starts with a random choice for the state and measurements and iterates the three optimizations until the value of the Bell parameter converges. From any starting point it will converge monotonically to a local optimum, but one cannot guarantee that it will reach the global optimum, i.e., the largest quantum value. Nevertheless, this heuristic is useful in practice, and when repeated with several different starting points it often does find the optimal quantum model.

Notably, the routine can be reduced to only two optimizations per iteration. This is achieved by considering the measurements of only one party and the ensemble of subnormalized states remotely prepared by the other party (i.e., the assemblage). Optimization over the latter can also be cast as the SDP

$$\begin{aligned} \max_{\{\varrho_{a|x}\}} \quad & \sum_{a,b,x,y} c_{abxy} \mathrm{tr}(\varrho_{a|x} B_{b|y}) \\ \text{such that} \quad & \sum_a \varrho_{a|x} = \sum_a \varrho_{a|x'} \quad \forall\, x, x', \\ & \sum_a \mathrm{tr}(\varrho_{a|x}) = 1 \quad \forall\, x, \\ & \varrho_{a|x} \succeq 0 \quad \forall\, a, x. \end{aligned} \tag{18}$$

Equation (18) seems to be part of the folklore; the earliest mention we are aware of was given by Quintino, Vértesi, and Brunner (2014) in their Appendix C. The crucial point is that every assemblage has a quantum realization. This is a well-known consequence of the Schrödinger-Gisin-Hughston-Jozsa-Wootters theorem (Schrödinger, 1935; Gisin, 1984; Hughston, Jozsa, and Wootters, 1993), as discussed by Sainz *et al.* (2015).

One is often interested in the maximal value of a Bell inequality when the correlations are not constrained to come from LHVs or quantum theory, but only to obey the principle of no signaling. No signaling is the assumption that the one party's outcome cannot depend on the input of the other, which can be physically justified through spacelike separation of the parties. This is formalized as

$$\begin{aligned} \sum_b p(a,b|x,y) &= \sum_{b'} p(a,b'|x,y') \quad \forall\, a, x, y, y', \\ \sum_a p(a,b|x,y) &= \sum_{a'} p(a',b|x',y) \quad \forall\, b, x, x', y. \end{aligned} \tag{19}$$

Since these conditions are linear, the set of all distributions satisfying them (known as no-signaling correlations) can be characterized by LP. The maximal value that one obtains is in general larger than with LHVs or quantum theory. For instance, no-signaling correlations can achieve the higher-than-quantum CHSH violation of $S_{\mathrm{CHSH}} = 4$ (Khalfin and Tsirelson, 1985; Popescu and Rohrlich, 1994).

[9]As any maximal eigenvalue problem, this can also be formulated as an SDP by computing the maximum of $\mathrm{tr}(\rho\mathcal{S})$ such that $\rho \succeq 0$ and $\mathrm{tr}(\rho) = 1$.

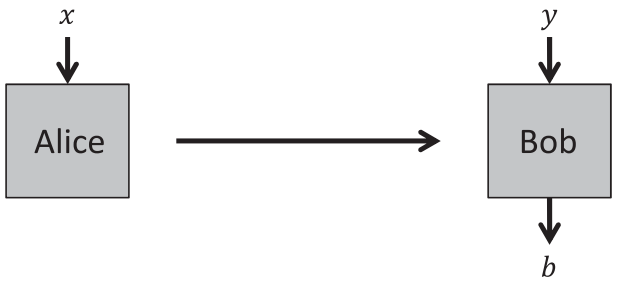


FIG. 3. The standard communication scenario. A sender (Alice) and a receiver (Bob) hold inputs $x$ and $y$, respectively. Alice chooses a message that is sent to and measured by Bob, producing an outcome $b$.

### 2. Communication-based scenarios

An important family of scenarios is those in which physical systems are not shared, but instead communicated from some parties to others. The simplest communication scenario is known as the prepare-and-measure scenario, which is illustrated in Fig. 3. A sender Alice privately selects an input $x$ and encodes it in a message that is sent over a communication channel to a receiver Bob, who privately selects an input $y$ and performs an associated decoding to receive an outcome $b$. In a quantum model, the message is described by a quantum state, i.e., $\rho_x$, and the measurements are described by POVMs $\{M_{b|y}\}$. Hence, the scenario amounts to preparing a number of different quantum states labeled $x$, and then measuring them with a number of different measurement settings labeled $y$. The quantum correlations established are given by Born's rule,

$$p(b|x,y) = \mathrm{tr}(\rho_x M_{b|y}). \tag{20}$$

In contrast, a classical model describes the messages as distinguishable and can without loss of generality be assigned integer values, but potentially also mixed via classical randomness. When the notations of quantum models are adopted, such classical messages are written $\rho_x = \sum_m p(m|x)|m\rangle\langle m|$ for some conditional message distribution $p(m|x)$. Since classical models admit no superpositions, all classical measurements are restricted to the same basis, namely, $M_{b|y} = \sum_m p(b|y,m)|m\rangle\langle m|$. Moreover, it is common to also consider a shared classical cause $\lambda$ between Alice and Bob. Following Born's rule, classical correlations then take the form

$$p(b|x,y) = \sum_{m,\lambda} p(\lambda) p(m|x,\lambda) p(b|y,m,\lambda). \tag{21}$$

Any correlation that does not admit such a model is called nonclassical. For the correlations to be interesting, a restricting assumption must be introduced. Otherwise, Alice can always send $x$ to Bob, who can then output $b$ according to any desired $p(b|x,y)$. Typically the restriction is put on the channel connecting the parties. For this purpose various approaches

have been proposed, all of which are closely linked to SDP techniques. We discuss them in Sec. VI.C.1.

Here we exemplify the most well-studied case, namely, when the Hilbert space dimension of the message is assumed or, equivalently, for classical models when the cardinality of the message alphabet is known. For a classical model with a message alphabet of size $d$, the set of correlations in Eq. (21) can be described by an LP (Gallego *et al.*, 2010). In analogy with discussions in Sec. II.B.1, any randomness in the encoding function $p(m|x,\lambda)$ and the decoding function $p(b|y,m,\lambda)$ can be absorbed into $p(\lambda)$. Since $d$ is fixed, there are only finitely many different encoding and decoding functions, which can be enumerated by $\lambda$. The LP for deciding whether a given $p(b|x,y)$ admits a classical model based on a $d$-dimensional message is

$$\begin{aligned} \max_{\{p(\lambda)\},t} \quad & t \\ \text{such that} \quad & \textstyle\sum_{\lambda} p(\lambda) \sum_{m=1}^{d} D(m|x,\lambda) D(b|y,m,\lambda) = p(b|x,y), \\ & p(\lambda) \geq t \quad \forall\, \lambda, \end{aligned} \tag{22}$$

where the normalization of $p(\lambda)$ is implicit in the equality constraint. For reasons analogous to the discussion of local models, the dual of this LP when $p(b|x,y)$ is nonclassical provides a hyperplane in the space of correlations that separates it from the classical polytope, i.e., an inequality of the form

$$S \equiv \sum_{b,x,y} c_{bxy}\, p(b|x,y) \geq 0, \tag{23}$$

for some coefficients $\{c_{bxy}\}$, satisfied by all classical models based on $d$-dimensional messages but violated by the target nonclassical distribution.

It is known that correlations obtained from $d$-dimensional quantum systems can violate the limitations of $d$-dimensional classical messages. The earliest example, based on comparing a bit message against a qubit message, was given by Wiesner (1983) and later rediscovered by Ambainis *et al.* (2002). This is known as a quantum random access code. To see that it is possible, consider that Alice holds two bits, $x = x_0 x_1 \in \{0,1\}^2$, and Bob holds one bit, $y \in \{0,1\}$, and that Bob is asked to output the value of Alice's $y$th bit. However, Alice may send only one (qu)bit to Bob. Classically one can convince oneself that on average the success probability can be no larger than $p_{\text{suc}} \equiv (1/8)\sum_{x_0,x_1,y} p(b = x_y|x_0,x_1,y) \leq 3/4$. This is achieved by Alice sending $x_0$ and Bob outputting $b = x_0$, irrespective of $y$. In contrast, a quantum model can achieve $p_{\text{suc}} = (1/2)(1 + 1/\sqrt{2})$ by having Bob measure the Pauli observables $\sigma_X$ and $\sigma_Z$ while Alice communicates the qubit states with Bloch vectors,[10] $((-1)^{x_0}, 0, (-1)^{x_1})/\sqrt{2}$. Such quantum communication advantages are also known to exist for any value of $d$ (Brunner, Navascués, and Vértesi, 2013; Tavakoli *et al.*, 2015).

If we are given an inequality of the form of Eq. (23) and asked to violate it in quantum theory, we can use a seesaw heuristic to numerically search for the optimal value of $S$ in analogy with the case of Bell inequalities (Tavakoli *et al.*, 2017). In the prepare-and-measure scenario, the optimization of $S$ becomes an SDP when the states $\rho_x$ are fixed, and a simple set of eigenvalue problems when the measurements $M_{b|y}$ are fixed. Specifically, for fixed states the problem becomes[11]

$$\begin{aligned} \max_{\{M_{b|y}\}} \quad & \textstyle\sum_{b,x,y} c_{bxy} \operatorname{tr}(\rho_x M_{b|y}) \\ \text{such that} \quad & \textstyle\sum_{b} M_{b|y} = \mathbb{1} \quad \forall\, y, \\ & M_{b|y} \succeq 0, \end{aligned} \tag{24}$$

and for fixed measurements it reduces to computing the eigenvectors with a maximal eigenvalue of the operators

$$\mathcal{S}_x = \sum_{b,y} c_{bxy} M_{b|y} \tag{25}$$

for each $x$. Thus, by starting from a randomized initial set of states, one can run the SDP in Eq. (24) and use the returned measurements to compute the optimal states from Eq. (25). The process is iterated until the value converges.

### C. Overview of semidefinite relaxation hierarchies

In Sec. II.B we saw how some classical correlation sets can be characterized via LPs and how SDPs facilitate some quantum correlation problems. However, the characterization of the set of quantum correlations in most scenarios cannot be achieved with a single SDP, but rather requires SDP relaxation hierarchies. These relaxation hierarchies and their applications are a major focus of the upcoming sections. Here we provide in Table I an overview of SDP relaxation hierarchies encountered in the study of quantum correlations, the scenario to which they apply, their convergence properties, their main domain of application, and the section in which they are further discussed. The overview is not comprehensive, as there are other correlation scenarios where such techniques apply; some of them are discussed in Sec. IX. Furthermore, the hierarchies are not unique: there can be several different SDP hierarchies addressing the same problem, as is the case in the two final rows of Table I.

Whether an SDP hierarchy converges to the targeted set of correlations is an interesting question, but it can come with noteworthy subtleties. For instance, as we will see later, in Bell nonlocality the tensor-product structure of the Hilbert space is relaxed to a single-system commutation condition. Several hierarchies converge to the latter characterization, which is known to be a strict relaxation of the bipartite tensor-product structure when infinite-dimensional systems are considered

[10] The Bloch vector of a qubit state $\rho$ uniquely determines the state and is given by $(\operatorname{tr}(\rho\sigma_X), \operatorname{tr}(\rho\sigma_Y), \operatorname{tr}(\rho\sigma_Z))$.

[11] When the outcomes are binary, this too is an eigenvalue problem and hence does not require an SDP formulation.

TABLE I. Overview of some of the SDP relaxation hierarchies for quantum correlations. Presented are the main reference, the considered correlation scenario, whether convergence to the quantum set is known to hold (✓) or it is unknown whether it holds (?), the main domain of application, and the relevant section of this review in which the hierarchy is discussed. The symbol ✓* indicates that convergence is achieved to the set of quantum correlations under the additional relaxation at which the tensor-product structure of the Hilbert space is replaced by a commutation structure.

| Reference | Scenario | Convergence | Selected application | Section |
|---|---|---|---|---|
| Navascués, Pironio, and Acín (2008) | Bell nonlocality | ✓* | Bell correlations | V.A |
| Moroder *et al.* (2013) | Bell nonlocality | ✓ | Entanglement quantification | V.B.3 |
| Doherty, Parrilo, and Spedalieri (2004) | Entanglement | ✓ | Entanglement detection | IV.A |
| Navascués and Vértesi (2015) | Bell nonlocality | ✓ | Dimension restrictions | V.B.2 |
| Navascués and Vértesi (2015) | Prepare and measure | ? | Dimension restrictions | VI.B.1 |
| Tavakoli, Zambrini Cruzeiro *et al.* (2022) | Prepare and measure | ? | Information restrictions | VI.C.1 |
| Tavakoli, Pauwels *et al.* (2021) | Entanglement-assisted prepare and measure | ✓ | Dimension restrictions | VI.B.3 |
| Brown, Fawzi, and Fawzi (2024) | Bell nonlocality | ? | Quantum key distribution | VII.A.2 |
| Pozas-Kerstjens *et al.* (2019) | Network nonlocality | ✓* | Network Bell tests | VIII.B.1 |
| Wolfe, Spekkens, and Fritz (2019) | Network nonlocality | ✓ | Causal inference network Bell tests | VIII.A |
| Wolfe *et al.* (2021) | Network nonlocality | ✓* | Causal inference network Bell tests | VIII.A |
| Ligthart, Gachechiladze, and Gross (2023)[a] | Network nonlocality | ✓ | Causal inference network Bell tests | VIII.A |
| Tavakoli, Zambrini Cruzeiro *et al.* (2021) | Prepare and measure | ? | Operational contextuality | IX.E |
| Chaturvedi, Farkas, and Wright (2021) | Prepare and measure | ? | Operational contextuality | IX.E |

[a]Note that this is a hierarchy of LPs that characterizes classical correlations.

(Ji *et al.*, 2020). Even if a hierarchy converges to the quantum set, but also when it does not, what is often of practical interest is how fast useful correlation bounds can be obtained since it is commonly the case that one cannot evaluate more than a few levels of relaxation.

## III. SEMIDEFINITE RELAXATIONS FOR POLYNOMIAL OPTIMIZATION

In this section we review the mathematical preliminaries for some of the SDP relaxation methods used in the subsequent sections. A crucial fact about SDPs is that they can be used to approximate solutions to optimization problems that themselves are not SDPs. That is, some optimization problems can be relaxed into a sequence, or hierarchy, of increasingly complex SDPs, each providing a more accurate bound on the solution than the previous one.

One example of this is polynomial optimization, which can be relaxed to a sequence of SDPs via the so-called moment approach, or its dual, known as *sum-of-squares programming*. Considering the various semidefinite programming relaxations discussed in this review, many of them fall into this framework of semidefinite relaxations for polynomial optimization. In such cases the original problem can be either viewed as or closely approximated by some polynomial optimization problem that can then be transformed into an SDP hierarchy via the aforementioned methods. In fact, polynomial optimization is at the core of many of the results discussed in the remaining sections. In light of this we now give an overview of the SDP relaxations of such optimization problems.

### A. Commutative polynomial optimization

Consider the following optimization problem:

$$\begin{aligned} \max_{\{x_j\}} \quad & f(x_1,\ldots,x_n) \\ \text{such that} \quad & g_i(x_1,\ldots,x_n)\geq 0 \quad \forall\, i, \end{aligned} \tag{26}$$

where $f$ and $g_i$ are polynomials in the variables $x_1,\ldots,x_n\in\mathbb{R}$. This type of problem is known as a commutative *polynomial optimization* problem. Apart from the applications discussed in this review, this family of optimization problems has found applications in control theory (Henrion and Garulli, 2005), probability theory (Bertsimas and Popescu, 2005), and machine learning (Hopkins *et al.*, 2016). However, polynomial optimization is known to be NP hard (Nesterov, 2000). The moment and sum of square hierarchies, which were first proposed by Parrilo (2000) and Lasserre (2001), offer a recipe to formulate a sequence of SDPs that under mild conditions will converge to the optimal value of Eq. (26). We now describe both hierarchies; see Laurent (2009) for a more precise treatment.

#### 1. Moment matrix approach

The moment matrix approach, commonly known as the Lasserre hierarchy, relaxes Eq. (26) into a sequence of SDPs. In the following we describe how these relaxations can be constructed, and toward this goal we must first introduce some notation. A monomial is any product of the variables $\{x_j\}_j$, and the length of a monomial denotes the number of terms in the product; for example, $x_1x_3^2$ has a length of 3 and $x_4x_5x_6^3$ has a length of 5. We define the constant 1 to have a length of 0. For $k\in\mathbb{N}$ let $\mathcal{S}_k$ denote the set of monomials with a length no larger than $k$. For a feasible point $x=(x_1,\ldots,x_n)$ of the problem (26), we define its moment matrix of level $k$, $G^k$, as a matrix indexed by monomials in $\mathcal{S}_k$ whose element in position $(u,v)$ is given by

$$G^k(u,v)=u(x)v(x), \tag{27}$$

where $u,v\in\mathcal{S}_k$. One crucial feature of moment matrices is that they are necessarily positive semidefinite, as

$$G^k=\left(\sum_u u(x)|u\rangle\right)\left(\sum_{u'}u'(x)|u'\rangle\right)^\dagger. \tag{28}$$

Furthermore, the value of any polynomial of degree no larger than $2k$ can be evaluated at the point $x$ by an appropriate linear combination of the elements of $G^k$. Thus, by taking $k$ to be large enough, the value of $f(x_1, \ldots, x_n)$ can be reconstructed from the moment matrix.

In addition to $G^k$, for each $g_i$ appearing in the constraints of Eq. (26) we introduce a *localizing moment matrix* of a level $k_i \in \mathbb{N}$, denoted $G^{k_i}_{g_i}$, which will act as a relaxation of the constraint $g_i(x) \geq 0$. This new matrix is indexed by elements of $\mathcal{S}_{k_i}$, and the element at index $(u, v)$ is given by

$$G^{k_i}_{g_i}(u, v) = u(x)v(x)g_i(x). \tag{29}$$

One natural choice of $k_i$ is $\lfloor k - \deg(g_i)/2 \rfloor$ since this ensures that the polynomial $u(x)v(x)g_i(x)$ is of a degree small enough to be expressed as a linear combination of the elements of the original moment matrix $G^k$. We assume in the remainder of this section that $k_i$ is chosen this way; see the remark in Sec. III.B.2 for a further discussion on choices of indexing sets. Finally, for any feasible point $(x_1, \ldots, x_n)$ of Eq. (26), one again necessarily has $G^{k_i}_{g_i} \succeq 0$.

The core idea of the Lasserre hierarchy is that, instead of directly optimizing Eq. (26), for each level $k$ one can optimize over all PSD matrices that satisfy the same constraints as the level-$k$ moment matrices of a feasible point of Eq. (26). When taking $k$ large enough so that all the polynomials in the problem can be expressed as linear combinations of the moment matrix elements, for example, $f(x) = \sum_{u,v \in \mathcal{S}_k} c_{uv} u(x)v(x)$ for some coefficients $c_{uv} \in \mathbb{R}$, then one arrives at the semidefinite program

$$\begin{aligned} \max \quad & \sum_{u,v \in \mathcal{S}_k} c_{uv} G^k(u, v) \\ \text{such that} \quad & G^k \succeq 0, \\ & G^{k_i}_{g_i} \succeq 0 \quad \forall\, i, \end{aligned} \tag{30}$$

where there are many implicit equality constraints relating the elements of $G^{k_i}_{g_i}$ matrices to linear combinations of the elements of $G^k$. There are other constraints based on the construction of the moment matrices, for example, $G^k(uw, v) = G^k(u, wv)$ for all monomials $u$, $v$, and $w$ such that $uw, wv \in S_k$, as well as the normalization constraint $G^k(1, 1) = 1$. Note that, as every feasible point of Eq. (26) defines a feasible point of Eq. (30), this new optimization problem is a relaxation, and its optimal value constitutes an upper bound on the optimal value of Eq. (26). Furthermore, Lasserre (2001) proved that under certain conditions the sequence of optimal values of Eq. (30) indexed by the relaxation level $k$ will converge to the optimal value of Eq. (26). Note, however, that the size of the SDPs grows rapidly[12] with $k$. Nevertheless, in many practical problems of interest, it has been observed that small relaxation levels can give accurate, and sometimes tight, bounds.

To better illustrate this method, we demonstrate its use in the following problem:

$$\begin{aligned} \max \quad & x_2^2 - x_1 x_2 - x_2 \\ \text{such that} \quad & x_1 - x_1^2 \geq 0, \\ & x_2 - x_2^2 \geq 0. \end{aligned} \tag{31}$$

The monomial set for level $k = 1$ is $\mathcal{S}_1 = \{1, x_1, x_2\}$. The corresponding relaxation of Eq. (31) at this level[13] is the SDP

$$\begin{aligned} \max \quad & y_{22} - y_{12} - y_{02} \\ \text{such that} \quad & \begin{pmatrix} 1 & y_{01} & y_{02} \\ & y_{11} & y_{12} \\ & & y_{22} \end{pmatrix} \succeq 0, \\ & y_{01} - y_{11} \geq 0, \\ & y_{02} - y_{22} \geq 0, \end{aligned} \tag{32}$$

which has an optimal value of $1/8$. The monomial set for the second level $k = 2$ is $\mathcal{S}_2 = \{1, x_1, x_2, x_1^2, x_1x_2, x_2^2\}$, and the corresponding relaxation is

$$\begin{aligned} \max \quad & y_{05} - y_{04} - y_{02} \\ \text{such that} \quad & \begin{pmatrix} 1 & y_{01} & y_{02} & y_{03} & y_{04} & y_{05} \\ & y_{03} & y_{04} & y_{13} & y_{14} & y_{15} \\ & & y_{05} & y_{14} & y_{15} & y_{25} \\ & & & y_{33} & y_{34} & y_{35} \\ & & & & y_{35} & y_{45} \\ & & & & & y_{55} \end{pmatrix} \succeq 0, \\ & \begin{pmatrix} y_{01} - y_{03} & y_{03} - y_{13} & y_{04} - y_{14} \\ & y_{13} - y_{33} & y_{14} - y_{34} \\ & & y_{15} - y_{35} \end{pmatrix} \succeq 0, \\ & \begin{pmatrix} y_{02} - y_{05} & y_{04} - y_{15} & y_{05} - y_{25} \\ & y_{14} - y_{35} & y_{15} - y_{45} \\ & & y_{25} - y_{55} \end{pmatrix} \succeq 0. \end{aligned} \tag{33}$$

At this level one can now see how the entries of the localizing moment matrices are linear combinations of the elements of the original moment matrix. If we solve Eq. (33) numerically, we find that it gives an objective value of 0.000 021. In particular, as we increase the relaxation level, the objective values converge toward the optimal value of the original problem, which is 0 and is achieved when $x_1 = 0$ and $x_2 = 1$.

### 2. Sum-of-squares approach

The problems dual to the moment matrix relaxations also have an interesting interpretation in terms of optimizing over sum-of-squares (SOS) polynomials (Parrilo, 2000); see also Laurent, 2009 for a discussion on the duality of the two approaches. A polynomial $p(x)$ is an SOS polynomial if it can be written as $p(x) = \sum_i r_i(x)^2$ for some polynomials $r_i(x)$. Note that an SOS polynomial is necessarily non-negative, i.e.,

[12]The moment matrix of level $k$ is of the size $|\mathcal{S}_k| \times |\mathcal{S}_k|$, with $|\mathcal{S}_k| = (k + n - 1)!/[(n - 1)!k!]$.

[13]Throughout this review when representing Hermitian matrices, we omit the elements below the diagonal since they are determined by the elements above the diagonal.

$p(x) \geq 0 \ \forall x$. We can therefore upper bound our original problem, given in Eq. (26), via the SOS problem

$$\begin{aligned} \min \quad & \lambda \\ \text{such that} \quad & \lambda - f(x) = s_0(x) + \textstyle\sum_{i=1}^{n-1} s_i(x) g_i(x), \\ & s_j \in \mathrm{SOS} \quad \forall\, j = 0, \ldots, n-1, \\ & \lambda \in \mathbb{R}, \end{aligned} \tag{34}$$

where the optimization is over $\lambda$ and the SOS polynomials $s_j$. Note that whenever we have an $x$ such that $g_i(x) \geq 0$ for every $i$ [i.e., $x$ is a feasible point of Eq. (26)] we know that the right-hand side of the equality constraint must be non-negative, and hence $f(x) \leq \lambda$. Therefore, this dual problem gives an upper bound on the maximum of $f(x)$. Like the original problem (26), this is not necessarily an easy problem to solve. Nevertheless, one can again relax it to a hierarchy of SDPs.

The key idea is to note that, for any SOS polynomial $p(x)$, one can always write it in the form $p(x) = w^T M w$, where $M$ is a PSD matrix and $w$ is a vector of monomials. Thus, one can obtain a hierarchy of relaxations by bounding the length of the monomials in the vector $w$. Let $\mathrm{SOS}_k$ be the set of all the SOS polynomials generated when $w$ is the vector of all the monomials in $\mathcal{S}_k$. We then have the following hierarchy of relaxations for $k \in \mathbb{N}$:

$$\begin{aligned} \min \quad & \lambda \\ \text{such that} \quad & \lambda - f(x) = s_0(x) + \textstyle\sum_{i=1}^{n-1} s_i(x) g_i(x), \\ & s_j \in \mathrm{SOS}_{2k - \deg(g_j)} \quad \forall\, j = 0, \ldots, n-1, \\ & \lambda \in \mathbb{R}, \end{aligned} \tag{35}$$

where $\deg(g_0) = 0$. This gives a sequence of SDP relaxations for Eq. (34). Moreover, the SDPs in Eq. (35) are precisely the dual SDPs of the moment matrix relaxations of Eq. (30) (Pironio, Navascués, and Acín, 2010).

By solving these SDPs, it is possible to extract an SOS decomposition of $\lambda - f(x)$, which gives a *certificate* that $f(x) \leq \lambda$ whenever $g_i(x) \geq 0 \ \forall\, i$. For instance, solving the level-1 relaxation of our previous example given in Eq. (31), we find that for $\lambda = 1/8$ we can write $1/8 - x_2^2 + x_1 x_2 + x_2$ as

$$\tfrac{1}{2}\left(\tfrac{1}{2} - x_1 - x_2\right)^2 + \tfrac{1}{2}\left(x_1 - x_1^2\right) + \tfrac{3}{2}\left(x_2 - x_2^2\right). \tag{36}$$

Whenever the constraints $x_1 \geq x_1^2$ and $x_2 \geq x_2^2$ are satisfied, Eq. (36) is non-negative and hence, as it is equal to $1/8 - x_2^2 + x_1 x_2 + x_2$, it must be that $x_2^2 - x_1 x_2 - x_2 \leq 1/8$. This is an analytical proof of the upper bound that can be extracted from the numerics.

### B. Noncommutative polynomial optimization

The polynomial optimization problems of Sec. III.A can also be extended to the setting wherein the variables do not commute. Historically this was discovered through the study of quantum nonlocality: based on the work of Tsirelson (1980), Wehner showed that the correlations of two-outcome Bell inequalities without marginals can be characterized via SDP (Wehner, 2006). The general case, which requires an SDP hierarchy, was discovered soon afterward by Navascués, Pironio, and Acín (2007). Only later were the connection to the commutative case and the extension to arbitrary polynomials realized (Doherty *et al.*, 2008; Navascués, Pironio, and Acín, 2008; Pironio, Navascués, and Acín, 2010).

Given some Hilbert space $\mathcal{H}$, we can now consider polynomials of bounded operators $X_1, \ldots, X_n$ on $\mathcal{H}$. In particular, consider the following optimization problem

$$\begin{aligned} \max \quad & \mathrm{tr}[\rho f(X_1, \ldots, X_n)] \\ \text{such that} \quad & \mathrm{tr}[\rho h_i(X_1, \ldots, X_n)] \geq 0 \quad \forall\, i, \\ & g_j(X_1, \ldots, X_n) \succeq 0 \quad \forall\, j, \\ & \mathrm{tr}(\rho) = 1, \\ & \rho \succeq 0, \end{aligned} \tag{37}$$

where the optimization is over all Hilbert spaces $\mathcal{H}$, all states $\rho$ on $\mathcal{H}$, and all bounded operators $X_1, \ldots, X_n$ on $\mathcal{H}$ and the polynomials $f$, $h_i$, and $g_j$ are all Hermitian[14] (although the variables $X_1, \ldots X_n$ need not necessarily be Hermitian). This noncommutative generalization of Eq. (26) naturally captures many problems in quantum theory and forms the basis for characterizing nonlocal correlations (see Sec. V), communication correlations (see Secs. VI.B and VI.C.1), computing key rates in cryptography (see Sec. VII), and characterizing network correlations (see Sec. VIII).

As in the commutative case, this problem is in general difficult to solve. Indeed, the noncommutative setting is a generalization of the former and hence inherits its complexity. Nevertheless, Pironio, Navascués, and Acín (2010) showed that relatively natural extensions of the moment and sum-of-squares hierarchies can be derived that lead to a hierarchy of SDPs that (under mild conditions[15]) will converge to the optimal value of Eq. (37).

#### 1. Moment matrix approach

Following the previous section closely, a *monomial* is any product of the operators $X_1, \ldots, X_n$, and its length is the number of elements in the product. We define the length of the identity operator to be 0. For $k \in \mathbb{N}$ let $\mathcal{S}_k$ denote the set of monomials with a length no larger than $k$, noting that if a variable $X_i$ is not Hermitian, then we also include its adjoint $X_i^\dagger$ in the set of variables generating the monomials in $\mathcal{S}_k$.

For any feasible point $(\mathcal{H}, \rho, X_1, \ldots, X_n)$ of the problem, it is possible to define a moment matrix $\Gamma^k$ of level $k$ that is a matrix indexed by elements of $\mathcal{S}_k$ and whose $(M, N)$ entry for $M, N \in \mathcal{S}_k$ is given by

$$\Gamma^k(M, N) = \mathrm{tr}(\rho M^\dagger N). \tag{38}$$

[14] A polynomial $f(X_1, \ldots, X_n)$ is called Hermitian if $f = f^\dagger$.

[15] A sufficient condition for convergence is that the constraints of the problem imply a bound on the operator norm of feasible points $(X_1, \ldots, X_n)$. Following the formulation given by Pironio, Navascués, and Acín (2010), one should be able to determine some constant $C$ such that $C^2 - \sum_{i=1}^n X_i^\dagger X_i \succeq 0$ for all feasible points $(X_1, \ldots, X_n)$. For example, if $X_i$ are all projectors, then we can take $C = \sqrt{n}$.

As in the commutative case, this moment matrix is necessarily PSD since for any vector $|w\rangle$ we have

$$\langle w|\Gamma^k|w\rangle = \mathrm{tr}(\rho R^\dagger R) \geq 0, \tag{39}$$

where $R = \sum_{N\in\mathcal{S}_k}\langle N|w\rangle N$. Note that, for any polynomial $p(X)$ of degree no larger than $2k$ in the variables $X_1,\ldots,X_n$, we find that $\mathrm{tr}[\rho p(X)]$ is a linear combination of the elements of $\Gamma^k$. For each polynomial $g_i$ appearing in the constraints of Eq. (37), we also introduce a localizing moment matrix of level $k_i$ denoted $\Gamma^{k_i}_{g_i}$ whose $(M,N)$ entry is

$$\Gamma^{k_i}_{g_i}(M,N) = \mathrm{tr}[\rho M^\dagger g_i(X) N]. \tag{40}$$

As in the commutative case, a natural choice of $k_i$ is $\lfloor k - \deg(g_i)/2\rfloor$ to ensure that all elements of $\Gamma^{k_i}_{g_i}$ can be expressed as linear combinations of elements of $\Gamma^k$. Note that if $g_i(X)$ is PSD, then its corresponding moment matrix is also PSD.

As in the case of the Lasserre hierarchy, it is possible to relax Eq. (37) to a hierarchy of SDPs by optimizing over semidefinite matrices that resemble moment matrices and localizing moment matrices of level $k$. In particular, if $\deg(f)$, $\deg(h_i) \leq 2k$, we can write $f(X) = \sum_{M,N\in\mathcal{S}_k} f_{MN} M^\dagger N$ and $h_i(X) = \sum_{M,N\in\mathcal{S}_k} h^i_{MN} M^\dagger N$, where $f_{MN}, h^i_{MN} \in \mathbb{C}$. Thus, for $k\in\mathbb{N}$ such that $\deg(f), \deg(h_i) \leq 2k$, we define the level-$k$ relaxation of Eq. (37) as the SDP

$$\begin{aligned} \max \quad & \sum_{M,N\in\mathcal{S}_k} f_{MN}\Gamma^k(M,N) & \\ \text{such that} \quad & \sum_{M,N} h^i_{MN}\Gamma^k(M,N) \geq 0 & \forall\, i, \\ & \Gamma^{k_j}_{g_j} \succeq 0 & \forall\, j, \\ & \Gamma^k \succeq 0. & \end{aligned} \tag{41}$$

As in the case of the Lasserre hierarchy, there are many implicit equality constraints in Eq. (37), for example, $\Gamma^k(A,BC) = \Gamma(B^\dagger A, C)$ and the normalization condition $\Gamma^k(\mathbb{1},\mathbb{1}) = 1$. Moreover, if $f_{MN}$ and $h^i_{MN}$ are all real, we can without loss of generality restrict $\Gamma^k$ to be real valued, as explained in Sec. IX.F.

We now take a look at a noncommutative extension of the example introduced in Sec. III.A.1; see Eq. (31). Suppose that $X_1$ and $X_2$ are now Hermitian operators and that we are interested in solving the following problem:

$$\begin{aligned} \max \quad & \mathrm{tr}[\rho(X_2^2 - \tfrac{1}{2}X_1X_2 - \tfrac{1}{2}X_2X_1 - X_2)] \\ \text{such that} \quad & X_1 - X_1^2 \succeq 0, \\ & X_2 - X_2^2 \succeq 0, \\ & \mathrm{tr}(\rho) = 1, \\ & \rho \succeq 0. \end{aligned} \tag{42}$$

The main difference between Eqs. (31) and (42) is that the monomial $x_1x_2$ is replaced by a noncommutative generalization $(X_1X_2 + X_2X_1)/2$. Note that if we were to add the condition $[X_1,X_2]=0$, then the optimal value of the problem would coincide with that of Eq. (31). When we consider the indexing set $\{\mathbb{1}, X_1, X_2\}$, the level-1 relaxation of Eq. (42) corresponds to the SDP

$$\begin{aligned} \max \quad & y_{22} - \tfrac{1}{2}y_{12} - \tfrac{1}{2}y_{21} - y_{02} \\ \text{such that} \quad & \begin{pmatrix} 1 & y_{01} & y_{02} \\ & y_{11} & y_{12} \\ & & y_{22} \end{pmatrix} \succeq 0, \\ & y_{01} - y_{11} \geq 0, \\ & y_{02} - y_{22} \geq 0. \end{aligned} \tag{43}$$

As the moment matrix is Hermitian and can be taken to be real (and thus $y_{12} = y_{21}$), we see that the SDP in Eq. (43) is equivalent to the level-1 relaxation for the corresponding commutative problem; see Eq. (32). Thus, as in the commutative setting, we find a value of $1/8$ at level 1. However, we see a difference between the commutative and noncommutative problems emerge at level 2. The level-2 relaxation is based on the indexing set $\{\mathbb{1}, X_1, X_2, X_1^2, X_1X_2, X_2X_1, X_2^2\}$, which is larger than the corresponding commutative indexing set and results in the SDP relaxation

$$\begin{aligned} \max \quad & y_{06} - \tfrac{1}{2}y_{04} - \tfrac{1}{2}y_{05} - y_{02} \\ \text{such that} \quad & \begin{pmatrix} 1 & y_{01} & y_{02} & y_{03} & y_{04} & y_{05} & y_{06} \\ & y_{03} & y_{04} & y_{13} & y_{14} & y_{15} & y_{16} \\ & & y_{06} & y_{14} & y_{24} & y_{16} & y_{26} \\ & & & y_{33} & y_{34} & y_{35} & y_{36} \\ & & & & y_{44} & y_{45} & y_{46} \\ & & & & & y_{55} & y_{56} \\ & & & & & & y_{66} \end{pmatrix} \succeq 0, \\ & \begin{pmatrix} y_{01} - y_{03} & y_{03} - y_{13} & y_{04} - y_{14} \\ & y_{13} - y_{33} & y_{14} - y_{34} \\ & & y_{24} - y_{44} \end{pmatrix} \succeq 0, \\ & \begin{pmatrix} y_{02} - y_{06} & y_{05} - y_{16} & y_{06} - y_{26} \\ & y_{15} - y_{55} & y_{16} - y_{56} \\ & & y_{26} - y_{66} \end{pmatrix} \succeq 0, \end{aligned} \tag{44}$$

where by taking the moment matrices to be real we find that $y_{04} = y_{05}$. Running Eq. (44), we again find that the optimal value is $1/8$, and it is possible to show that the hierarchy had already converged at level 1. This value is achieved by the qubit state $\rho = |0\rangle\langle 0|$ together with the projectors

$$X_1 = \frac{1}{4}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & 3 \end{pmatrix}, \qquad X_2 = \frac{1}{4}\begin{pmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & 3 \end{pmatrix}. \tag{45}$$

This implies that the optimal value of $1/8$ for the noncommutative problem (42) is different from the optimal value of the commutative problem (31), which was 0.

### 2. Sum-of-squares approach

In the same spirit as Sec. III.A, the dual problem to the moment matrix approach can be seen as an optimization over SOS polynomials, in this case with noncommuting variables. Given a polynomial of operators $p(X_1,\ldots,X_n)$, we say that $p$ is a sum of squares if it can be written in the form

$$p(X_1,\ldots,X_n)=\sum_i r_i^\dagger(X_1,\ldots,X_n)r_i(X_1,\ldots,X_n) \tag{46}$$

for some polynomials $r_i$. It is evident that SOS polynomials are necessarily PSD. It is thus possible to find an upper bound on the problem Eq. (37) by instead solving the problem

$$\begin{aligned}
\min\quad & \lambda \\
\text{such that}\quad & \lambda - f(X) = s_0(X) + \sum_i \nu_i h_i(X) \\
& \qquad\qquad + \sum_{i,j} r_{ij}^\dagger(X) g_j(X) r_{ij}(X), \\
& \nu_i \geq 0 \quad \forall\, i, \\
& s_0 \in \mathrm{SOS}, \\
& \lambda \in \mathbb{R},
\end{aligned} \tag{47}$$

where the optimization is over $\lambda$, the non-negative real numbers $\nu_i$, the sum-of-squares polynomial $s_0$, and arbitrary polynomials $r_{ij}(X)$. Given a feasible point of Eq. (47) and any quantum state $\rho$, it is clear that if $g_j(X)\succeq 0$ and $\mathrm{tr}[\rho h_i(X)]\geq 0$, then we must have $\lambda \geq \mathrm{tr}[\rho f(X)]$. Therefore, any feasible point of Eq. (47) provides an upper bound on the optimal value of Eq. (37).

This SOS optimization can furthermore be relaxed to a hierarchy of SDPs. To see this first note that a polynomial $p(X)$ is a sum of squares if and only if there exists a PSD matrix $M$ such that $p(X)=w^\dagger M w$, where $w$ is a vector of monomials. Thus, by considering vectors $w$ whose entries are monomials up to degree $k$ (i.e., elements of $\mathcal{S}_k$), one optimizes over SOS polynomials up to degree $2k$ and the constraint $s_0\in\mathrm{SOS}$ is relaxed to the SDP constraint $s_0\in\mathrm{SOS}_{2k}$. The real variables $\lambda$ and $\nu_i$ all appear linearly in the problem and are therefore valid variables for an SDP problem. Finally, we have terms of the form

$$\sum_i r_i^\dagger(X) g(X) r_i(X). \tag{48}$$

Equation (48) is similar to an SOS polynomial $\sum_i r_i^\dagger(X) r_i(X)$, except that it is centered around a polynomial $g(X)$. As in the case of an SOS polynomial, for a bounded degree of $r_i$, this quantity can be rewritten as a PSD matrix $M$ with its entries multiplied by $g(X)$, thereby creating a new matrix $M_g$ that satisfies $w^\dagger M_g w=\sum_i r_i^\dagger(X)g(X)r_i(X)$. Thus, this term can be reinterpreted as a PSD condition. Following the notation for SOS polynomials, we denote the set of $g$-centered SOS polynomials of degree up to $d$ by $\mathrm{SOS}_d^g$.

For each large enough $k\in\mathbb{N}$, one arrives at the following hierarchy of semidefinite programming relaxations for Eq. (47):

$$\begin{aligned}
\min\quad & \lambda \\
\text{such that}\quad & \lambda - f(X) = s_0(X) + \sum_i \nu_i h_i(X) + \sum_j s_j(X) \\
& \nu_i \geq 0 \qquad\qquad \forall\, i, \\
& s_0 \in \mathrm{SOS}_{2k}, \\
& s_j \in \mathrm{SOS}^{g_j}_{2k-\deg(g_j)} \quad \forall\, j, \\
& \lambda \in \mathbb{R}.
\end{aligned} \tag{49}$$

By relaxing the noncommutative problem (42) to level 1 of the SOS hierarchy, we find that the polynomial $1/8 - X_2^2 + (1/2)(X_1X_2 + X_2X_1) + X_2^2$ can be written as

$$\tfrac{1}{2}(\tfrac{1}{2} - X_1 - X_2)^\dagger(\tfrac{1}{2} - X_1 - X_2) + \tfrac{1}{2}(X_1 - X_1^2) + \tfrac{3}{2}(X_2 - X_2^2), \tag{50}$$

which provides an analytical proof that, for any Hermitian operators $(X_1, X_2)$ that satisfy $X_1 - X_1^2 \succeq 0$ and $X_2 - X_2^2 \succeq 0$, we must have $\mathrm{tr}\{\rho[X_2^2 - (1/2)(X_1X_2 + X_2X_1) - X_2]\} \leq 1/8$.

*Remark*. Throughout this section we have repeatedly used a monomial indexing that was chosen up to some degree $k$. In both the moment and SOS approaches, this $k$ defines the index of the SDP hierarchy. Note, however, that it is not necessary to construct a hierarchy with these sets, and in general indexing by any set of monomials $\mathcal{S}$ will lead to a valid semidefinite relaxation of the problem. Such constructions can lead to more accurate bounds with fewer computational resources or to interesting physical constraints (Moroder *et al.*, 2013). Note that this also applies to the indexing sets of the localizing moment matrices.

## IV. ENTANGLEMENT

Entangled states are fundamental in quantum information science. In this section we discuss the use of SDP relaxation methods for detecting and quantifying entanglement.

### A. Doherty-Parrilo-Spedalieri hierarchy

Recall that a bipartite state is separable when it can be written in the form given by Eq. (4). Otherwise, it is said to be entangled. This leads to an elementary question: Is a given bipartite density matrix separable or entangled? While a general solution is challenging (Gurvits, 2003; Gharibian, 2010), the problem can be solved through a converging hierarchy of semidefinite relaxations of the set of separable states known as the Doherty-Parrilo-Spedalieri (DPS) hierarchy (Doherty, Parrilo, and Spedalieri, 2002, 2004). This hierarchy can also be adapted to entangled states of many parties; see Sec. IV.C.1.

Consider a quantum state $\rho_{AB}\in\mathcal{H}_A\otimes\mathcal{H}_B$. If the state is separable, then for any positive integer $n$ we can construct a *symmetric extension* of this quantum state, that is, a quantum state $\rho_n\in\mathcal{H}_A\otimes\mathcal{H}_B^{\otimes n}$ that is invariant under permutation of the subsystems in $\mathcal{H}_B^{\otimes n}$, and such that taking the partial trace over the additional subsystems recovers $\rho_{AB}$. For a separable state written as in Eq. (4), such an extension is given by

$$\rho_n^{\mathrm{sep}}=\sum_\lambda p(\lambda)\phi_\lambda\otimes\varphi_\lambda^{\otimes n}. \tag{51}$$

The main idea behind the DPS hierarchy is that this does not hold for entangled states: for any fixed entangled $\rho_{AB}$ there is a threshold $n_0$ such that symmetric extensions with $n>n_0$ do not exist.

Testing whether such a symmetric extension exists can be cast as an SDP; therefore, this gives a complete SDP hierarchy for testing entanglement. However, this test can quickly

become computationally demanding. Two more ideas can be used to make it more tractable. The first idea is to combine the test for symmetric extensions with the PPT criterion, which was described in Sec. II.B.1: we add the requirement that the extension $\rho_n$ must have positive partial transposition across all possible bipartitions.[16] This is satisfied by $\rho_n^{\mathrm{sep}}$. The second idea is to make use of the symmetry of $\rho_n^{\mathrm{sep}}$ in order to reduce the size of the problem.[17] The key observation is that $\rho_n^{\mathrm{sep}}$ not only is invariant under the permutation of $\mathcal{H}_B^{\otimes n}$ but also satisfies a stronger condition[18] known as Bose symmetry, that is,

$$\rho_n^{\mathrm{sep}} = (\mathbb{1}_A \otimes P_B)\rho_n^{\mathrm{sep}} = \rho_n^{\mathrm{sep}}(\mathbb{1}_A \otimes P_B) \tag{52}$$

for any permutation $P$. This implies that we can additionally require that $\rho_n^{\mathrm{sep}}$ belongs to the symmetric subspace over the copies of $B$ (Doherty, Parrilo, and Spedalieri, 2004), which has dimension $s_n = \binom{d_B+n-1}{n}$, as opposed to $d_B^n$, the dimension of the entire space. Let then $V_B$ be an isometry from $\mathbb{C}^{s_n}$ to the symmetric subspace of $\mathcal{H}_B^{\otimes n}$. With all the pieces in place, we can state the DPS SDP,

$$\begin{aligned} \max_{\sigma,t} \quad & t \\ \text{such that} \quad & \mathrm{tr}(\sigma) = 1, \\ & \sigma \succeq t\mathbb{1}, \\ & \rho_n = (\mathbb{1}_A \otimes V_B)\sigma(\mathbb{1}_A \otimes V_B^\dagger), \\ & \rho_{AB} = \mathrm{tr}_{B_2,\ldots,B_n}(\rho_n), \\ & \rho_n^{T_{B_1},\ldots,T_{B_k}} \succeq t\mathbb{1} \quad \forall\, k, \end{aligned} \tag{53}$$

where $\sigma$ is an auxiliary operator used to characterize the symmetric subspace.

The variable $t$ has been introduced to make the problem strictly feasible as in Sec. I. The dimension of $\sigma$ is $d_A s_n$, which for fixed $d_B$ increases exponentially fast with $n$, reflecting the fact that determining separability is an NP-hard problem. It is possible to compute convergence bounds on the DPS hierarchy; i.e., until which $n$ does one need to go in order to test whether a given quantum state is $\epsilon$-close to the set of separable states (Navascués, Owari, and Plenio, 2009b)?

From the dual of the DPS hierarchy, one can in principle obtain an entanglement witness for any entangled state. Moreover, the dual of the DPS hierarchy can also be interpreted as a commutative sum-of-squares hierarchy (Fang and Fawzi, 2021b).

The hierarchy collapses at the first level if $d_A d_B \leq 6$ since in this case the PPT criterion is necessary and sufficient for determining whether a state is entangled (Horodecki, Horodecki, and Horodecki, 1996). A natural question is then whether it also collapses at a finite level for larger dimensions. Surprisingly the answer is negative, and moreover one can show that no single SDP can characterize separability in these dimensions (Fawzi, 2021). It is possible, however, to solve a weaker problem with a single, albeit large, SDP: optimizing linear functionals over the set of separable states (Harrow, Natarajan, and Wu, 2017).

While the DPS hierarchy gives converging outer SDP relaxations of the separable set, it is also possible to construct converging inner relaxations of the same set (Navascués, Owari, and Plenio, 2009a). These relaxations closely follow the ideas of the DPS relaxations and are based on the observation that small linear perturbations can destroy the entanglement of states with $n$-fold Bose symmetric extension. However, they differ in the fact that the resulting set of SDPs is not a hierarchy, as the next criterion is not always strictly stronger than the previous.

### B. Bipartite entanglement

In this section we review the application of SDP methods to the simplest entanglement scenario, namely, that of entanglement between two systems.

#### 1. Quantifying entanglement

Once a quantum state is known to be entangled, a natural question is to quantify its entanglement; see the review by Plenio and Virmani (2007). In the standard paradigm, where the parties can perform local operations assisted by classical communication (LOCC) and have access to asymptotically many copies of the state, it is natural to consider conversion rates between a given state and the maximally entangled state as quantifiers of entanglement. Two important quantifiers are the distillable entanglement $E_D$ and the entanglement cost $E_C$.

The distillable entanglement $E_D$ addresses the largest rate $R$ at which one can convert, by means of LOCC, a given bipartite state $\rho_{AB}$ into a $d$-dimensional maximally entangled state $\phi_d^+$ (Bennett, Bernstein *et al.*, 1996). This is equivalent to asking how many copies of a maximally entangled qubit pair can be extracted asymptotically from $\rho_{AB}$. While this definition may appear to be somewhat arbitrary, in the asymptotic setting many alternative definitions turn out to be equivalent to it (Rains, 1999). Therefore,

$$\begin{aligned} E_D(\rho_{AB}) = \sup \quad & R \\ \text{such that} \quad & \lim_{n\to\infty} \inf_{\mathcal{L}} \|\mathcal{L}(\rho_{AB}^{\otimes n}) - \phi_{2^{\lfloor nR \rfloor}}^+\|_1 = 0, \end{aligned} \tag{54}$$

where $\|O\|_1 = \mathrm{tr}\sqrt{O^\dagger O}$ is the trace norm and $\mathcal{L}$ is the set of LOCC operations.

The entanglement cost is the smallest rate required to convert maximally entangled states into a given state by means of LOCC,

$$\begin{aligned} E_C(\rho_{AB}) = \inf \quad & R \\ \text{such that} \quad & \lim_{n\to\infty} \inf_{\mathcal{L}} \|\rho_{AB}^{\otimes n} - \mathcal{L}(\phi_{2^{\lfloor nR \rfloor}}^+)\|_1 = 0. \end{aligned} \tag{55}$$

Equation (55) remains unaltered by changing the distance measure (Hayden, Horodecki, and Terhal, 2001). In general

[16]Note that, because of the symmetry of $\rho_n$, only $n$ partial transpositions need to be considered, not the $2^n$ possible ones.

[17]Symmetrization techniques are useful for a wide class of SDPs and are further discussed in Sec. IX.F.

[18]To see that this is stronger, consider the state $|\psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$. It is not symmetric, as $\mathrm{SWAP}|\psi^-\rangle = -|\psi^-\rangle$, but it is permutation invariant, as $\mathrm{SWAP}|\psi^-\rangle\langle\psi^-|\mathrm{SWAP} = |\psi^-\rangle\langle\psi^-|$.

$E_D \leq E_C$, with equality holding for pure states (Vidal and Cirac, 2001; Horodecki, Sen(De), and Sen, 2003). In fact, a large class of entanglement measures can be shown to be bounded from above by $E_C$ and from below by $E_D$ (Horodecki, Horodecki, and Horodecki, 2000; Donald, Horodecki, and Rudolph, 2002). Thus, computing these quantities is of particular interest. However, owing to the difficulty of characterizing $\mathcal{L}$ (Chitambar *et al.*, 2014), such computations are difficult (Huang, 2014), but they can be efficiently bounded using SDP methods.

A frequently used entanglement measure is the logarithmic negativity of entanglement (Vidal and Werner, 2002). This is defined as $E_{\mathcal{N}} = \log \|\rho^{T_B}\|_1$, and it bounds the distillable entanglement as $E_D(\rho) \leq E_{\mathcal{N}}(\rho)$. It can be computed as the following SDP:

$$\begin{aligned} \|\rho^{T_B}\|_1 = \min_{\sigma_\pm} \quad & \mathrm{tr}(\sigma_+) + \mathrm{tr}(\sigma_-) \\ \text{such that} \quad & \rho^{T_B} = \sigma_+ - \sigma_-, \\ & \sigma_\pm \succeq 0. \end{aligned} \tag{56}$$

To see the connection between the trace norm and SDP, note that every Hermitian operator $O$ can be written as $O = \sigma_+ - \sigma_-$ for some PSD operators $\sigma_\pm$. A related SDP-computable quantity is the tempered negativity, which is defined for a given $\rho$ as $\sup\{\mathrm{tr}(\rho X) \colon \|X^{T_A}\|_\infty \leq 1, \|X\|_\infty = \mathrm{tr}(\rho X)\}$. This is a lower bound on both the negativity and the entanglement cost $E_C$. It was introduced to show the irreversibility of entanglement theory when the free operations are not restricted to LOCC but instead can be arbitrary nonentangling operations (Lami and Regula, 2023).

Consider that we are given one copy of a nonmaximally entangled state and we want to distill a state with as large a fidelity with the maximally entangled state as possible. By relaxing the LOCC paradigm to the technically more convenient superset of global operations that preserve PPT, one can bound the fidelity by an SDP (Rains, 2001). However, this bound is not additive (Wang and Duan, 2017b). Therefore, once we move into the many-copy regime, the size of the SDP grows with the number of copies $n$, making it unwieldy for the asymptotic limit $n \to \infty$. Notably, in this LOCC-to-PPT relaxed setting, the irreversibility of entanglement (i.e., $E_D \neq E_C$) still persists, as shown via SDP by Wang and Duan (2017a); see also Ishizaka and Plenio (2005). Wang and Wilde (2020) introduced an SDP-computable measure for quantifying non-PPT entanglement under global operations that are completely PPT preserving. This can be used to bound from above and below the one-shot exact entanglement cost under such free operations.[19]

An alternative upper bound on $E_D$, reported by Wang and Duan (2016a), is fully additive under tensor products, thus resolving the limit issue, and computable by SDP. It is given by $E_W = \log W(\rho_{AB})$, where

$$\begin{aligned} W(\rho_{AB}) = \min \quad & \|\sigma_{AB}^{T_B}\|_1 \\ \text{such that} \quad & \sigma_{AB} \succeq \rho_{AB}. \end{aligned} \tag{57}$$

Equation (57) is bounded from below by the bound given by Rains (2001) and from above by the logarithmic negativity.

While the asymptotic setting is conceptually interesting, a more applied approach often considers imperfect conversions between states using finitely many copies. In this so-called one-shot setting, SDP methods have been used for bounding the rate of entanglement distillation for a given degree of error (Fang *et al.*, 2019). This has been considered using many different relaxations of LOCC that admit either LP or SDP formulations (Regula *et al.*, 2019). Rozpędek *et al.* (2018) used SDPs for entanglement distillation under realistic limitations on the number of copies, errors, and exchanges of messages in LOCC, including the setting in which success is only probabilistic.

Another entanglement measure is the squashed entanglement (Christandl and Winter, 2004). It has several desirable properties: it is fully additive under tensor products, it obeys a simple entanglement monogamy relation (Koashi and Winter, 2004), and it is faithful; i.e., it is nonzero if and only if the state is entangled (Brandão, Christandl, and Yard, 2011). The definition draws inspiration from quantum key distribution by considering the smallest possible quantum mutual information between Alice and Bob upon conditioning on a third, "eavesdropper" system $E$ with which the state may be correlated. The squashed entanglement is defined as

$$\begin{aligned} E_{sq}(\rho_{AB}) = \min_{\rho_{ABE}} \quad & \tfrac{1}{2} I(A\colon B|E) \\ \text{such that} \quad & \rho_{AB} = \mathrm{tr}_E(\rho_{ABE}), \end{aligned} \tag{58}$$

where the quantum conditional mutual information can be given in terms of the conditional von Neumann entropy as $I(A\colon B|E) = H(A|E) - H(A|BE)$. While this is NP hard to compute (Huang, 2014), it can be bounded from below by means of a hierarchy of SDPs (Fawzi and Fawzi, 2022). By defining a new system $D$ such that $\rho_{ABED}$ is pure, it follows from entropic duality relations that $I(A\colon B|E) = H(A|E) + H(A|D)$. This transforms the objective function into a non-negative sum of von Neumann entropies that can then be lower bounded using techniques similar to those discussed in Sec. VII. It is unknown whether the hierarchy converges to $E_{sq}$, but nontrivial lower bounds can already be obtained at the first level for particular states.

A complementary class of entanglement measures are based on convex roof constructions. This means that one considers every possible decomposition of a mixed state $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ and evaluates the minimal entanglement as averaged over the entanglement of the pure states in the decomposition, i.e., $E_{\mathrm{roof}}(\rho) = \min \sum_i p_i E(|\psi_i\rangle)$, for some pure-state entanglement measure $E$. Examples of this are the entanglement of formation (Bennett, DiVincenzo *et al.*, 1996; Wootters, 1998) and geometric measures of entanglement (Wei and Goldbart, 2003). Tóth, Moroder, and Gühne (2015) showed that convex roofs of polynomial entanglement measures can be viewed as separability problems. An illustrative example is the linear entropy $E(|\psi_{AB}\rangle) = 1 - \mathrm{tr}(\rho_A^2)$.

[19]The exact entanglement cost is a more restrictive variation of Eq. (55) where $\rho_{AB}$ is generated exactly instead of with asymptotically vanishing error (Audenaert, Plenio, and Eisert, 2003).

By observing that $E(|\psi_{AB}\rangle) = \mathrm{tr}(\mathbb{P}^{\mathrm{asym}}_{AA'}|\psi\rangle\langle\psi|_{AB} \otimes |\psi\rangle\langle\psi|_{A'B'})$, where $\mathbb{P}^{\mathrm{asym}}$ is the projector onto the antisymmetric subspace, the convex roof of the linear entropy can be written as $E_{\mathrm{roof}}(\rho) = \mathrm{tr}(\mathbb{P}^{\mathrm{asym}}\sigma)$ where $\sigma = \sum_i p_i|\psi_i\rangle\langle\psi_i|_{AB} \otimes |\psi_i\rangle\langle\psi_i|_{A'B'}$. The state $\sigma$ is separable with respect to $AB|A'B'$ and symmetric when these systems are swapped, and its marginal is $\mathrm{tr}_{A'B'}(\sigma) = \rho$. Thus, by relaxing separability to PPT, one can bound $E_{\mathrm{roof}}$ through an SDP.

Finally, we mention that the SDP-based discussion of entanglement quantification and conversion can be extended to many other quantum resource theories, e.g., fidelity distillation of basis coherence (instead of entanglement as the resource) under incoherent operations (instead of LOCC as the free operation) (Lami, Regula, and Adesso, 2019). Similarly, conversion rates can be addressed by SDPs for resource theories of Gaussian states under Gaussian operations (Lami *et al.*, 2018), basis-coherent states (Napoli *et al.*, 2016; Bischof, Kampermann, and Bruß, 2019), entanglement in complex versus real Hilbert spaces (Kondra, Datta, and Streltsov, 2023), and asymmetry of states under group actions (Piani *et al.*, 2016).

### 2. Detecting the entanglement dimension

Suppose that a bipartite state with a local dimension $d$ is certified to be entangled. Does the preparation of the state truly require one to generate entanglement between $d$ degrees of freedom? For pure states this idea of an entanglement dimension is formalized in the Schmidt rank of a state $|\psi\rangle$. Every pure bipartite state, up to local unitaries, admits a Schmidt decomposition $|\psi\rangle = \sum_{i=1}^{s}\lambda_i|i,i\rangle$ for some real and normalized, non-negative coefficients $\{\lambda_i\}$. The Schmidt rank is the number of nonzero terms ($1 \leq s \leq d$) in the Schmidt decomposition. For mixed states this concept is extended to the Schmidt number. Let $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ be a decomposition. The Schmidt number is the largest Schmidt rank of the pure states $\{|\psi_i\rangle\}$ minimized over all possible decompositions of $\rho$ (Terhal and Horodecki, 2000).

One way to witness the Schmidt number is based on the range of $\rho$. If the range of $\rho$ is not spanned by pure states that have a Schmidt rank of at most $s$, then $\rho$ must have a Schmidt number of at least $s+1$. However, verifying that the range cannot be spanned by such states is generally not easy. Johnston, Lovitz, and Vijayaraghavan (2022) showed that the more general question of whether a given subspace of pure quantum states contains any product states (or states with a Schmidt rank of $s$) can be addressed by means of a hierarchy of LPs. This method exploits elementary properties of local antisymmetric projections applied to tensor products of the basis elements of the considered space. Every entangled subspace is detected at some finite level of this hierarchy and is more efficient to compute than with SDP-based approaches.

In analogy with entanglement witnesses, a relevant endeavor is to witness the Schmidt number from partial information about the state $\rho_{AB}$, i.e., to find an observable $O$ such that $\mathrm{tr}(O\rho) \leq \alpha$ holds for all states with a Schmidt number of at most $s$ but is violated for at least one state with a larger Schmidt number. Determining the value of $\alpha$ for any given $O$ can be related to a separability problem in a larger Hilbert space (Hulpke *et al.*, 2004). Specifically,

$$\alpha = \max_{\sigma} \quad s^2\mathrm{tr}(O_{AB} \otimes |\phi_s^+\rangle\langle\phi_s^+|_{A'B'}\sigma_{AA'BB'}), \tag{59}$$

where the four-partite state $\sigma$ is separable with respect to the bipartition $AA'|BB'$. This is a useful connection because, among other things, it allows us to use known SDP-compatible relaxations of separability to compute bounds on $\alpha$. However, its drawback is that the dimension of global Hilbert space scales as $(ds)^2$; thus, evaluating a bound for a larger Schmidt number becomes more demanding. This type of approach, which is based on auxiliary spaces $A'B'$, can also be used to address the Schmidt number of $\rho_{AB}$ directly, without a witness observable, via a hierarchy of SDPs that naturally generalizes the DPS construction (Weilenmann *et al.*, 2020; Gühne, Mao, and Yu, 2021). One treats the density matrix $\sigma_{AA'BB'}$ as a variable and imposes the conditions that $\rho_{AB} = s\Pi^{\dagger}_{A'B'}\sigma\Pi_{A'B'}$ and that $\sigma$ has a $k$-symmetric extension that is PPT in the sense of DPS. Notably, constructions of this sort, which connect Schmidt number witnessing to separability problems, can also be leveraged to certify higher-dimensional entanglement in the steering scenario (de Gois *et al.*, 2023). Furthermore, one can systematically search for adaptive Schmidt number witness protocols that use one-way LOCC from Alice to Bob. This has been proposed in a hypothesis testing framework that aims to minimise the total probability of false positives and false negatives for the Schmidt number detection scheme (Hu *et al.*, 2021). To achieve this, one can employ the SDP methods of Weilenmann, Aguilar, and Navascués (2021), and, in particular, the dual of the DPS-type approach to Schmidt numbers, to relax the set of possible witnesses.

An alternative approach to Schmidt number detection is to do away with the computational difficulty associated with the auxiliary spaces $A'B'$ by trading it for other relaxations. For example, a Schmidt number no larger than $s$ implies that $\langle\phi_d^+|\rho|\phi_d^+\rangle \leq s/d$ for every maximally entangled state $\phi_d^+$ (Terhal and Horodecki, 2000). Knowing that $\rho$ is close to a particular maximally entangled state thus yields a potentially useful semidefinite relaxation of states with a Schmidt number of $s$. Another option is to use the positive but not completely positive generalized reduction map $R(\sigma) = \mathrm{tr}(\sigma)\mathbb{1} - (1/s)\sigma$. Applied to one share of a state $\rho_{AB}$ with a Schmidt number of $s$, it still returns a valid quantum state (Tomiyama, 1985) that constitutes a semidefinite constraint on $\rho_{AB}$. Either of these conditions can be incorporated into an SDP, now with a size of only $d^2$, for computing an upper bound on an arbitrary linear witness. An iterative SDP-based algorithm that constructs Schmidt number witnesses by leveraging this type of ideas was discussed by Wyderka *et al.* (2023).

Further, we note that SDP relaxation methods are used in many other contexts of entanglement detection. This includes the construction of entanglement witnesses from random measurements in both discrete (Szangolies, Kampermann, and Bruß, 2015) and continuous variables (Mihaescu *et al.*, 2020), the evaluation of perturbations to known entanglement witnesses due to small systematic measurement errors (Morelli *et al.*, 2022), unification of semidefinite criteria for entanglement detection via covariance matrices (Gittsovich *et al.*, 2008), and the problem of determining

the smallest number of product states required to decompose a separable state (Gribling, Laurent, and Steenkamp, 2022).

### C. Multipartite entanglement

When considering states of more than two subsystems, one must deal both with an exponentially growing Hilbert space dimension and with an increasing number of qualitatively different entanglement configurations. SDP methods can be useful in both regards.

#### 1. Entanglement detection

Multipartite systems are said to be entangled if they are not fully separable, i.e., when they cannot be expressed as convex combinations of individual states held by each of the parties. Fully separable states of $N$ subsystems take the form

$$\rho = \sum_{\lambda} p(\lambda) \psi_{\lambda}^{(1)} \otimes \cdots \otimes \psi_{\lambda}^{(N)}. \tag{60}$$

It is possible to extend the original, bipartite DPS hierarchy discussed in Sec. IV.A to the multipartite case (Doherty, Parrilo, and Spedalieri, 2005), and thereby to decide the multipartite separability problem via SDP in the limit of large levels in the hierarchy. Essentially one considers symmetric extensions of the form of Eqs. (51) and (52) for all but one of the parties. Considering the dual problem as well leads to witnesses of multipartite entanglement (Brandão and Vianna, 2004a, 2004b). Owing to the aforementioned increase in computational cost, a naive use of this approach is limited in practice to the study of small multipartite systems, both in the number of constituents and in their dimension. A way to circumvent this problem is to limit the state space by considering representations of multipartite states in the form of tensor networks (Navascués, Singh, and Acín, 2020). This approach is used for detecting both entanglement and nonlocality in systems composed of hundreds of particles. Another approach is to use all of the symmetries that arise when considering the existence of symmetric extensions of the global state. Navascués, Baccari, and Acín (2021) found hierarchies that are efficient in time and space requirements, that allow entanglement from two-body marginals in systems of hundreds of particles to be detected, and that can be used even for infinite systems with appropriate symmetries. The approach followed by Navascués, Baccari, and Acín (2021), namely, formulating entanglement detection as asking whether given marginals are consistent with a joint separable state, is an instance of the *quantum marginal problem* that we review in Sec. IV.C.2.

It is also possible to construct SDP relaxations of the set of separable states from the interior. Ohst *et al.* (2024) developed a seesawlike method in which single-system state spaces are approximated with a polytope. By considering larger polytopes, one obtains better inner relaxations of separability at the price of computing more demanding SDPs. This was used to compute bounds on visibilities and robustness measures against full separability for systems up to five qubits or three qutrits.

SDP hierarchies have also been proposed for deciding the full separability of specific states. One example is multipartite Werner states. These states have the defining property that they are invariant under the action of any $n$-fold unitary $U^{\otimes n}$. For such states it is possible, using representation theory (Huber *et al.*, 2022), to provide a characterization that does not depend on the dimension and that can be tested via Lasserre's hierarchy or via SDP hierarchies for trace polynomials (Klep, Magron, and Volčič, 2022). These hierarchies, therefore, give entanglement witnesses that are valid independently of the local dimensions. Another class of examples is pure product states. These can be characterized in terms of suitable degree-3 polynomials in commuting variables (Eisert *et al.*, 2004). Thus, optimizations under the set of multipartite pure product states can be solved via the Lasserre SDP hierarchy. This approach has been followed for computing entanglement measures for three- and four-qubit states.

The multipartite separability problem has also been formulated as an instance of the *truncated moment* problem (Bohnet-Waldraff, Braun, and Giraud, 2017; Frérot, Baccari, and Acín, 2022); see also Milazzo, Braun, and Giraud (2020) for an application to the separability of quantum channels. This problem consists of obtaining a probability measure that reproduces some finite number of observed moments and can be solved via SDP (Laurent, 2009). In the context of entanglement, this translates into determining whether there is a separable quantum state that reproduces some observed expectation values. Frérot, Baccari, and Acín (2022), building on the results of Bohnet-Waldraff, Braun, and Giraud (2017), addressed this problem by developing a Navascués-Pironio-Acín (NPA)-like hierarchy of matrices that are all PSD if the observed expectation values can be reproduced by a separable state. This gives us a tool for detecting many-body entanglement that recovers the covariance matrix criterion of Gittsovich, Hyllus, and Gühne (2010) and the spin-squeezing inequalities of Tóth *et al.* (2009) at concrete finite levels of the hierarchy. However, this tool fails to address finer notions of entanglement (i.e., failure of $k$ separability for $k > 2$). Multipartite entanglement detection has also been formulated in terms of adaptive strategies (Weilenmann, Aguilar, and Navascués, 2021), which can be formulated in terms of Lasserre-like SDP hierarchies (Weilenmann, Budroni, and Navascués, 2024).

According to Eq. (60), a state is already entangled if two particles are entangled, even if the rest of the particles remain in a separable state. A stronger requirement is called genuine multipartite entanglement (GME). A state has GME if it cannot be generated by classically mixing quantum states that are separable with respect to some bipartition of the subsystems. We can let $\tau$ denote a bipartition of all the particle labels $\{1, \ldots, N\}$ and associate a state $\sigma_\tau$ that is biseparable across $\tau$. If no model of the form $\rho = \sum_\tau p(\tau)\sigma_\tau$ exists, where $\tau$ ranges over all the possible bipartitions, then $\rho$ has GME.

While some simple witnesses of GME can be systematically constructed without SDPs [see Bourennane *et al.* and (2004) and Zhang *et al.* (2024)], SDP methods offer an effective approach for reasonably small particle numbers. A sufficient condition for GME is obtained by replacing the separable states $\sigma_\tau$ with quantum states $\omega_\tau$ that are PPT with respect to the bipartition $\tau$. By defining the subnormalized operators $\tilde{\omega}_\tau = p(\tau)\omega_\tau$ and adding the normalization

condition $\sum_\tau \mathrm{tr}(\tilde{\omega}_\tau) = 1$, one obtains an SDP relaxation of GME (Jungnitsch, Moroder, and Gühne, 2011a). If no such decomposition of $\rho$ is found, SDP duality allows for the construction of an inequality that witnesses GME. This method has been found to be practical for detecting GME in systems up to around seven qubits. Sometimes this SDP can even be reduced to an LP, thereby enabling easier computations (Jungnitsch, Moroder, and Gühne, 2011b).

The aforementioned procedure can be generalized to any positive map that acts on only one element of a bipartition (Lancien *et al.*, 2015); namely, one relaxes each state $\sigma_\tau = \sum_i p_i \sigma_{\tau_1}^{(i)} \otimes \sigma_{\tau_2}^{(i)}$ via another state $\sigma_{\Lambda_\tau}$ that satisfies $\Lambda_{\tau_1} \otimes \mathbb{1}_{\tau_2}[\sigma_{\Lambda_\tau}] \succeq 0$ for a given positive map $\Lambda_\tau$. This has the apparent disadvantage that one would potentially need to run over all possible $\Lambda_\tau$ in order to prove that a state admits such a decomposition, but in practice it turns out that simple maps such as the aforementioned transposition map, the Choi map, and the Hall-Breuer map (Clivaz *et al.*, 2017) allow large families of GME states to be identified. This connection between separable states and positive maps is also exploited in order to build witnesses of GME from witnesses of bipartite entanglement (Huber and Sengupta, 2014). Moreover, this connection has also been used in linear algebra, where the Lasserre hierarchy is used for determining whether linear maps and matrices are positive and separable, respectively (Nie and Zhang, 2016).

### 2. Quantum marginal problems

The quantum marginal problem (QMP) asks whether there is a global entangled state that is compatible with a given collection of few-body states. That is, given a collection of quantum states $\{\rho_i\}_{i=1}^I$, each supported in a set of quantum systems $K_i \subset [1, \ldots, N]$ (generally with $K_i \cap K_j \neq \varnothing$), the QMP asks whether a joint state $\rho \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ exists that satisfies $\rho_i = \mathrm{tr}_{\setminus K_i}(\rho)$ for all $i$, where $\mathrm{tr}_{\setminus K_i}$ denotes the partial trace over all systems except $K_i$. The QMP is naturally cast as an SDP (Hall, 2007) since it involves only positive operators (the marginal quantum states) and linear constraints between them. However, solving these SDPs is generally expensive due to the exponential growth of its size with $N$ and the dimension of the subsystems. In fact, in terms of computational complexity, the QMP is a Quantum Merlin Arthur (QMA)-complete problem (Liu, Christandl, and Verstraete, 2007). Roughly speaking, QMA is one proposed quantum computing counterpart of the complexity class NP; see Kitaev, Shen, and Vyalyi (2002) and Gharibian (2024). Nevertheless, particular cases are tractable or admit tractable relaxations.

One such particular case is that in which the global state is pure, i.e., $\rho = |\psi\rangle\langle\psi|$. In this case, the QMP can be connected to a separability problem. This restriction makes the problem no longer an SDP, since the requirement of having a global pure state introduces a nonlinear constraint $\rho^2 = \rho$. Yu *et al.* (2021) overcame this issue by considering a symmetric extension of the complete global state, where pure states can be characterized by the restriction $\mathrm{Tr}(S_{AB}\rho \otimes \rho) = 1$, with the operator $S_{AB}$ denoting the swap operator $S_{AB} = \sum_{i,j} |ij\rangle\langle ji|$ [note that $\mathrm{Tr}(S_{AB}\rho \otimes \sigma) = \mathrm{Tr}(\rho\sigma)$]. The separability of $\rho \otimes \rho$ can then be relaxed via the DPS hierarchy to an SDP. This procedure was generalized by Huber and Wyderka (2022), who formulated the compatibility problem in terms of spectra. Namely, rather than asking for a joint state that reproduces some given reduced density matrices, Huber and Wyderka (2022) asked whether there is a joint state such that the spectra of marginals coincides with some given set. Working with spectra instead of density matrices allows one to exploit symmetries in order to reduce the computational load of the problem. This approach, moreover, produces witnesses of incompatibility for arbitrary local dimensions.

A case where the characterization can be done exactly in terms of an efficient SDP is that of states that are invariant under permutation of the parties (Aloy, Fadel, and Tura, 2021). In such a case the symmetries first greatly reduce the number of marginals; namely, there is only one possible marginal for each number of subsystems. Thus, it suffices to consider only the problem of compatibility with a single marginal. Moreover, the number of parameters required for the description of the joint state is also small. This allowed Aloy, Fadel, and Tura (2021) to give necessary and sufficient conditions for the QMP as a single, tractable SDP for systems composed of up to 128 particles.

The compatibility problem has also been formulated in terms of quantum channels. On the one hand, Haapasalo *et al.* (2021) considered the problem of whether a global broadcasting channel $\Phi_{A\to B_1,\ldots,B_N}$ exists that has a given set of channels $\Phi_{A\to B_i}$ as marginals. This problem can be connected to a state compatibility problem via the Choi-Jamiołkowski isomorphism (Jamiołkowski, 1972; Choi, 1975), which allows the previously outlined methods to be used. On the other hand, Hsieh, Lostaglio, and Acín (2022) considered the more general problem of whether a global evolution is compatible with a set of local dynamics, giving a measure of robustness that can be computed exactly via SDP.

A problem related to the QMP is determining, from a set of marginals of a joint state, properties of other marginals. For instance, one can ask, given some entangled states that are marginals of an unknown joint state, whether the remaining marginals must be entangled as well. This problem can be addressed via entanglement witnesses whose optimization can be cast as SDPs (Tabia *et al.*, 2022). The QMP has also been tackled via tools from the study of nonlocality (Bermejo Morán, Pozas-Kerstjens, and Huber, 2023) that are the subject of Sec. V.

## V. QUANTUM NONLOCALITY

In this section we discuss SDP relaxation methods for quantum nonlocality and their applications to quantum information.

### A. The Navascués-Pironio-Acín hierarchy

A fundamental question in Bell nonlocality is to characterize the set of distributions that are predicted by quantum theory in a Bell scenario (see Fig. 2) with a given number of inputs ($X$ and $Y$) and outputs ($N$ and $M$). This corresponds to deciding whether for any given distribution $p(a, b|x, y)$ there exists a bipartite quantum state of any dimension $|\psi\rangle$ and local measurements for Alice and Bob $\{A_{a|x}\}_{a,x}$ and $\{B_{b|y}\}_{b,y}$,

respectively, such that the distribution can be written in the form[20]

$$p(a,b|x,y) = \langle\psi|A_{a|x} \otimes B_{b|y}|\psi\rangle. \tag{61}$$

In contrast to the set of correlations associated with local models (see Sec. II.B.1), the set of quantum correlations for arbitrary input-output scenarios, denoted by $\mathcal{Q}$, admits in general no simple and useful characterizations: checking membership is known to be undecidable (Ji *et al.*, 2020). However, $\mathcal{Q}$ can be approximated by a sequence of supersets $\{\mathcal{Q}_k\}_{k=1}^{\infty}$ in such a way that

$$\mathcal{Q}_1 \supseteq \mathcal{Q}_2 \supseteq \cdots \supseteq \mathcal{Q}_\infty \supseteq \mathcal{Q}, \tag{62}$$

where the membership of $p$ in $\mathcal{Q}_k$ can be decided by an SDP. Thus, if there exists some $k$ for which a hypothesized distribution $p$ fails to be a member of $\mathcal{Q}_k$, it follows that no quantum model for $p$ exists. This hierarchy of outer SDP relaxations to the quantum set of Bell nonlocal correlations is known as the NPA hierarchy (Navascués, Pironio, and Acín, 2007). In the limit of the sequence $k \to \infty$, the NPA hierarchy converges to a set of distributions $\mathcal{Q}_\infty$. This set corresponds to quantum models in which the tensor product demarcating the separation of parties is relaxed to the commutation condition $[A_{a|x}, B_{b|y}] = 0$ (Doherty *et al.*, 2008; Navascués, Pironio, and Acín, 2008). This corresponds to changing Eq. (61) to

$$p(a,b|x,y) = \langle\psi|A_{a|x}B_{b|y}|\psi\rangle. \tag{63}$$

In finite dimensions, the commutation condition is equivalent to the tensor product, and thus $\mathcal{Q}_\infty = \mathcal{Q}$. In infinite dimensions the conditions are inequivalent (Scholz and Werner, 2008) and, moreover, a strict separation exists (Ji *et al.*, 2020). Therefore, the NPA hierarchy generally does not converge to $\mathcal{Q}$. However, for a specific distribution in a specific input-output scenario, it sometimes is the case that there exists some finite $k$ for which the membership of $p$ in $\mathcal{Q}_k$ is necessary and sufficient for a quantum model.

The NPA hierarchy is a noncommutative polynomial relaxation hierarchy of the type discussed in Sec. III.B. Define a list of all linearly independent measurement operators in the Bell scenario $L = \{\mathbb{1}, \mathbf{A}, \mathbf{B}\}$ where $\mathbf{A} = (A_{1|1}, \ldots, A_{N-1|X})$ and $\mathbf{B} = (B_{1|1}, \ldots, B_{M-1|Y})$. Then let $\mathcal{S}_k$ be the set of all products of length at most $k$ of the operators appearing in $L$. Note that one is free to also include some but not all products of a given length; in such cases one speaks of intermediate hierarchy levels, which are often useful in practice; see the remark in Sec. III.B.2. We associate with level $k$ an $|\mathcal{S}_k| \times |\mathcal{S}_k|$ moment matrix whose rows and columns are indexed by elements $u, v \in \mathcal{S}_k$,

$$\Gamma(u,v) = \langle\psi|u^\dagger v|\psi\rangle \tag{64}$$

for some unknown state $|\psi\rangle$. This moment matrix encodes constraints from quantum theory, namely, that $\Gamma(\mathbb{1},\mathbb{1}) = 1$, $\Gamma(u,v) = \Gamma(s,t)$ whenever $u^\dagger v = s^\dagger t$, and $\Gamma(u,v) = 0$ whenever $u^\dagger v = 0$. This implies, for example, that $\Gamma(B_{b|y}, B_{b'|y}A_{a|x}) = \delta_{b,b'}\Gamma(A_{a|x}, B_{b|y})$ since we are assuming without loss of generality that the measurements are projective. In addition, we want to constrain the moment matrix to reproduce the probability distribution in question, which requires $\Gamma(A_{a|x}, B_{b|y}) = p(a,b|x,y)$, $\Gamma(A_{a|x}, \mathbb{1}) = p_A(a|x)$, and $\Gamma(\mathbb{1}, B_{b|y}) = p_B(b|y)$. Following Sec. III the key observation is that a necessary condition for the existence of a quantum model for $p$ is that the remaining free variables composing the moment matrix, i.e., all variables not fixed by $p$ and the additional equality constraints, can be chosen such that $\Gamma \succeq 0$. Finally, since these constraints are all real, one can without loss of generality restrict $\Gamma$ to be real valued, as explained in Sec. IX.F.

For example, the first level of the hierarchy ($k = 1$) corresponds to the moment matrix[21]

$$\Gamma = \begin{array}{c} \\ \mathbb{1} \\ \mathbf{A}^\dagger \\ \mathbf{B}^\dagger \end{array} \begin{array}{c} \begin{array}{ccc} \mathbb{1} & \mathbf{A} & \mathbf{B} \end{array} \\ \begin{pmatrix} 1 & P_A & P_B \\ P_A^T & S_A & P_{AB} \\ P_B^T & P_{AB}^T & S_B \end{pmatrix} \end{array}. \tag{65}$$

The matrix in Eq. (65) has size $|\mathcal{S}_1| = 1 + (N-1)X + (M-1)Y$, where $P_A = [p_A(1|1), p_A(2|1), \ldots, p_A(N-1|X)]$ and $P_B = [p_B(1|1), p_B(2|1), \ldots, p_B(M-1|Y)]$ are Alice's and Bob's marginal probabilities, ${P_{AB}}^{(ax)(by)} = \langle\psi|A_{a|x}B_{b|y}|\psi\rangle = p(a,b|x,y)$ is the table of joint probabilities, and ${S_A}^{(ax)(a'x')} = \langle\psi|A_{a|x}A_{a'|x'}|\psi\rangle$ and ${S_B}^{(by)(b'y')} = \langle\psi|B_{b|y}B_{b'|y'}|\psi\rangle$ are the matrices of second moments of Alice and Bob. Thus, the submatrices $P_A$, $P_B$, and $P_{AB}$ are completely fixed by $p$, whereas the matrices $S_A$ and $S_B$ are entirely composed of unknown variables, except on their diagonals. If they can be completed such that $\Gamma \succeq 0$, then $p \in \mathcal{Q}_1$.

This SDP, however, is generally not strictly feasible, which sometimes causes numerical difficulties when one checks for membership in $\mathcal{Q}_k$ (Araújo, 2023). A straightforward variation is always strictly feasible (see Appendix B): instead of constraining $\Gamma$ to reproduce a particular probability distribution, one leaves those terms as free variables and optimizes a Bell functional over them. This allows one to compute bounds on the optimal quantum violation of a Bell inequality. The generic Bell functional in Eq. (14) can be expressed in terms of the moment matrix as $\sum_{a,b,x,y} c_{abxy}\Gamma(A_{a|x}, B_{b|y})$. In our example with $\mathcal{Q}_1$, this corresponds to $P_A, P_B$, and $P_{AB}$ not being fixed matrices but instead matrices composed of free variables, a linear combination of which is the objective function of the SDP.

[20]Note that, since there are no restrictions on the dimension, we can without loss of generality assume the quantum state to be pure and the measurements to be projective.

[21]The symbols outside the matrix in Eq. (65) and, equivalently, in Eq. (119) denote the element of $\mathcal{S}_k$ that indexes the corresponding row or column.

It is also interesting to consider the dual of this SDP. As the primal SDP can be considered a particular case of noncommutative polynomial optimization, the dual can be considered a particular case of optimization over SOS polynomials. Let $y$ be a vector of all the free variables in the moment matrix, and write $\Gamma = \Gamma_0 + \sum_i y_i \Gamma_i$. The primal SDP is thus given by

$$\begin{aligned} \max_{y} \quad & \langle b, y \rangle \\ \text{such that} \quad & \Gamma_0 + \sum_i y_i \Gamma_i \succeq 0, \end{aligned} \tag{66}$$

where $b$ encodes the Bell functional in question. The dual SDP is then given by

$$\begin{aligned} \min_{X} \quad & \langle \Gamma_0, X \rangle \\ \text{such that} \quad & \langle \Gamma_i, X \rangle = -b_i, \\ & X \succeq 0. \end{aligned} \tag{67}$$

Any feasible solution to the dual SDP then gives an SOS proof that the optimal quantum violation is bounded above by $\langle \Gamma_0, X \rangle$. To see this let $w$ be the vector of all monomials in $\mathcal{S}_k$ (ordered using the same ordering as the primal problem), then $S = w^\dagger X w = w^\dagger Q^\dagger Q w$ is an SOS polynomial where we have written $X = Q^\dagger Q$ since $X$ is PSD. In this notation $Qw$ is a vector of polynomials $P_i$ such that $S = \sum_i P_i^\dagger P_i$. Finally, if $\Gamma$ is the level $k$ moment matrix for any feasible quantum model, then we have

$$\langle \Gamma_0, X \rangle - \langle b, y \rangle = \langle \Gamma, X \rangle = \mathrm{tr}(\rho S) \geq 0. \tag{68}$$

Besides proving bounds on the optimal violation, this is also useful for self-testing; see Sec. V.B. Last, note that the NPA hierarchy applies equally well to scenarios that feature more than two parties.

### 1. Macroscopic Locality and almost-quantum correlations

There is a large body of research aiming to identify the physical principles that constrain quantum correlations. Some of these correspond to certain low levels of the NPA hierarchy. One such principle is Macroscopic Locality (Navascués and Wunderlich, 2010), which stipulates that classicality must reemerge in the macroscopic limit of a Bell experiment. Consider that the source in the Bell scenario does emits not one pair of particles but instead $N$ independent and identical pairs. When Alice and Bob perform their measurements, they will direct the incoming beam of particles onto their detectors, causing them all to fire, but with different detection rates. Assuming that intensity fluctuations in the beam can be detected to the order $\sqrt{N}$, one can define the intensity fluctuation around the mean as $I_u = (1/\sqrt{N}) \sum_{i=1}^{N} [d_i^u - p(u)]$, where $u$ indicates the input-output pair for either Alice or Bob and $d_i^u$ is the indicator function for whether particle number $i$ impinged on the corresponding detector. When $N \to \infty$, the central limit theorem implies that Alice and Bob will observe a Gaussian intensity fluctuation with vanishing mean and covariance matrix $\Gamma_{uv} = \langle I_u I_v \rangle = (1/N) \sum_{i,j=1}^{N} \langle d_i^u d_j^v \rangle$. Recalling that the particle pairs are identical and independent, one has $\Gamma_{uv} = \langle d_1^u d_1^v \rangle$. Using the facts that the mean and the covariance matrix completely characterize the Gaussian and that the latter is always PSD, one can show that Macroscopic Locality is characterized by $\mathcal{Q}_1$, i.e., the existence of a matrix of the form of Eq. (65) that is PSD (Navascués and Wunderlich, 2010). However, macroscopically local correlations are insufficiently restrictive to capture the limitations of quantum theory. From a physical point of view, this follows from the fact that such correlations violate (Cavalcanti, Salles, and Scarani, 2010) the principle of Information Causality, which quantum theory is known to obey (Pawłowski *et al.*, 2009). Alternatively, this same follows immediately from the fact that in general $\mathcal{Q}_1 \neq \mathcal{Q}$.

A more precise constraint on the quantum set is known as almost-quantum correlations (Navascués, Guryanova *et al.*, 2015). These correlations satisfy several established elementary principles[22] other than Macroscopic Locality, namely, no trivial communication complexity (van Dam, 1999; Brassard *et al.*, 2006), no advantage for nonlocal computation (Linden *et al.*, 2007), and Local Orthogonality (Fritz *et al.*, 2013). Almost-quantum correlations are those that can be written in the form $p(a, b|x, y) = \langle \psi | \tilde{A}_{a|x} \tilde{B}_{b|y} | \psi \rangle$, where $\sum_a \tilde{A}_{a|x} = \sum_b \tilde{B}_{b|y} = \mathbb{1}$ (normalization) and $A_{a|x} B_{b|y} |\psi\rangle = B_{b|y} A_{a|x} |\psi\rangle$ for all $a$, $x$, $b$, and $y$. This natural relaxation of quantum theory admits a simple SDP characterization that is equivalent to choosing a monomial indexing set $\mathcal{S}_{1+AB} = \{\mathbb{1}, \mathbf{A}, \mathbf{B}, \mathbf{A} \times \mathbf{B}\}$ in the NPA hierarchy (Navascués, Guryanova *et al.*, 2015). This level is intermediate between $k = 1$ and 2 and is often referred to as level "$1 + AB$"; see the remark in Sec. III.B.2.

For practical purposes, an important problem is the speed of convergence of the NPA hierarchy. In bipartite Bell scenarios with a small number of inputs and outputs, it was systematically investigated by empirical means by Lin, Vértesi, and Liang (2022). Typically almost-quantum correlations are significantly more constraining than macroscopically local correlations, and the relative difference often increases with the number of outputs.

### 2. Tsirelson bounds

A natural application of the NPA hierarchy is to compute bounds on the optimal quantum violation of Bell inequalities. This value is known as the Tsirelson bound, named after Boris Tsirelson's analytical derivation (Tsirelson, 1980, 1993) of the maximal quantum violation of the CHSH inequality (Clauser *et al.*, 1969). However, with the exception of particularly convenient families of Bell inequalities (some examples were given by Epping, Kampermann, and Bruß (2013), Salavrakos *et al.* (2017), Augusiak *et al.* (2019), and Tavakoli, Farkas *et al.* (2021), the Tsirelson bound is too difficult to determine analytically. Therefore, the NPA hierarchy provides a practically viable approach to bounding it. Many concrete instances of Bell inequalities have been analyzed by means of the NPA hierarchy, such as in the context of noise tolerance of nonlocality (Vértesi, 2008; Tavakoli and Gisin, 2020; Lin,

[22]However, almost-quantum correlations distinguish between measurements that are mathematically well defined and measurements that are physically allowed; i.e., they violate the so-called no-restriction hypothesis (Sainz *et al.*, 2018).

Vértesi, and Liang, 2022), many outcomes in Bell tests (Liang, Lim, and Deng, 2009; Tavakoli *et al.*, 2016, 2017), multipartite Bell tests (Vértesi and Pál, 2011; Grandjean *et al.*, 2012; López-Rosa, Xu, and Cabello, 2016; Vallins, Sainz, and Liang, 2017), Bell tests with additional constraints (Bernards and Gühne, 2020), nonlocal games with conflicting party interests (Pappa *et al.*, 2015), and the detection loophole of Bell experiments (Vértesi, Pironio, and Brunner, 2010; Branciard, 2011; Szangolies, Kampermann, and Bruß, 2017; Cope, 2021).

For a simple but large class of Bell inequalities, the Tsirelson bound is guaranteed (Navascués and Wunderlich, 2010) to coincide with the bound associated with the first level of the NPA hierarchy (i.e., Macroscopic Locality $\mathcal{Q}_1$). These Bell tests have binary outputs for Alice and Bob and correspond to Bell functionals of the form $\sum_{x,y} c_{xy}\langle A_x B_y\rangle$, where $c_{xy}$ are arbitrary real coefficients and $A_x \equiv A_{1|x} - A_{2|x}$ and $B_y \equiv B_{1|y} - B_{2|y}$ are observables for Alice and Bob. The quantum model corresponding to the value associated with $\mathcal{Q}_1$ is known as the Tsirelson construction. This construction stipulates that, for any set of dichotomic quantum observables, one can find unit vectors $\vec{u}_x, \vec{v}_y \in \mathbb{R}^{X+Y}$ such that $\langle A_x B_y\rangle = \vec{u}_x^T \vec{v}_y$, and, conversely, for any unit vectors $\vec{u}_x, \vec{v}_y \in \mathbb{R}^n$, one can find observables $A_x$ and $B_y$ such that $\langle A_x B_y\rangle_\psi = \vec{u}_x^T \vec{v}_y$, where $\psi$ is a maximally entangled state of dimension $2^{\lceil n/2\rceil}$ (Tsirelson, 1980; Tsirelson, 1987). This construction also provides a connection between Tsirelson bounds and the Grothendieck constant (Grothendieck, 1953).

The link between Tsirelson's construction and SDPs has been used to derive the Tsirelson bound for the Braunstein-Caves Bell inequalities (Wehner, 2006), and analyses based on $\mathcal{Q}_1$ have yielded quantum Bell inequalities (i.e., inequalities satisfied by all quantum nonlocal correlations) for dichotomic observables (Yang *et al.*, 2011; Ishizaka, 2020; Mikos-Nuszkiewicz and Kaniewski, 2023). Notably, for the simplest scenario with binary inputs and outputs, a quantum Bell inequality in the spirit of CHSH that gives a complete characterization of the two-point correlators was known well before the advent of SDP relaxation methods (Tsirelson, 1987; Landau, 1988; Masanes, 2003). However, an approach based on $\mathcal{Q}_1$ leads to more accurate characterizations that now also take the marginal probabilities into account. An example of such a $\mathcal{Q}_1$-based quantum Bell inequality in the spirit of CHSH is

$$\arcsin D_{11} + \arcsin D_{12} + \arcsin D_{21} - \arcsin D_{22} \leq \pi, \quad (69)$$

where $D_{xy} = (\langle A_x B_y\rangle - \langle A_x\rangle\langle B_y\rangle)/\sqrt{(1-\langle A_x\rangle^2(1-\langle B_y\rangle^2)}$. However, these inequalities are still not tight, as there are quantum correlations in the binary input-output scenario that satisfy Eq. (69) but are not members of $\mathcal{Q}_2$ (Navascués, Pironio, and Acín, 2007). Moreover, some more general classes of Bell inequalities, including some with many outputs, can be efficiently approximated using SDP methods without the need for hierarchies (Masanes, 2005; Kempe, Regev, and Toner, 2010).

An illuminating application of the NPA hierarchy is to the Bell inequality known as $I_{3322}$ (Froissart, 1981; Śliwa, 2003; Collins and Gisin, 2004). It pertains to the second simplest Bell scenario: it is the only nontrivial facet of the local polytope for the bipartite Bell scenario with three inputs and two outputs (other than a lifting[23] of CHSH). It can be written as

$$I_{3322} = -p_{11} - p_{22} - p_{12} - p_{21} - p_{13} - p_{31} + p_{23} + p_{32} + p_1^A + p_1^B \leq 1, \quad (70)$$

where we write $p_{xy} = p(1,1|x,y)$. While the Tsirelson bound of the simplest Bell inequality, namely, CHSH, is straightforward to obtain analytically, the opposite is the case for $I_{3322}$. If one restricts to qubit systems, the maximal violation is $I_{3322} = 5/4$, but the seesaw heuristic (discussed at the end of Sec. II.B.1) has revealed that larger violations are possible when higher-dimensional systems are employed. In fact, it is conjectured that the Tsirelson bound is saturated only by an infinite-dimensional quantum state (Pál and Vértesi, 2010). Upper bounds to the Tsirelson bound of $I_{3322}$ have been computed via the NPA hierarchy. These are illustrated in Table II. Relaxations up to $\mathcal{Q}_3$ were evaluated by Navascués, Pironio, and Acín (2008). Pál and Vértesi (2009, 2010) then computed $\mathcal{Q}_4$, and Rosset (2018) evaluated $\mathcal{Q}_5$. The computational requirements scale rapidly in the relaxation level, as is typically the case with SDP relaxation hierarchies, whereas the bounds rapidly converge. The results for $\mathcal{Q}_4$ and $\mathcal{Q}_5$ are identical up to at least 17 digits and match the best known quantum violation of $I_{3322}$ to within $10^{-16}$ (Pál and Vértesi, 2010).

TABLE II. Upper bounds on the Tsirelson bound of the $I_{3322}$ Bell inequality for different levels of the NPA hierarchy, along with the size of the corresponding SDP matrix.

| Relaxation level | Value of SDP | Size of SDP matrix |
|---|---|---|
| 1 | 1.375 000 00 | 7 |
| 1 + AB | 1.251 470 90 | 16 |
| 2 | 1.250 939 72 | 28 |
| 3 | 1.250 875 56 | 88 |
| 4 | 1.250 875 38 | 244 |
| 5 | 1.250 875 38 | 628 |

### B. Device-independent certification

Device-independent quantum information is the study of quantum information protocols executed under minimal assumptions (Pironio, Scarani, and Vidick, 2016). This typically amounts to assuming only the validity of quantum mechanics in otherwise uncharacterized experiments, or sometimes even just the no-signaling principle. Here we consider the former assumption and discuss how SDP relaxation methods for quantum nonlocality can be employed to device-independently certify properties of the underlying quantum systems.

[23]Every Bell inequality that is a facet for a given number of inputs and outputs can be lifted to a facet when the number of parties, inputs, or outputs is increased (Pironio, 2005).

### 1. Self-testing

Self-testing is a sophisticated form of quantum certification where Alice and Bob are ideally able to pinpoint their shared quantum state and measurements only from examining their nonlocal correlations (Mayers and Yao, 2004). These cannot be precisely deduced because quantum correlations in Bell scenarios are invariant under collective changes of reference frame. Hence, at best they can be determined up to local transformations that leave the correlations invariant. Such transformations are those that preserve inner products; they are called isometries.[24] A simple example is that, from any correlations achieving the Tsirelson bound of the CHSH inequality, one can deduce that the state is a singlet up to local isometries (Summers and Werner, 1987; Braunstein, Mann, and Revzen, 1992; Popescu and Rohrlich, 1992; Tsirelson, 1993). For a review of self-testing, see Šupić and Bowles (2020).

SDP techniques offer a powerful approach to self-testing. To showcase this we first define an operator

$$\mathcal{B} = \beta_Q \mathbb{1} - \sum_{a,b,x,y} c_{abxy} A_{a|x} \otimes B_{b|y}. \tag{71}$$

The second term is the Bell operator associated with a quantum model for a generic Bell functional. We use $\beta_Q$ to denote the Tsirelson bound of that Bell inequality, i.e., the maximal quantum value of the Bell parameter. Hence, one can think of Eq. (71) as a shifted Bell operator tailored such that $\langle\psi|\mathcal{B}|\psi\rangle \geq 0$ for all quantum states; i.e., the operator is PSD. Assume now that we are able to find a decomposition of $\mathcal{B}$ as a sum of squares of some operators $\{P_l\}$,

$$\mathcal{B} = \sum_l P_l^\dagger P_l, \tag{72}$$

where $P_l$ are polynomials of the local measurement operators $\{A_{a|x}\}$ and $\{B_{b|y}\}$. Witnessing the Tsirelson bound, namely, $\langle\psi|\mathcal{B}|\psi\rangle = 0$, therefore implies that $P_l|\psi\rangle = 0$ for all $l$. These relations can be useful for deducing properties of the local measurements (Yang and Navascués, 2013; Bamps and Pironio, 2015). Take the CHSH inequality, for which finding an SOS decomposition for Eq. (71) is particularly simple: working with the observables instead of the POVM elements, one can choose $P_1 = (A_1 + A_2)/\sqrt{2} - B_1$ and $P_2 = (A_1 - A_2)/\sqrt{2} - B_2$. Following the given procedure, one deduces that $\{A_1, A_2\}|\psi\rangle = \{B_1, B_2\}|\psi\rangle = 0$; i.e., the local measurements must anticommute on the support of the state. One can then take this further and leverage these relations together with a well-chosen local isometry to deduce the shared state.

The key component in this discussion is to first find the Tsirelson bound $\beta_Q$ and then find an SOS decomposition of the form of Eq. (72). By considering a sufficiently high level of the NPA hierarchy, one can often recover $\beta_Q$. To verify that the bound returned by the NPA hierarchy is optimal, one can match it with an explicit quantum strategy for the Bell test. An SOS decomposition can then also be extracted. As we saw in Sec. III.B, such SOS decompositions correspond to the dual of a noncommutative polynomial optimization problem. By considering both primal and dual SDPs (Doherty *et al.*, 2008) of the NPA hierarchy, one can systematically approach the problem. Indeed, this can be done analytically even for some Bell inequalities by identifying a suitable relaxation level (Yang and Navascués, 2013; Bamps and Pironio, 2015). In particular, explicit SOS decompositions have been reported for the tilted CHSH inequalities (Yang and Navascués, 2013; Bamps and Pironio, 2015), a three party facet Bell inequality without a quantum violation (Almeida *et al.*, 2010), multioutcome generalizations of the CHSH inequality (Kaniewski *et al.*, 2019), chained Bell inequalities (Šupić *et al.*, 2016), and Bell inequalities tailored for graph states (Baccari *et al.*, 2020). Further methods have been developed to generate Bell inequalities that will always admit SOS decompositions (Barizien, Sekatski, and Bancal, 2024), resulting in a method to design Bell inequalities to self-test a given quantum state. Notably, however, this general SDP approach is not guaranteed to lead to a self-testing statement for both states and measurements.

When the Bell inequality violation is nonmaximal, self-testing is also possible, albeit with other techniques. A useful approach employs SDP methods to place a lower bound on the fidelity of the state with the ideal state that would have been certified had the Tsirelson bound been reached. This is achieved using the swap method (Yang *et al.*, 2014; Bancal *et al.*, 2015). The main idea can be illustrated for the case of CHSH. Since CHSH targets a two-qubit state in the registers $A$ and $B$, we can introduce qubit ancillas $A'$ and $B'$ into which the parties aim to swap their state. To do this, they need to individually use the SWAP operator. For Alice the SWAP operator can be written as $S_{AA'} = WVW$, where $W = \mathbb{1} \otimes |0\rangle\langle 0| + \sigma_X \otimes |1\rangle\langle 1|$ and $V = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_X$ are CNOT gates. One cannot assume the specific operation on system $A$, because of the device-independent picture, but can instead try to emulate the SWAP operator using an operation that on $A$ depends only on Alice's measurements. While emulation is not unique and less immediate approaches can enhance the results, a concrete example is instructive. Knowing that the local measurements are ideally qubits and anticommuting, it is reasonable to target a correspondence of $A_1$ and $B_1$ to $\sigma_Z$ and a correspondence of $A_2$ and $B_2$ to $\sigma_X$. The optimal maximally entangled state is then a local rotation of the singlet $|\psi^-_{\text{target}}\rangle$. Hence, the emulated SWAP operator corresponds to $W = \mathbb{1} \otimes |0\rangle\langle 0| + A_2 \otimes |1\rangle\langle 1|$ and $V = (\mathbb{1} + A_1)/2 \otimes \mathbb{1} + (\mathbb{1} - A_1)/2 \otimes \sigma_X$ for Alice and, analogously, for Bob. The swapped state is

$$\rho'_{A'B'} = \text{tr}_{AB}(S\psi_{AB} \otimes |0\rangle\langle 0|_{A'} \otimes |0\rangle\langle 0|_{B'} S^\dagger), \tag{73}$$

where $S = S_{AA'} \otimes S_{BB'}$. In Eq. (73) $\rho'_{A'B'}$ is a $4 \times 4$ matrix whose entries are linear combinations of moments; see Eq. (64). Its fidelity with the target state $F = \langle\psi^-_{\text{target}}|\rho'|\psi^-_{\text{target}}\rangle$ is therefore also a linear combination of moments. Thus, if we relax the quantum set of correlations

[24] An isometry can be seen as a linear map that consists of a possible appending of additional degrees of freedom to the system followed by a unitary transformation. They are defined as linear operators $V$ satisfying $V^\dagger V = \mathbb{1}$.

into a moment matrix problem *à la* NPA, we can view the fidelity as a linear objective and thus obtain a robust self-testing bound via SDP. This applies also to other Bell inequalities and other constructions of the SWAP operator. The SDP relaxation for the fidelity, at the $k$th level of the NPA hierarchy, becomes

$$\begin{aligned} \min_{\Gamma_k} \quad & F(\Gamma_k) \\ \text{such that} \quad & \sum_{a,b,x,y} c_{abxy}\Gamma_k(A_{a|x}, B_{b|y}) = \beta, \\ & \Gamma_k \succeq 0, \end{aligned} \tag{74}$$

where $\beta \leq \beta_Q$ is the witnessed Bell parameter. A practically useful relaxation typically requires selected monomials from different levels (i.e., an intermediate level; see the remark in Sec. III.B.2) in order to ensure that all moments appearing in $F$ also appear in the moment matrix. An important subtlety is that for some Bell scenarios and choices for emulating the SWAP operator, the operation may cease to be unitary in general. This can be remedied (Bancal *et al.*, 2015) with the introduction of localizing matrices in the SDP relaxation (74). In the literature, the swap method has been applied to noisy self-testing of partially entangled two-qubit states (Bancal *et al.*, 2015), three-dimensional states (Salavrakos *et al.*, 2017), the three-qubit $W$ state (Wu *et al.*, 2014), four-qubit Greenberger-Horne-Zeilinger (GHZ) and cluster states (Pál, Vértesi, and Navascués, 2014), and symmetric three-qubit states (Li *et al.*, 2020). The aforementioned relaxation naturally provides an upper bound on the minimal Bell inequality violation required to certify a nontrivial fidelity with $|\psi^-_{\text{target}}\rangle$. Complementing this, SDPs were used by Valcarce *et al.* (2020) to search for systems producing Bell inequality violations with trivial fidelities, thereby providing lower bounds on the minimal CHSH violation needed to obtain nontrivial robust self-testing statements.

### 2. Entanglement dimension

Hilbert space dimension roughly represents the number of controlled degrees of freedom in a physical system. It is therefore unsurprising that it plays a significant role in quantum nonlocality: by creating entanglement in higher dimensions, one can potentially increase the magnitude of a Bell inequality violation, and sometimes quantum correlations even necessitate infinite dimensions (Coladangelo and Stark, 2020; Beigi, 2021). We now discuss different approaches to characterizing the set of quantum nonlocal correlations when states and measurements are limited to a fixed dimension $d$.

Dimensionally restricted quantum nonlocality can be linked to the separability problem of quantum states (Navascués, de la Torre, and Vértesi, 2014). To see the connection, let Alice and Bob share a two-qubit ($d = 2$) state $\rho_{AB}$ on which they perform basis projections $\{|a_x\rangle\langle a_x|, \mathbb{1} - |a_x\rangle\langle a_x|\}$ and $\{|b_y\rangle\langle b_y|, \mathbb{1} - |b_y\rangle\langle b_y|\}$, respectively. One can now shift the status of these operators from measurement projections to ancillary states. To do that, we append the main registers $A$ and $B$ with additional $X$- and $Y$-qubit registers, respectively, $A_1, \ldots, A_X$ and $B_1, \ldots, B_Y$ and define the $(2 + X + Y)$-qubit state $\sigma = \rho_{AB} \bigotimes_{x=1}^{X} |a_x\rangle\langle a_x| \bigotimes_{y=1}^{Y} |b_y\rangle\langle b_y|$. The quantum correlations can be recovered by Alice (Bob) applying operators $G_{a,x}$ ($H_{b,y}$) that act as the identity on all ancillary registers except $A_x$ ($B_y$), which instead are swapped with system $A$ ($B$) via the two-qubit SWAP operator $S$ for outcome $a = 1$ and, respectively, its complement $\mathbb{1} - S$ for outcome $a = 2$. This yields $p(a, b|x, y) = \text{tr}(\sigma G_{a,x} \otimes H_{b,y})$. The optimum of any Bell parameter for qubits is then converted into a type of entanglement witnessing problem where one must evaluate the optimum of $\text{tr}(\sigma\mathcal{B})$ for a known Bell operator $\mathcal{B} = \sum_{a,b,x,y} c_{abxy} G_{a,x} \otimes H_{b,y}$ over a multiqubit state $\sigma$ that is separable with respect to the partition $AB|A_1|\ldots|A_X|B_1|\ldots|B_Y$, where all ancillary registers are separated from each other and from the joint register $AB$. As discussed in Sec. IV.A, this problem can be addressed systematically via the DPS hierarchy. This method has also been extended to scenarios with more outcomes and parties. However, it is useful mainly when the number of inputs is small owing to the increasing number of subsystems in $\sigma$. It can be found to be more efficient when only some parties have a restricted dimension since the other parties then can be treated as in the NPA hierarchy.

Another way to link fixed-dimensional quantum nonlocality problems to the separability problem was proposed by Jee *et al.* (2021). This method has the advantage of coming with good bounds on the convergence rate of the resulting SDP relaxations, and the disadvantage of poor performance in practice. In the case of free games, i.e., nonlocal games where the probability distribution over the inputs is a product between a distribution for Alice and another for Bob, the complexity of computing an $\epsilon$-close approximation to the $d$-dimensional Tsirelson bound scales polynomially in the input size and quasipolynomially in the output size. In the general case the complexity is still quasipolynomial in the output size but becomes exponential in the input size.

The problem can also be approached without connecting it to a separability problem and instead adding dimension constraints directly to the NPA moment matrix. This may consist of identifying operator equalities that hold only up to dimension $d$. For example, the identity $[X_1, [X_2, X_3]^2] = 0$ holds for all complex square matrices of dimension $d \leq 2$. However, this is difficult to do in practice since a complete set of operator equalities is not known for $d \geq 3$. A handy alternative is instead to implicitly capture the constraints associated with a dimensional restriction, on the level of the NPA moment matrix, by employing numerical sampling in the $d$-dimensional space (Navascués and Vértesi, 2015). See Sec. VI.B.1 for more details. This method is known to converge to the quantum set of correlations and is often useful for practical purposes when problems are not too large (Navascués, Feix *et al.*, 2015).

For the special case of restricting to bipartite maximally entangled states of dimension $d$, it is possible to construct a sampling-free SDP relaxation hierarchy based on tracial moments of measurement operators that act only on a single Hilbert space (Lang, Vértesi, and Navascués, 2014). This is a consequence of the identity $\text{tr}(A \otimes B\phi_d^+) = (1/d)\text{tr}(AB^T)$. Systematic implementations based on projective measurements were reported by Lin, Vértesi, and Liang (2022).

### 3. Entanglement certification

Quantum nonlocality, understood as the absence of an explanation of correlations in terms of an LHV model (11), implies entanglement and therefore allows for device-independent entanglement certification. This is an inference of entanglement without any modeling of the experimental measurement apparatus. Fundamentally this black-box approach to entanglement comes at the cost of some entangled states not being detectable (Werner, 1989; Augusiak, Demianowicz, and Acín, 2014), although this can be at least partly remedied by considering more complicated nonlocality experiments; see Sen(De) *et al.* (2005), Cavalcanti *et al.* (2011), Bowles *et al.* (2018), and Bowles, Hirsch, and Cavalcanti (2021). Nevertheless, a variety of interesting entangled states can still be certified, typically those that are not too noisy, and SDPs offer an effective path for that purpose.

Local measurements performed on an $n$-partite fully separable quantum system always yield local correlations. Hence, one can certify entanglement device independently for a given correlation $p$ by evaluating the LP in Eq. (12) that checks its membership to the local polytope. However, this is demanding because the number of variables in the LP scales exponentially in the number of parties and inputs, and polynomially in the number of outputs. Using simplex methods for linear programming, states of up to $n = 7$ qubits were certified by Gruca *et al.* (2010). This was increased to $n = 11$ qubits by Gondzio *et al.* (2014), who adopted a matrix-free approach for interior-point solvers that reduces memory requirements (Gondzio, 2012).

However, one can go further by considering SDP relaxations of the local polytope. A key observation is that any local correlation between $n$ parties can be obtained from locally commuting measurements on a quantum state. Take the fully separable state $\rho = \sum_\lambda p(\lambda)|\lambda\rangle\langle\lambda|^{\otimes n}$, and let the $x_l$th POVM of the $l$th party be $M_{x_l}^{a_l} = \sum_\mu D(a_l|x_l,\mu)|\mu\rangle\langle\mu|$, where $D(a_l|x_l,\mu)$ is a deterministic distribution. All of these POVMs commute. Evaluating the Born rule, one finds the generic local model given in Eq. (11). Thus, a sufficient condition for nonlocality is that $p$ fails some level of the NPA hierarchy under the extra constraint that all local measurements commute. The latter appears in the form of additional equality constraints between the elements of the NPA moment matrix of Eq. (64) that effectively turn it into a Lasserre hierarchy; see Sec. III.A. When the second level relaxation[25] of the commuting NPA hierarchy was used, nonlocality was reported[26] for $W$ states, GHZ states, and graph states reaching up to $n = 29$ qubits (Baccari *et al.*, 2017). A similar approach can also be used to certify entanglement in the steering scenario. On Alice's side one imposes commutation in the NPA relaxation, whereas on Bob's side one replaces the unknown measurements with known measurements and uses their algebraic relations to further constrain the moment matrix (Kogias *et al.*, 2015). A simple example of the latter is to assume that Bob's measurements are qubit and mutually unbiased and impose it on the moment matrix by having the corresponding observables anticommute.

A natural next question is how one can device-independently quantify entanglement. The main intuition is that a stronger violation of a Bell inequality ought to require stronger forms of entanglement. This question can be addressed through a reinterpretation of the NPA hierarchy of Moroder *et al.* (2013). Consider that we apply local completely positive maps $\Lambda_A\colon \mathcal{H}_A \to \mathcal{H}_{A'}$ and $\Lambda_B\colon \mathcal{H}_B \to \mathcal{H}_{B'}$ to a bipartite state $\rho_{AB}$. Their action can be represented in terms of unnormalized Kraus operators, i.e., a set of operators $\{K_{i,A}\}_i$ and $\{K_{i,B}\}_i$. We now put Alice's and Bob's local POVM elements in lists $\mathbf{A} = \{\mathbb{1}, A_{1|1}, \ldots, A_{N|X}\}$ and $\mathbf{B} = \{\mathbb{1}, B_{1|1}, \ldots, B_{M|Y}\}$, respectively. We then define Kraus operators of Alice as $K_{i,A} = \sum_{l_1,\ldots,l_k} |l_1, \ldots, l_k\rangle i\mathbf{A}_{l_1}\ldots\mathbf{A}_{l_k}$, and analogously for Bob, where the index $k$ is the level of the hierarchy. The moment matrix $\Gamma = \Lambda_A \otimes \Lambda_B[\rho]$ becomes

$$\Gamma = \sum_{\bar{r},\bar{l}} \sum_{\bar{s},\bar{k}} \mathrm{tr}(\rho \mathcal{A}_{\bar{r},\bar{l}} \otimes \mathcal{B}_{\bar{s},\bar{k}})|\bar{l},\bar{k}\rangle\langle\bar{r},\bar{s}|, \tag{75}$$

where $\bar{l} = (l_1, \ldots, l_k)$, and similarly for $\bar{k}$, $\bar{r}$, and $\bar{s}$, and where $\mathcal{A}_{\bar{r},\bar{l}} = (\mathbf{A}_{r_1}\ldots\mathbf{A}_{r_k})^\dagger \mathbf{A}_{l_1}\ldots\mathbf{A}_{l_k}$, and similarly for $\mathcal{B}_{\bar{s},\bar{k}}$. This moment matrix would be the same as that of the NPA hierarchy if instead of local completely positive maps we had opted for global completely positive maps. The advantage of this formulation is that it comes with an explicit bipartition on the level of the moment matrix. This allows for the PPT constraint, which is needed for device-independent entanglement quantification via the entanglement negativity measure, to be imposed. The negativity $N(\rho_{AB})$ is defined as the sum of the negative eigenvalues of $\rho_{AB}^{T_A}$, which can itself be cast as an SDP; see Eq. (56). On the level of the moment matrix, the SDP becomes $N(\rho_{AB}) = \min \mathrm{tr}(\chi_-)$ such that $\rho = \chi_+ - \chi_-$, where $(\chi_\pm)^{T_A} \succeq 0$. Thus, the negativity can be bounded by employing the aforementioned SDP relaxation for both the operators $\chi_\pm$, imposing their PPT property on $\Gamma$ and noting that the objective function is simply an element of the moment matrix. The idea of building a moment matrix featuring a bipartition can also be extended to the steering scenario (Pusey, 2013). This allows for one-side device-independent quantification of entanglement, which has also been considered for highly symmetric scenarios with multiple outcomes (Huang *et al.*, 2021).

While the negativity is relevant as one possible quantifier of bipartite entanglement, other approaches are needed for multipartite entanglement. If we have a multipartite quantum state, a natural question is to ask for the smallest cluster of subsystems that must be entangled in order to model the correlations $p$. The smallest number of entangled subsystems required $D$ is known as the entanglement depth (Sørensen and Mølmer, 2001). Nonlocality alone gives only a device-independent certificate that some entanglement is present, i.e., that $D \geq 2$. It was first noted by Bancal *et al.* (2011) that the NPA hierarchy with suitably imposed local measurement-commutation relations can be used to detect a maximal entanglement depth of $D = 3$ in a three-partite system. For systems of more particles, one can employ the hierarchy of

[25]Note that local commutation is a trivial constraint at the first level of relaxation; i.e., the associated correlation set is still $\mathcal{Q}_1$.

[26]For some states one requires small additions to the second level, but these can be independent of the number of qubits.

Moroder *et al.* to relax separability across a given bisection of the subsystems to a PPT condition and use that to bound the entanglement depth (Liang *et al.*, 2015; Lin *et al.*, 2019).

Furthermore, by restricting to few-body correlators that are symmetric under permutations of parties, one can formulate a hierarchy of SDP relaxations of the corresponding party-permutation-invariant local polytope that benefits considerably from the imposed symmetry. This was showcased by Fadel and Tura (2017), who first relaxed the local polytope to a semialgebraic set. It is then leveraged that such sets can be relaxed to SDPs (Gouveia, Parrilo, and Thomas, 2010; Gouveia and Thomas, 2012). The advantage of this approach is that the number of subsystems is featured as an explicit parameter in the SDP and does not impact the size of the moment matrix. In this way one can obtain party-permutation-invariant Bell inequalities for any number of parties via the dual SDP. Permutation-invariant Bell expressions based on two-body correlators have been used to build device-independent witnesses of entanglement depth using relaxations to PPT conditions (Aloy *et al.*, 2019; Tura *et al.*, 2019).

#### 4. Joint measurability

It has been known since the early development of quantum theory that the values of some sets of measurements, such as position and momentum, cannot be simultaneously known (Heisenberg, 1925). This fundamental feature of quantum theory, which is known as measurement incompatibility, has been at the forefront of significant research and development within quantum theory (Heinosaari, Miyadera, and Ziman, 2016; Gühne *et al.*, 2023).

Formally, given a collection of POVMs $\{A_{a|x}\}_a$ indexed by some $x$, we say the collection is *compatible* or *jointly measurable* if there exist a parent POVM $\{M_\lambda\}_\lambda$ and a conditional probability distribution $p(a|x,\lambda)$ such that

$$A_{a|x} = \sum_\lambda p(a|x,\lambda) M_\lambda \tag{76}$$

for all $a$ and $x$. Operationally the statistics of compatible measurements can be simulated by measuring the "parent" measurement $\{M_\lambda\}_\lambda$ and then postprocessing the results. If such a decomposition does not exist, then we say that the measurements are incompatible.

It is well known that incompatible measurements are necessary for Bell nonlocality (Fine, 1982), although not sufficient (Bene and Vértesi, 2018; Hirsch, Quintino, and Brunner, 2018). However, when a party in a Bell test has access to more than two measurements, it is possible that some subsets of their measurements are compatible, while the entire set of measurements remains incompatible. A collection of subsets for which the measurements are compatible is referred to as a compatibility structure. Quintino *et al.* (2019) investigated how different compatibility structures can be device-independently ruled out by large enough Bell inequality violations. From the perspective of nonlocality, if the behavior is restricted to the subsets of inputs for which the measurements are compatible, then it necessarily becomes local. Thus, by combining linear programming constraints for compatible subsets [see Eq. (12)] with the NPA hierarchy, one can explore relaxations of the sets of correlations with different compatibility structures and in turn find Bell-like inequalities that rule out different structures in a device-independent manner.

Once the presence of measurement incompatibility has been device-independently detected, a natural follow-up question is whether the degree of incompatibility can be quantified. One such measure of incompatibility is the so-called incompatibility robustness (Haapasalo, 2015; Uola *et al.*, 2015). For a collection of measurements $\{A_{a|x}\}_{a,x}$, this is defined as

$$\begin{aligned} \min \quad & t \\ \text{such that} \quad & \left\{\tfrac{1}{1+t}(A_{a|x}+tN_{a|x})\right\}_{a,x} \quad \text{are compatible,} \\ & \textstyle\sum_a N_{a|x} = \mathbb{1} \quad \forall\, x, \\ & N_{a|x} \succeq 0 \qquad \forall\, a,x, \\ & t \geq 0, \end{aligned} \tag{77}$$

which roughly captures the amount of noise, represented by a shift toward another set of POVMs $N_{a|x}$ that one needs to add to the measurements $A_{a|x}$ in order to make them compatible. There are many other such measures of incompatibility, and these measures can often themselves be expressed as SDPs (Gühne *et al.*, 2023). This includes the incompatibility robustness that can be computed by the SDP,

$$\begin{aligned} \min \quad & \tfrac{1}{d}\mathrm{tr}(M_\lambda) \\ \text{such that} \quad & \textstyle\sum_\lambda D(a|x,\lambda) G_\lambda \succeq A_{a|x} \quad \forall\, a,x, \\ & \textstyle\sum_\lambda G_\lambda = \mathbb{1}\,\tfrac{1}{d}\sum_\lambda \mathrm{tr}(G_\lambda), \\ & G_\lambda \succeq 0, \end{aligned} \tag{78}$$

where $D(a|x,\lambda)$ are deterministic distributions; see Eq. (8).

Chen *et al.* (2016) related the incompatibility problem to a steering problem to show that the incompatibility robustness can be lower bounded by a steering robustness quantity, which is an analogous quantity for quantifying steerability. A hierarchy of SDP device-independent lower bounds on the latter quantity can then be derived to give a method to compute device-independent lower bounds on incompatibility. Several additional lower bounds on the incompatibility robustness in terms of other robustness quantities were provided by Cavalcanti and Skrzypczyk (2016), such as the consistent nonlocal robustness, which can similarly be turned into device-independent lower bounds on the incompatibility robustness using the NPA hierarchy. Cavalcanti and Skrzypczyk, who surveyed many robustness measures and their computability via SDPs, also introduced a new quantity called the consistent steering robustness, which provides tighter lower bounds on the incompatibility robustness than the standard robustness of steering. By combining this with moment matrix techniques developed by Chen *et al.* (2016), one can obtain even stronger device-independent bounds on the incompatibility robustness, which in some cases can even be shown to be tight (Chen *et al.*, 2018). Later a general method to obtain device-independent

bounds on SDP representable incompatibility measures was presented by Chen *et al.* (2021). Avoiding proxy quantities facilitates a much stronger characterization of the incompatibility robustness that can even be shown to be tight for the correlations achieving the Tsirelson bounds of the tilted CHSH inequalities.

## VI. QUANTUM COMMUNICATION

In this section we discuss quantum correlations in the prepare-and-measure scenario, introduced in Sec. II.B.2, in which Alice prepares messages and Bob measures them. Such correlations have been studied for several different types of communication, and SDP relaxations play a central role in their characterization and applications.

### A. Channel capacities

We provide an overview of channel coding before proceeding to the role of SDPs in the topic. In information theory a paradigmatic task is to encode a message, send it over a channel, and then reliably decode it. Specifically, the sender selects a message from an alphabet of size $M$ and encodes it into a code word consisting of $n$ letters, where $n$ is called the block-length. Each letter is then sent over the channel $\Lambda$, which in the classical case can be represented as a conditional probability distribution $p_\Lambda(y|x)$ mapping the input $x$ to the output $y$. Since the channel is noisy, it outputs a distorted code word, which the receiver must decode into the original message; see Fig. 4.

The seminal work of Claude Shannon (Shannon, 1948) showed how to address the efficiency of the communication when the distributions of the letters in the code word are independent and identical. The key idea of Shannon was to allow a small error probability in the decoding, which then tends to zero in the limit of large $n$. In this setting, when a memoryless noisy classical channel is used asymptotically many times, it is natural to consider the largest rate $R = \log_2 M/n$, i.e., the ratio of the number of message bits and the number of channel uses, at which information can reliably be transmitted. This rate $\mathcal{C}_{cc}(\Lambda)$ is called the capacity of the channel, and Shannon proved that it is given by the largest single-copy mutual information between the channel's input and output (Shannon, 1948),

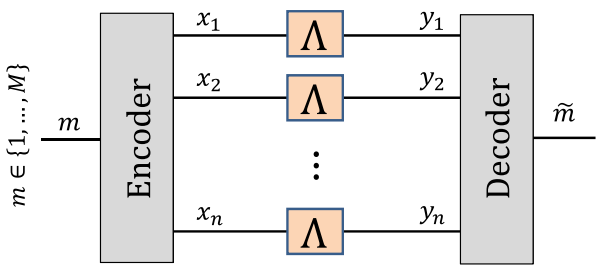


FIG. 4. Unassisted classical channel coding scenario. A message $m$ is selected from a given alphabet and encoded into a code word consisting of $n$ letters. Each letter $x_i$ is then sent through the channel, returning distorted letters $y_i$ that are decoded into a guess $\tilde{m}$ of the original message.

$$\mathcal{C}_{cc}(\Lambda) = \max_{\{p_x\}} I(X;Y), \tag{79}$$

where $I(X;Y) = H(X) + H(Y) - H(X,Y)$ and $H$ denotes the Shannon entropy.

A natural endeavor is to extend this type of question to scenarios with quantum resources; see Holevo and Giovannetti (2012), Wilde (2013), and Gyongyosi, Imre, and Nguyen (2018) for a thorough discussion and Holevo (2020) for an overview. The Holevo-Schumacher-Westmoreland theorem (Schumacher and Westmoreland, 1997; Holevo, 1998) generalizes Eq. (79) to the scenario where the channel instead is quantum; i.e., the message is encoded in a quantum state. The classical capacity of a quantum channel is given by

$$\mathcal{C}_{cq}(\Lambda) = \lim_{n\to\infty} \frac{\chi(\Lambda^{\otimes n})}{n}, \tag{80}$$

where $\chi(\Lambda) = \max_{\{p_x\},\{\rho_x\}} H[\sum_x p_x \Lambda(\rho_x)] - \sum_x p_x H[\Lambda(\rho_x)]$ is called the Holevo capacity of the channel and the maximization is taken over all input ensembles to the channel. In contrast to the classical case, the possibility of entanglement in the quantum code word implies that the Holevo capacity is not additive[27] (Hastings, 2009), and hence Eq. (80) cannot generally be reduced to a single-letter formula, i.e., a closed expression based on a single use of $\Lambda$, but exceptions are known for convenient special cases; see Bennett, DiVincenzo, and Smolin (1997) and King (2002, 2003). Nonadditivity makes the computation of $\mathcal{C}_{cq}(\Lambda)$ difficult.

A contrasting situation is when the sender and receiver additionally are allowed to share entanglement. The resulting entanglement-assisted classical capacity of the quantum channel admits a single-letter formula similar to Eq. (79), but instead of maximizing the classical mutual information one maximizes the quantum mutual information of the bipartite state $(\mathbb{1} \otimes \Lambda)[\rho_{AB}]$ over all entangled states $\rho_{AB}$ (Bennett *et al.*, 1999, 2002).

Another natural scenario is when the message itself is a quantum state. One then speaks of quantum capacities. In a general picture it is possible to characterize the performance of a classical or quantum protocol in terms of the triplet $(R, n, \epsilon)$, where $\epsilon$ is the error tolerated in the decoding. This error is favorably represented in terms of the fidelity between the maximally entangled state and the state obtained by sending half of it through the communication scheme. The central question is then to characterize the set $(R, n, \epsilon)$ that is achievable for a given quantum channel. In the asymptotic setting $(n \to \infty)$ and independent channel uses, the quantum capacity of the quantum channel $\mathcal{C}_{qq}(\Lambda)$ is the largest rate $R$ at which the error tends to zero. It is given by the Lloyd-Shor-Devetak theorem (Lloyd, 1997; Devetak, 2005) in terms of the largest coherent information[28] when optimized over all bipartite input states after half of it is passed through the channel. However, this quantity must be regularized; i.e., one must take a many-copy limit

[27]The failure of additivity for the Holevo capacity implies that several other entropic quantities are also not additive (Shor, 2004).

[28]The coherent information is defined as $I_{\mathrm{coh}}(\rho_{AB}) = H(\rho_B) - H(\rho_{AB})$.

analogous to that in Eq. (80). This renders the capacity nonadditive and therefore difficult to compute.

### 1. Classical capacities

In the conventional setting, the decoding errors are tolerated as long as they vanish in the limit of large block-length. A stricter approach in which errors are exactly zero for any $n$ is called zero-error coding[29] (Shannon, 1956). In zero-error capacity problems, one needs only to consider whether two distinct messages could be confused with each other after they are sent through the channel. Therefore, if the channel is used only once, one can represent the zero-error problem as a graph where each vertex represents a message and each edge represents the possibility that two messages can be mapped onto the same output. The one-shot zero-error capacity is given by the largest set of independent vertices in this graph, known in the literature as the confusability graph. For larger block-length one must consider the strong power of the graph. However, computing the independence number is NP hard (Karp, 1972). The prominent work of Lovász (1979) showed that the independence number of a graph $G$ can be upper bounded via the so-called Lovász theta function, which admits an SDP formulation

$$\begin{aligned} \vartheta(G) = \max \quad & \mathrm{tr}(XE) \\ \text{such that } & X_{ij} = 0 \quad \text{if } i \text{ and } j \text{ are connected}, \\ & \mathrm{tr}(X) = 1, \\ & X \succeq 0, \end{aligned} \tag{81}$$

where $E_{ij} = 1$. The Lovász theta function has the important property that it factors under strong products of graphs, which allows one to address the asymptotic limit for zero-error coding. It has been proven that this SDP also bounds the entanglement-assisted zero-error classical capacity (Beigi, 2010; Duan, Severini, and Winter, 2013). Bounds of this sort are important because it is known that the one-shot zero-error classical capacity can be increased by means of shared entanglement (Cubitt *et al.*, 2010). In fact, this is connected to proofs of the Kochen-Specker theorem, which in turn can be represented in the language of graph theory (Cabello, Severini, and Winter, 2014). Entanglement-assisted advantages are also possible for asymptotic zero-error coding. Perhaps surprisingly the zero-error capacity can sometimes even equal the classical capacity of a quantum channel (80) (Leung *et al.*, 2012). In contrast, the zero-error problem becomes simpler if the sender and receiver are permitted to share general bipartite no-signaling correlations. The capacity can then be computed via an LP which corresponds to the fractional packing number of the confusability graph (Cubitt *et al.*, 2011). This can also be generalized to parties that share quantum no-signaling correlations[30]: in the one-shot setting, the capacity is given by an SDP, and sometimes an SDP can also be formulated for the asympototic capacity. If quantum no-signaling correlations are permitted, the Lovász theta function corresponds to the smallest zero-error classical capacity of any channel associated with the same confusability graph (Duan and Winter, 2016).

A related problem considers a one-shot classical channel and a given number of messages and then addresses the largest average success probability with which they can be communicated through the channel. The answer can be approximated in polynomial time only up to a factor of $1 - 1/e$, and obtaining a better approximation is NP hard (Barman and Fawzi, 2016). An upper bound is nevertheless known (Polyanskiy, Poor, and Verdú, 2010). This bound admits a good physical interpretation as it is equivalent to the optimal success probability obtained from assisting the classical channel with bipartite no-signaling correlations (Matthews, 2012). As made intuitive from this connection, the solution can be bounded by means of relaxation to an LP. Beyond point-to-point channels, the capacity regions of broadcast and multiple-access channels under no-signaling assistance can also be analyzed using linear programming (Fawzi and Fermé, 2024a, 2024b). This classical information problem can also be considered in the quantum case. For a given block-length and a given tolerance for the error, upper bounds on the optimal transmission rate over a general quantum channel (also when assisted by entanglement) can be obtained by means of SDP by relating the problem to hypothesis testing relative entropies (Matthews and Wehner, 2014). These bounds were later made tighter by Wang, Xie, and Duan (2018), applied also to the entanglement-assisted case, and used to give SDP upper bounds on the classical capacity of the qubit amplitude-damping channel. For the large block-length limit, namely, the asymptotic channel coding scenario, Fawzi, Shayeghi, and Ta (2022) showed how to compute a sequence of upper bounds on $\mathcal{C}_{cq}$ via a hierarchy of SDP-tailored Rényi divergences (Fawzi and Fawzi, 2021), but its convergence to $\mathcal{C}_{cq}$ is not presently known. These SDPs are rendered considerably more efficient by invoking symmetry properties in the spirit of the discussion in Sec. IX.F. SDP methods in this vein can sometimes also be used to obtain strong converse bounds[31] on the classical capacity (Wang, Xie, and Duan, 2018; Ding *et al.*, 2023). An alternative strong converse bound is obtained from the quantum reverse Shannon theorem (Berta, Christandl, and Renner, 2011; Bennett *et al.*, 2014): if one sends messages at a rate above the entanglement-assisted classical capacity, then the error tends to unity exponentially with $n$.

As highlighted by Fawzi and Fawzi (2018), this capacity can be approximated by SDP due to the possibility of establishing SDP bounds on the quantum relative entropy

[29]This is not only of independent interest: the zero-error capacity is also relevant for how rapidly the error tends to zero for an increasing block-length in the standard capacity (Shannon, Gallager, and Berlekamp, 1967).

[30]Quantum no-signaling correlations are completely positive and trace-preserving bipartite linear maps that forbid signaling of classical information in either direction.

[31]The strong converse property means that the error probability tends exponentially to 1 if the rate exceeds the bound. This property is known for some quantum channels; see Ogawa and Nagaoka (1999), Winter (1999), König and Wehner (2009), and Wilde, Winter, and Yang (2014).

(Fawzi, Saunderson, and Parrilo, 2019). As mentioned in Sec. VII.B.2, recent algorithmic developments have made it possible to optimize the quantum relative entropy directly, and thus compute the channel capacity, without relying on relaxations (He, Saunderson, and Fawzi, 2024).

### 2. Quantum capacities

In general it is difficult to determine capacities in a computable way. A mathematically tractable framework is to view the encoding and decoding operations as a single global, bipartite operation $Z_{AA'BB'}$, where $A$ and $B$ are input systems and $A'$ and $B'$ are output systems (Leung and Matthews, 2015); see Fig. 5. In practice $B$ depends on $A'$ since system $A'$ is sent through the channel. One can think of $Z$ as linearly transforming the channel $\Lambda$ into a new channel, and it is known as a superchannel or supermap (Chiribella, D'Ariano, and Perinotti, 2008). To it we assign a Choi matrix $J_Z = d_A d_{B'}(\mathcal{I} \otimes Z)(\phi^+)$, where $\mathcal{I}$ is the identity channel. For the operation $Z_{AA'BB'}$ to be completely positive and trace preserving, the Choi matrix must be PSD and must satisfy $\mathrm{tr}_{A'B'}(J_Z) = \mathbb{1}_{AB}$. Moreover, it must not signal from receiver to sender, which corresponds to $\mathrm{tr}_{B'}(J_Z) = \mathrm{tr}_{BB'}(J_Z) \otimes \mathbb{1}_B$; note that the first factor is the Choi matrix of the sender's transformation. In addition, if the sender and receiver do not share postclassical resources, we need to ensure that they are not entangled with each other. A convenient relaxation of this constraint is to impose the condition that $Z$ is PPT preserving; i.e., that every PPT state remains PPT after being sent through $Z$, which translates into $J_Z^{T_{AA'}} \succeq 0$. The key observation here is that all of these constraints are either linear or semidefinite in the variable $J_Z$.

To address the one-shot quantum capacity of $\Lambda$, we now consider the fidelity between the maximally entangled state and the state obtained from sending half of it through the communication scheme. The fidelity is particularly convenient because it too can be written in terms of the Choi matrix: $F = \mathrm{tr}[J_Z(J_\Lambda^T \otimes \phi^+)]$. Putting it all together, Leung and Matthews (2015) obtained an SDP bound on the one-shot quantum capacity that applies both when the quantum channel is unassisted (relaxation to no signaling and PPT preserving) and when it is entanglement assisted (relaxation to no signaling only). Berta *et al.* (2022) extended this relaxation, by means of connection to a separability problem and using symmetric extensions, into a hierarchy of SDPs that converges to the fidelity $F$. The concept of bounding quantum capacities by means of relaxation to PPT-preserving and/or no-signaling codes was further explored by Wang, Fang, and Duan (2019), who gave SDP bounds for the one-shot, bounded-error capacity. Complementarily, and in a similar spirit, Tomamichel, Berta, and Renes (2016) showed how to determine an SDP upper bound the largest rate $R$ for a fixed number of channel uses $n$ and a fixed error $\epsilon$.

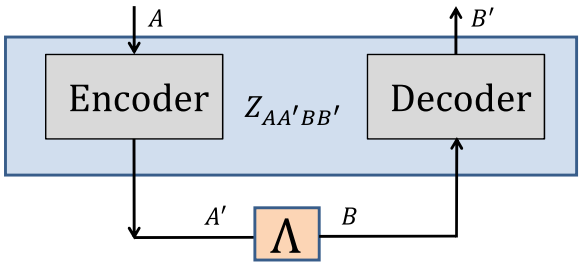


FIG. 5. SDP relaxations of channel coding problems can be obtained by viewing the parties as single bipartite operations.

In the asymptotic setting, deciding whether a given number of quantum states can be sent over many channel uses with zero error is known to be QMA complete (Beigi and Shor, 2007). However, Duan, Severini, and Winter (2013) showed that, in the same way as the SDP-computable Lovász theta function in Eq. (81) can bound the classical problem, the quantum capacity can be bounded via an analogous SDP quantity. Moreover, in the context of strong converse bounds on the asymptotic quantum capacity, one finds good use of SDPs. Taking the diamond norm[32] of the channel after applying a transposition map $T$ consitutes a strong converse bound. Specifically, if the rate exceeds $\log \|\Lambda \circ T\|_\diamond$, then the error tends to unit in the number of channel uses (Müller-Hermes, Reeb, and Wolf, 2016). Note that the diamond norm can be computed efficiently using an SDP (Watrous, 2009, 2013). Another strong converse SDP bound was provided by Wang and Duan (2016b) and Wang, Fang, and Duan (2019). This bound is stronger than the one based on the diamond norm but weaker than another known bound, based on the so-called Rains information of the channel but not straightforward to compute (Tomamichel, Wilde, and Winter, 2017). The SDP bound is given by

$$\begin{aligned} \log \quad & \max_{\rho_A, F_{AB}} && \mathrm{tr}(J_\Lambda F_{AB}) \\ & \text{such that} && -\rho_A \otimes \mathbb{1} \leqslant F_{AB}^{T_B} \leqslant \rho_A \otimes \mathbb{1}, \\ & && \mathrm{tr}(\rho_A) = 1, \\ & && F_{AB}, \rho_A \succeq 0, \end{aligned} \tag{82}$$

and it is additive under tensor products of channels. In fact, this is closely related to the entanglement measure $E_W$ discussed around Eq. (57), and it can be interpreted as the largest value of $E_W$ taken over all purifications of $\rho_A$ when half of the purification is sent through the channel.

Fang and Fawzi (2021a) showed how to systematically compute bounds on several different classical and quantum channel capacities via SDP. These capacities are evaluated from a single use of the channel (no regularization needed), they are computable for general channels, and they admit a strong converse. This method relies on a quantity known as the geometric Rényi divergence that has many convenient properties, such as additivity under tensor products and chain rule (Matsumoto, 2018).

Another type of quantum capacity where SDPs are useful concerns the ability of bipartite quantum channels (such as a noisy control gate) to create entanglement (Bennett *et al.*, 2003). The rate of distilling maximally entangled states over such an interaction can be bounded from above by an entropic quantity, which can in turn be evaluated using an SDP (Bäuml, Das, and Wilde, 2018; Das, Bäuml, and Wilde, 2020).

[32]The diamond norm is defined by $\|\Lambda\|_\diamond = \max_{\rho_{AB}} \|\mathbb{1} \otimes \Lambda(\rho_{AB})\|_1$.

### B. Dimension constraints

A natural quantifier of communication is the dimension of the alphabet of the message sent from Alice to Bob. Classically Alice's message is selected from a $d$-valued alphabet $\{1,\ldots,d\}$, whereas in the quantum case the message is a state $\rho_x$ selected from a $d$-dimensional Hilbert space. While Holevo's theorem (Holevo, 1973) ensures that such quantum systems cannot be used to transmit a message more efficiently than the corresponding classical systems, it is well known that there are many other communication tasks in which quantum messages provide an advantage over classical messages. Examples are the random access codes mentioned in Sec. II.B.2 (Nayak, 1999; Ambainis *et al.*, 2002) and distributed computation (Galvão, 2001).

A central goal is to characterize the set of quantum correlations $\mathcal{Q}$ that can be generated between Alice and Bob for a fixed number of inputs ($X$ and $Y$, respectively) and a fixed number of outputs for Bob ($N$) when Alice sends a $d$-dimensional state to Bob; see Sec. II.B.2. These correlations are given by the Born rule in Eq. (20). This problem is commonly investigated while granting Alice and Bob unbounded shared randomness. This renders $\mathcal{Q}$ convex and the task particularly suitable to SDP methods. Note that the same problem without shared randomness deals with a nonconvex correlation set, which leads to much different quantum predictions; see Hayashi *et al.* (2006), Bowles, Quintino, and Brunner (2014), de Vicente (2017), and Tavakoli (2020). Outer and inner approximations to $\mathcal{Q}$ not only are important for determining the nonclassicality enabled by quantum theory but also serve as an important tool for quantum information applications. SDP relaxations of $\mathcal{Q}$ are useful for this purpose, in particular, since conventional analytical bounds on $\mathcal{Q}$ are possible only in rare special cases; see Brunner, Navascués, and Vértesi (2013), Frenkel and Weiner (2015), and Farkas and Kaniewski (2019).

#### 1. Bounding the quantum set

SDP relaxation hierarchies can be constructed to bound the set of quantum correlations in the prepare-and-measure scenario for arbitrary input-output alphabets and arbitrary dimensions. They are typically based on tracial moments [see Burgdorf and Klep (2012)], on which constraints specific to a $d$-dimensional Hilbert space must be imposed. To this end let $L=\{\mathbb{1},\boldsymbol{\rho},\mathbf{M}\}$, where $\boldsymbol{\rho}=(\rho_1,\ldots,\rho_X)$ and $\mathbf{M}=(M_{1|1},\ldots,M_{N|Y})$, be the list of all operators appearing in the quantum prepare-and-measure scenario. We define $\mathcal{S}_k$ as a set of monomials over $L$ of length $k$. Recall from the remark in Sec. III.B.2 that it is interesting to consider subsets of all the monomials with a given length. An $|\mathcal{S}_k|\times|\mathcal{S}_k|$ moment matrix can be constructed whose entries are given by

$$\Gamma(u,v)=\mathrm{tr}(u^\dagger v) \tag{83}$$

for $u,v\in\mathcal{S}_k$. The moment matrix inherits many constraints from quantum theory. First, normalization implies that $\Gamma(\rho_x,\mathbb{1})=1$. Second, one can without loss of generality restrict to pure states, i.e., $\rho_x^2=\rho_x$. Third, under the restriction of projective measurements,[33] it holds that $M_{b|y}M_{b'|y}=M_{b|y}\delta_{b,b'}$. Fourth, the moment matrix contains elements that are equal to the probabilities observed between Alice and Bob, namely, $\Gamma(\rho_x,M_{b|y})=p(b|x,y)$. In addition, the cyclicity of the trace implies a number of additional equalities between the moments, for example, $\Gamma(\rho_x,M_{b|y}\rho_x)=\Gamma(\rho_x^2,M_{b|y})=\Gamma(\rho_x,M_{b|y})=p(b|x,y)$. Last, an argument analogous to that in Eq. (28) determines that the moment matrix must be PSD.

The key issue is how to add constraints to $\Gamma$ that are specific to the dimension $d$. One option is to identify polynomial operator identities or inequalities that pertain only to dimension $d$. However, such relations are typically unknown, and finding them is difficult. Navascués and Vértesi (NV) (Navascués and Vértesi, 2015) proposed a solution by employing numerical sampling to construct a basis of moment matrices. The prescription is to randomly sample the states and measurements from the $d$-dimensional Hilbert space and then compute a moment matrix sample $\Gamma^{(1)}$ that will automatically satisfy all the aforementioned constraints. The sampling procedure is repeated until a moment matrix sample is found to be linearly dependent on all of the previous samples. This can be quickly checked by vectorizing the samples, arranging them in a matrix, and computing its rank. The process is then truncated and the collected samples $\{\Gamma^{(1)},\ldots,\Gamma^{(m)}\}$ are certain to span[34] a relaxation of the subspace of moment matrices compatible with dimension $d$. To preserve normalization, namely, $\mathrm{tr}(\mathbb{1})=d$, the final moment matrix becomes an affine combination of the samples

$$\Gamma=\sum_{i=1}^{m}\gamma_i\Gamma^{(i)},\quad \text{where}\ \sum_{i=1}^{m}\gamma_i=1. \tag{84}$$

The coefficients $\{\gamma_i\}$ serve as the SDP variables in the necessary condition for the existence of a $d$-dimensional quantum model for $p(b|x,y)$, namely, that it is possible to find $\Gamma\succeq 0$ such that $\Gamma(\rho_x,M_{b|y})=p(b|x,y)$. Note that, by relaxing the latter condition, one can equally well employ the NV hierarchy to bound the extremal quantum value of an arbitrary linear objective function $\sum_{b,x,y}c_{bxy}p(b|x,y)$ characterized by some real coefficients $c_{bxy}$. It is currently unknown whether this hierarchy converges to $\mathcal{Q}$ in its asymptotic limit. Notably, one can also incorporate POVMs by explicitly performing a Neumark dilation in the measurements, albeit at the cost of employing a larger dimension. Alternatively, one can sample directly from the set of POVMs, but that requires the use of localizing matrices to enforce the bounds $M_{b|y}\succeq 0$ and $\sum_{b=1}^{N-1}M_{b|y}\preccurlyeq\mathbb{1}$.

For scenarios with a reasonably small number of inputs and outputs or a fairly low dimension, the NV hierarchy is an effective tool; see the examples given by Navascués, Feix *et al.* (2015) and Bermejo Morán, Pozas-Kerstjens, and Huber

[33] In general, one must also consider POVMs when fixing the dimension.

[34] The probability that the $m$ samples do not span the full space but the next sample is nevertheless found to be linearly dependent is essentially zero.

(2023). However, for middle-sized problems it becomes less handy. A first reason is that the size of the moment matrix, for a fixed level of relaxation, scales polynomially in the size of $L$. Second, the number of SDP variables $m$ increases rapidly with any one of the parameters[35] $(X, Y, N, d)$. Third, one typically obtains better bounds on $\mathcal{Q}$ by separately considering different rank combinations for the projective measurements and then selecting the best bound, but the number of combinations increases quickly with $(N, Y, d)$.

Pauwels, Pironio, Woodhead, and Tavakoli (2022) developed an alternative SDP hierarchy that applies to bounding correlations obtained from systems that can be represented nearly as $d$ dimensional. This permits analysis of correlations of systems that approximate qubits to any desirable extent and, in the special case in which the approximation is exact, it provides bounds on $\mathcal{Q}$. The main idea is to supplement the set $L$ with an additional operator $V$ that is meant to emulate the $d$-dimensional identity projection. Therefore, it is given the properties $V^2 = V$ and $\mathrm{tr}(V) = d$. One can then proceed with building the moment matrix as described after Eq. (83). This method circumvents sampling and immediately takes POVMs into account. In addition, its computational requirements are constant in the dimension parameter. The main drawback is that the hierarchy does not converge to the quantum set, because it inherently relaxes dimension-restricted communication to communication that on average has dimension $d$; such systems have been studied independently in the context of entanglement using SDP relaxations (Gribling, de Laat, and Laurent, 2018). In some concrete instances this can lead to worse bounds on linear objective functions. An alternative method is based on transforming Bell scenarios into prepare-and-measure scenarios by considering the remote states prepared by Alice for Bob, ideally via a maximally entangled state (Mironowicz, Li, and Pawłowski, 2014). The dimension constraint is relaxed to a marginal constraint in the Bell scenario; one uses the NPA hierarchy under the extra constraint that one of Alice's outputs for each input has the marginal probability $1/d$. This, however, can be a crude relaxation, and it does not converge in general (Navascués, Feix *et al.*, 2015).

### 2. Applications

Bounds on $\mathcal{Q}$ obtained by means of SDP relaxations are broadly useful. An evident application is determining upper bounds on the magnitude of quantum advantages in useful communication tasks. An important class of examples is quantum random access codes in which Bob aims to randomly access a piece of information in a larger database held by Alice (Ambainis *et al.*, 2002). Direct application of the NV hierarchy has given tight upper bounds in low dimensions (Tavakoli *et al.*, 2015), and lower bounds have been obtained via SDPs in seesaw heuristics when the channel is noisy (da Silva and Marques, 2023). The former can be made vastly more efficient by exploiting symmetries inherent to the problem in order to reduce the complexity of the SDP; see Aguilar *et al.* (2018), Tavakoli, Rosset, and Renou (2019), and Pauwels, Pironio, Woodhead, and Tavakoli (2022). Such symmetry methods are further discussed in Sec. IX.F.

In other classes of communication tasks inspired by the high-dimensional Bell inequalities of Collins *et al.* (2002), SDP relaxations of $\mathcal{Q}$ can showcase dimensional thresholds, i.e., a critical dimension above which the optimal quantum strategy qualitatively changes (Tavakoli *et al.*, 2017; Martínez *et al.*, 2018). Moreover, suitably chosen linear objective functions over $\mathcal{Q}$ can be linked to the long-standing problem of determining the number of mutually unbiased bases in dimension 6. The hypothesis that no more than three such bases exist could, in principle and if true, be proven through a sufficiently precise SDP relaxation of $\mathcal{Q}$ based on a chaining of quantum random access codes (Aguilar *et al.*, 2018). There are also other SDP-based approaches to this problem, some that take the route of nonlocality (Colomer *et al.*, 2022; Gribling and Polak, 2024) and others that consider the existence of so-called Gröbner bases (Brierley and Weigert, 2010). Nevertheless, owing to the computational complexity, the problem remains open.

A complementary consideration is to, in a given dimension, bound the optimal quantum violation of facet inequalities for the polytope of classical prepare-and-measure correlations in a given input-output scenario (Mironowicz, Li, and Pawłowski, 2014; Navascués, Feix *et al.*, 2015). From another perspective such bounds can be seen as device-independent tests of quantum dimensions, which is a task where Alice and Bob aim to certify a lower bound on the dimension of their quantum channel without assuming any model for their preparation and measurement devices (Gallego *et al.*, 2010).

Applications also pertain to semi-device-independent quantum information processing, i.e., practically motivated protocols performed solely under the assumption that the communicated quantum state is of a limited dimension. Self-testing protocols based on the prepare-and-measure scenario have been developed in such settings. Drawing inspiration from the swap method for noisy self-testing discussed in Sec. V.B.1, one can employ the NV hierarchy to bound the average fidelity of Alice's qubit preparations with the ensemble used in the paradigmatic BB84 quantum key distribution protocol (Tavakoli *et al.*, 2018). This type of self-testing has also been extended to quantum instruments in three-partite communication scenarios featuring a sender, a transformer, and a receiver, both with (Miklin, Borkała, and Pawłowski, 2020) and without SDPs (Mohan, Tavakoli, and Brunner, 2019). Miklin, Borkała, and Pawłowski (2020) showed how the NV hierarchy can be extended to such prepare-transform-measure scenarios.

It is also possible to certify qualitative properties. For instance, by restricting sampling to real-valued Hilbert spaces, the NV hierarchy has been used to test complex-valued quantum operations in a given dimension (Navascués, Feix *et al.*, 2015). Furthermore, a particularly natural use for dimension-restricted systems is to certify nonprojective quantum measurements, i.e., measurements that cannot be simulated with standard projective measurements and classical randomness (D'Ariano, Presti, and Perinotti, 2005). The reason is that such measurements cannot be certified when

[35]The memory required in a single iteration of a typical primal-dual solver scales quadratically in both $m$ and $|\mathcal{S}|$ while the CPU time scales cubically in both $m$ and $|\mathcal{S}|$.

ancillary degrees of freedom are available due to the possibility of Neumark dilations (Nielsen and Chuang, 2010). The NV hierarchy has been used to certify nonprojective measurements of dimension 2 (Mironowicz and Pawłowski, 2019; Tavakoli, Smania *et al.*, 2020), dimension 4 (Martínez *et al.*, 2023), and up to dimension 6 (Tavakoli, Rosset, and Renou, 2019). All of these works rely on suitable witness constructions, but notably that is not essential for the SDP relaxation method to work. By analogous means, SDP methods have enabled certification of nonprojective measurements in Bell scenarios under the assumption of a limited entanglement dimension (Gómez *et al.*, 2016; Smania *et al.*, 2020). The SDP seesaw methods for probing $\mathcal{Q}$ (see Sec. II.B.1) can be used to reproduce the numerical estimates for the output rate of semi-device-independent quantum random number generators (Li *et al.*, 2011, 2012). Proper randomness bounds can be obtained via the NV hierarchy (Mironowicz *et al.*, 2016) or other relaxation methods (Mironowicz, Li, and Pawłowski, 2014).

However, many actual implementations of dimension-restricted quantum systems, such as spontaneous parametric down-conversion sources of single photons or weak coherent pulses, only nearly represent a proper dimension-restricted system. This can be leveraged to hack a semi-device-independent protocol. Using the SDP relaxation hierarchy of Pauwels, Pironio, Woodhead, and Tavakoli (2022), which was originally discussed in Sec. VI.B.1 only for standard dimension constraints, the small inaccuracies of such "almost qudit systems" can be taken into account when constructing quantum information protocols. The deviations from the dimension assumption can be quantified and incorporated as a linear inequality constraint on suitable elements of the corresponding moment matrix.

### 3. Entanglement-assisted communication

In Sec. VI.B the parties in the prepare-and-measure scenario communicated quantum states while sharing classical randomness. In this section we discuss the prepare-and-measure scenario when the parties additionally share an entangled state. The entanglement-assisted prepare-and-measure scenario is illustrated in Fig. 6.

Consider now a situation where the operations of Alice are not constrained to a binary choice. Instead, they may be arbitrary but the message she sends over the channel to Bob is classical and of dimension $d$. Such correlations are interesting because they can boost the performance of classical messages in various communication tasks (Buhrman *et al.*, 2010). The source emits an entangled state $\Phi$ of local dimension $D$. Given $x$, Alice transforms her share into a $d$-valued classical message. Hence, she applies a $d$-outcome POVM $\{N_{a|x}\}_{a=1}^{d}$ and, upon receiving the outcome $a$, she sends the classical state $|a\rangle\langle a|$ to Bob. Averaged over the probability $p(a|x)$, Bob's total state thus becomes $\sum_a |a\rangle\langle a| \otimes \mathrm{tr}_A(N_{a|x} \otimes \mathbb{1}\Phi^{AB})$, where the second factor is the unnormalized state of Bob's quantum system conditioned on Alice's outcome. In the most general situation, Bob can now first read the received message and then use the value $a$ to choose a POVM $\{M_{b|y,a}\}$ with which he measures his share of the entangled state. The correlations become

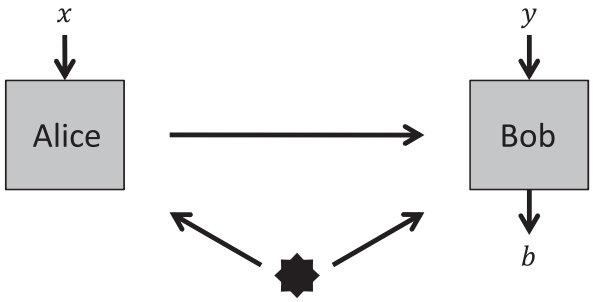


FIG. 6. A bipartite entanglement-assisted prepare-and-measure scenario. A source distributes an entangled state between Alice and Bob. Conditioned on her input $x$, Alice maps her system onto a message that is sent over the channel to Bob. Conditioned on $y$, Bob measures both the systems and obtains the outcome $b$.

$$p(b|x,y) = \sum_{a=1}^{d} \mathrm{tr}(N_{a|x} \otimes M_{b|y,a}\Phi^{AB}). \tag{85}$$

Equation (85) can be interpreted as marginalized Bell correlations with signaling from Alice to Bob and can also immediately be extended to nonidentity classical channels connecting the parties. In the most general case, the entanglement dimension $D$ is unrestricted, and Bob can adapt his measurement to the incoming message. One can then bound the set of quantum correlations from the exterior when the alphabet size for the inputs and outputs is fixed by a converging SDP relaxation hierarchy *à la* the NPA hierarchy (Tavakoli, Pauwels *et al.*, 2021), which was discussed in Sec. V.A. An alternative SDP relaxation hierarchy for this type of problem was presented by Berta, Fawzi, and Scholz (2016). At the first level this hierarchy is more constraining than the NPA approach due to the possibility of requiring all elements in the moment matrix to be non-negative (Sikora and Varvitsiotis, 2017). Furthermore, when the entanglement dimension is known, one can instead employ SDP relaxations in the spirit of dimension-restricted NPA, as discussed in Sec. V.B.2. Another interesting situation arises when one requires Bob not to adapt his measurement to the message, i.e., that a Bell test is performed first, and only afterward does classical communication take place. Correlations from such nonadaptive strategies can also be bounded by SDP relaxations (Pauwels, Pironio, Zambrini Cruzeiro, and Tavakoli, 2022), specifically by imposing the commutation relation $[M_{b|y,a}, M_{b'|y,a'}] = 0 \ \forall\, y, b, b', a, a'$ in the NPA-type matrix.

When the messages are $d$-dimensional quantum systems, it is well known from the dense coding protocol that stronger correlations are possible than are with classical $d$-dimensional messages (Bennett and Wiesner, 1992). For quantum messages Alice applies a quantum channel $\Lambda_x^{A\to C}$ that maps the incoming $D$-dimensional system to a $d$-dimensional message state that is sent to Bob. The message space is denoted as $C$. The total state held by Bob becomes $\tau_x^{CB} = \Lambda_x^{A\to C} \otimes \mathbb{1}_B[\Phi_{AB}]$, to which he applies a POVM $\{M_{b|y}^{CB}\}$. The resulting correlations become

$$p(b|x,y) = \mathrm{tr}(\tau_x^{CB} M_{b|y}^{CB}). \tag{86}$$

The only nontrivial constraint on the total state is no signaling, namely, $\tau_x^B = \tau^B$. In a given dimension this allows for alternating convex search methods to be used for exploring the correlation set. In particular, for a maximally entangled two-qubit state, the entanglement-assisted correlation set is equivalent to the correlations achievable in an unassisted prepare-and-measure scenario when Alice sends real-valued four-dimensional systems (Pauwels, Tavakoli *et al.*, 2022). This permits SDP outer bounds via the NV hierarchy restricted to real Hilbert spaces. More generally when $D$ is unknown and when any quantum channel is used between Alice and Bob, outer bounds can be obtained by a convergent hierarchy of SDPs (Tavakoli, Pauwels *et al.*, 2021). This hierarchy is based on an explicit Kraus operator parametrization of the quantum message space. It can be seen as a variation of the NPA hierarchy, and therefore its convergence properties are inherited. An important caveat is that this SDP hierarchy scales more rapidly than the adaptation of the NPA hierarchy to the classical case: the number of operators used to build the SDP matrix scales quadratically in $d$, as compared to linearly in the classical case. This quickly makes implementation demanding, although it may be possible to circumvent the issue via symmetrization methods; see Sec. IX.F. The alternative, unrelated SDP hierarchy of Tavakoli, Pauwels *et al.* (2021) becomes relevant here since it can be applied to efficiently obtain bounds. This hierarchy is based on the concept of informationally restricted correlations (Tavakoli, Zambrini Cruzeiro *et al.*, 2020) (see Sec. VI.C.1) and relies on moment matrices with a size independent of $d$. While this hierarchy does not converge to the quantum set in the entanglement-assisted scenario, it can give useful and even tight bounds in specific cases. Notably, when Alice and Bob are connected by an identity channel and entanglement is a free resource, the correlation set for quantum messages is identical to the correlation set for classical messages of twice as many bits (Vieira *et al.*, 2023). Consequently one can still use the SDP hierarchy for classical messages to address the scenario with quantum messages.

SDP methods for the entanglement-assisted prepare-and-measure scenario have found several applications. For instance, to fully capture the spirit of a device-independent test of classical or quantum dimensions, i.e., to place a lower bound on the dimension of a message without making assumptions about the internal working of the involved devices, one must allow for the possibility that the preparation and measurement devices share a potentially unrestricted amount of entanglement. Tavakoli, Pauwels *et al.* (2021) used the SDP relaxations to make known dimension witnesses (Gallego *et al.*, 2010; Ahrens *et al.*, 2014) robust to entangled devices. Furthermore, bounds on the quantum correlations have enabled a number of quantum resource inequalities. For instance, it has been shown that protocols in which Bob adapts his setting to a classical message are generally more powerful than the nonadaptive protcols, and that this distinction is crucial for using entanglement and one bit of classical communication to simulate correlations obtained from an unassisted qubit in the prepare-and-measure scenario, depending on whether it is measured with projective measurements or POVMs (Pauwels, Pironio, Zambrini Cruzeiro, and Tavakoli, 2022). For example, nonadaptive protocols based on Bell inequality violations followed by classical communication are known that improve the task of random access coding (Pawłowski and Żukowski, 2010; Tavakoli *et al.*, 2016). Using adaptive measurements and higher-dimensional entanglement can yield larger quantum advantages (Vaisakh *et al.*, 2021; Pauwels, Tavakoli *et al.*, 2022). Moreover, while it is well known that entanglement cannot increase the capacity of a classical channel, the same is not true in general when the capacity is considered in the nonasymptotic setting (Cubitt *et al.*, 2010). For some noisy classical channels, the advantage of entanglement can even be linked to the CHSH inequality (Prevedel *et al.*, 2011), and SDP relaxations showcase the notion that such strategies are in fact optimal (Berta, Fawzi, and Scholz, 2016).

#### 4. Teleportation

Entanglement-assisted communication can also be considered when the inputs themselves are quantum states, rather than classical symbols. The best known instance of such a scenario is teleportation, where a quantum state is sent by means of a shared maximally entangled state and classical communication (Bennett *et al.*, 1993). However, if the state $\rho_{AB}$ is not maximally entangled, then the teleportation channel will not flawlessly simulate the quantum identity channel. The traditional approach to quantifying the ability of an entangled state to perform teleportation is via the average fidelity of the target state and the teleported state. It is known that teleportation fidelity is a function of the maximally entangled fraction (Horodecki, Horodecki, and Horodecki, 1999),

$$F(\rho) = \max \langle \psi | \rho | \psi \rangle, \tag{87}$$

where $|\psi\rangle$ is any maximally entangled state. However, if one has prior knowledge of $\rho$, one could consider applying a $\rho$-dependent LOCC protocol to potentially enhance the teleportation fidelity. Verstraete and Verschelde (2003) showed that the optimal fidelity under such LOCC protocols, i.e., $\max_{\Lambda:\mathrm{LOCC}} F[\Lambda(\rho)]$, can be determined exactly when $\rho$ is a two-qubit state, and moreover that a single round of one-way communication is sufficient. To achieve this Verstraete and Verschelde first considered lower bounds by restricting to LOCC protocols of the form

$$\begin{aligned}\Lambda(\rho) = {} & (A \otimes B)\rho(A^\dagger \otimes B^\dagger) \\ & + \mathrm{tr}[(\mathbb{1} - A^\dagger A) \otimes (\mathbb{1} - B^\dagger B)\rho] |v\rangle\langle v| \otimes |w\rangle\langle w|,\end{aligned} \tag{88}$$

where $A$ and $B$ are Kraus operators with the corresponding outcome operators satisfying $0 \preccurlyeq A^\dagger A, B^\dagger B \preccurlyeq \mathbb{1}$, and $|v\rangle$ and $|w\rangle$ are any qubit states. Through a meticulous choice of $|v\rangle$ and $|w\rangle$ and a change of variables for $A$ and $B$, Verstraete and Verschelde (2003) showed that $\max_\Lambda F[\Lambda(\rho)]$, where the maximization is over LOCC channels of the form of Eq. (88), is equivalent to the optimization

$$\begin{aligned}\max_C \quad & \tfrac{1}{2} - \langle \phi^+ | (C \otimes \mathbb{1}) \rho^{T_B} (C^\dagger \otimes \mathbb{1}) | \phi^+ \rangle \\ \text{such that} \quad & C^\dagger C \preccurlyeq \mathbb{1}.\end{aligned} \tag{89}$$

To derive upper bounds they relax the optimization of $F$ from LOCC channels to PPT channels, i.e., channels whose Choi matrix is PPT, leading to the SDP relaxation

$$\begin{aligned} \max \quad & \mathrm{tr}[(\rho_{AB}^{T}\otimes|\phi^{+}\rangle\langle\phi^{+}|)C_{ABA'B'}] \\ \text{such that} \quad & \mathrm{tr}_{A'B'}(C_{ABA'B'})=\mathbb{1}_{AB}, \\ & C_{ABA'B'}^{T_{BB'}}\succeq 0, \\ & C_{ABA'B'}\succeq 0. \end{aligned} \tag{90}$$

Using the symmetries of $|\phi^{+}\rangle$ under unitary twirling, one can reduce this problem to the simpler SDP $\max[1/2-\mathrm{tr}(X\rho^{T_B})]$, with $X$ constrained to satisfy $0\preccurlyeq X\preccurlyeq\mathbb{1}$ and $-\mathbb{1}\preccurlyeq 2X^{T_B}\preccurlyeq\mathbb{1}$, which can be shown to be maximized by a rank-one operator $X=(A^{\dagger}\otimes\mathbb{1})|\phi^{+}\rangle\langle\phi^{+}|(A\otimes\mathbb{1})$ for some matrix $A$ satisfying $A^{\dagger}A\preccurlyeq\mathbb{1}$. However, for such rank-1 operators, this optimization is exactly the same as the lower bound in Eq. (89) and hence is achievable with a single-round LOCC protocol. Notably, this gives an example where the relaxation to PPT channels is tight.

A more general approach to teleportation was proposed by Cavalcanti, Skrzypczyk, and Šupić (2017). In this approach a verifier supplies a given number of states $\psi_x$ to Alice and asks her to teleport them to Bob. Alice applies a POVM $A_a^{VA}$ to $\psi_x$ and her share of the entangled state $\rho_{AB}$. The resulting unnormalized states of Bob are $\sigma_{a|\psi_x}=\mathrm{tr}_V[A_a^{VB}(\psi_x\otimes\mathbb{1}^B)]$, where $A_a^{VB}=\mathrm{tr}_A[(A_a^{VA}\otimes\mathbb{1}^B)(\mathbb{1}^V\otimes\rho_{AB})]$. However, if the state is separable, then this simplifies to separable operators $A_a^{VB}=\sum_\lambda p_\lambda A_{a|\lambda}^{V}\otimes\varphi_\lambda^{B}$, where $A_{a|\lambda}^{V}=\mathrm{tr}_A[A_a^{VA}(\mathbb{1}^V\otimes\rho_\lambda^A)]$. Note also that completeness of $\{A_a^{VA}\}_a$ implies that $\sum_a A_a^{VB}=\mathbb{1}^V\otimes\rho^B$. We can then quantify the amount of white noise that must be added to a given set $\{\sigma_{a|\psi_x}\}_{a,x}$ in order to model it classically,

$$\begin{aligned} \min \quad & t \\ \text{such that} \quad & \tfrac{\sigma_{a|\psi_x}}{1+t}+\tfrac{t}{1+t}\tfrac{\mathbb{1}^B}{dN}=\mathrm{tr}_V[A_a^{VB}(\psi_x\otimes\mathbb{1}^B)], \\ & \sum_a A_a^{VB}=\mathbb{1}^V\otimes\left(\tfrac{\rho^B}{1+t}+\tfrac{t}{1+t}\tfrac{\mathbb{1}^B}{d}\right), \\ & A_a^{VB}\in\mathrm{SEP}\quad\forall\, a, \end{aligned} \tag{91}$$

where $N$ is the number of outcomes for Alice and $d$ is the dimension of system $B$. If the solution has $t>0$, there is no classical teleportation model. By relaxing the set of separable operators to a semidefinite constraint, for example, PPT, this becomes an SDP criterion for classicality of teleportation. A resource theory for this type of teleportation, where SDPs again are relevant, was developed by Lipka-Bartosik and Skrzypczyk (2020). Šupić, Skrzypczyk, and Cavalcanti (2019) showed how one can estimate entanglement measures using an SDP analysis of the data generated in teleportation experiments.

Ideal teleportation can be seen as simulating a noiseless quantum channel using entanglement and classical communication. Holdsworth, Singh, and Wilde (2023) developed SDP methods for bounding various forms of simulation errors for how well the teleportation channel approximates the noiseless quantum channel. A key component for this analysis is to use SDP relaxations of the set of one-way LOCC channels, i.e., relaxations of procedures where Alice measures locally and sends her outcome to Bob, who then performs a local channel. To this end, as in Fig. 5, we view the actions of Alice and Bob as a single bipartite channel $\Lambda_{AB\to A'B'}$. If this bipartite channel preserves PPT states, which is an SDP condition on the level of the Choi matrix associated with the channel (Rains, 1999, 2001), it is also a one-way LOCC channel. Alternatively, it is possible to relax one-way LOCC channels by imposing that $\Lambda_{AB\to A'B'}$ is $k$ extendible[36] (Kaur *et al.*, 2019, 2021). This concept is analogous to the constraints appearing in the DPS hierarchy. It means that one can associate another channel $\mathcal{N}_{AB_1\ldots B_k\to A'B'_1\ldots B'_k}$, which is invariant under permutations of Bob's inputs and outputs, and such that if all but one of Bob's systems are discarded, $\Lambda_{AB\to A'B'}$ is recovered. These two relaxations can be combined into a single SDP relaxation of one-way LOCC channels. The former type of relaxation has also been used to address simulation errors when both Alice and Bob want to teleport states to each other (Siddiqui and Wilde, 2023).

A related task is known as port-based teleportation (Ishizaka and Hiroshima, 2008). In it Bob does not need to perform a correcting quantum channel upon receiving Alice's outcome. To achieve this Alice and Bob share $n$ copies of the maximally entangled state and Alice jointly measures her input state and all of her $n$ shares and sends the outcome to Bob. The outcome tells Bob in which share he can find the teleported state. Optimization of protocols of this type has been cast as an SDP (Studziński *et al.*, 2017; Mozrzymas *et al.*, 2018).

### C. Distinguishability problems

#### 1. Distinguishability constraints for quantum communication

It is often interesting to benchmark quantum communication not by its dimension but by another property that is either physically or conceptually well motivated. This pertains partly to understanding the conditions under which quantum correlations go beyond classical limits and partly to building useful protocols for semi-device-independent quantum information processing, where deductions are made under weak and reasonable physical assumptions. Many different frameworks have been proposed, all based on the general idea of limiting the distinguishability of the states sent from Alice to Bob. What they have in common is that SDPs are typically crucial for their analysis. Here we survey the main idea of each of these frameworks from an SDP perspective. Some of the cryptographic applications of these SDP methods are surveyed in Sec. VII.C.

A natural experimental setting is that Alice knows which state $|\psi_x\rangle$ she is trying to prepare for Bob. However, since she does not have flawless control of her lab, she ends up preparing another state $\rho_x$ that is close but not identical to $\psi_x$. The accuracy of her preparation can be quantified by the fidelity $F_x=\langle\psi_x|\rho_x|\psi_x\rangle$. Alice can either measure this quantity in her lab or estimate it from an error model and name $\epsilon_x$

[36] An alternative definition of $k$-extendible channels and their relevance to SDP was given by Berta *et al.* (2022).

the deviation in the fidelity from the ideal unit result. The communication between Alice and Bob is then based only on the assumption that Alice can control her state preparation up to an accuracy $\epsilon_x$ (Tavakoli, 2021). The key observation for characterizing such correlations, based on quantitative distrust, is that Uhlmann's theorem (Uhlmann, 1976) allows one to substitute a mixed state $\rho$ for a purification $|\phi\rangle$ such that the fidelity is preserved. Since $N$ pure states span at most an $N$-dimensional space, the correlations can be thought of as arising in a dimension-restricted space to which the NV hierarchy applies, as described in Sec. VI.B.1. One can therefore use the ideas of the NV hierarchy, but now extending the operator list to also include all of the target states $\{\psi_x\}$. The fidelity constraints can then be imposed as additional linear inequality constraints $F_x = \Gamma(\rho_x, \psi_x) \geq 1 - \epsilon_x$ on the moment matrix. This was used by Tavakoli (2021) to certify collections of nonclassical measurements as a function of $\epsilon_x$.

An alternative approach limits the distinguishability, not with respect to a target state but rather with respect to the collection of states prepared by Alice. Wang *et al.* (2019) considered a set of $Z$ pure bipartite states $\{|\psi_z\rangle\}$ that were distributed between Alice and Bob. The Gram matrix of the states is known, i.e., all pairs of overlaps $\lambda_{ij} = \langle\psi_i|\psi_j\rangle$ are fixed. The correlations then become $p(a, b|x, y, z) = \langle\psi_z|A_{a|x} \otimes B_{b|y}|\psi_z\rangle$. To bound the correlation set via an SDP hierarchy, consider a set of monomials $\mathcal{S}$ consisting of products of the global projective measurements $A_{a|x} \otimes \mathbb{1}$ and $\mathbb{1} \otimes B_{b|y}$. Define the $|\mathcal{S}|Z \times |\mathcal{S}|Z$ moment matrix

$$\Gamma(u, v) = \sum_{i,j=1}^{Z} G^{ij} \otimes |i\rangle\langle j|, \tag{92}$$

where for each pair $(i, j)$ we define the matrix $G^{ij}(u, v) = \langle\psi_i|u^\dagger v|\psi_j\rangle$ for $u, v \in \mathcal{S}$. The standard properties of projective quantum measurements and the known Gram matrix imply constraints on $\Gamma$. In particular, one recovers the probabilities as $G^{zz}(A_{a|x}, B_{b|y}) = p(a, b|x, y, z)$ and the overlaps as $\sum_a G^{ij}(A_{a|x}, \mathbb{1}) = \lambda_{ij}$. Combined with $\Gamma \succeq 0$, this gives an SDP relaxation that, in the limit of a large relaxation level, converges to the quantum set of correlations. In the special case of only two pure states, the Gram matrix trivializes to a single nontrivial entry, and the correlation set can then be characterized completely with a single SDP (Bohr Brask *et al.*, 2017). This two-state case was used by Shi *et al.* (2019) to certify a genuine three-outcome measurement. Furthermore, SDP relaxations based on the Gram matrix have been used to compute upper bounds on quantum state discrimination problems for optical modes with arbitrary commutation relations limited by a fixed average photon number (Primaatmaja, Ho, and Scarani, 2021).

A conceptually motivated framework for the prepare-and-measure scenario is to generalize dimension restrictions to information restrictions (Tavakoli, Zambrini Cruzeiro *et al.*, 2020); see also Chaturvedi and Saha (2020). The main idea is to consider the cost of creating correlations in terms of the amount of knowledge that Alice must make available about her input random variable $X$. The classical information carried by Alice's ensemble $\mathcal{E} = \{p_x, \rho_x\}$ is defined as the difference between the min-entropy before and after Bob has received the communication, $I(\mathcal{E}) = H_{\min}(X) - H_{\min}(X|B)$. Here the first term is determined by the largest probability in Alice's prior $H_{\min}(X) = -\log \max_x p_x$. The conditional min-entropy has an elegant operational interpretation in terms of minimal error quantum state discrimination (König, Renner, and Schaffner, 2009): if $P_g$ is the largest average probability of state discrimination of the ensemble $\mathcal{E}$, then $H_{\min}(X|B) = -\log P_g$. The state discrimination task can be written as the following SDP:

$$\begin{aligned} P_g = \max_{\{M_x\}} \quad & \sum_x p_x \mathrm{tr}(\rho_x M_x) \\ \text{such that} \quad & \sum_x M_x = \mathbb{1}, \\ & M_x \succeq 0. \end{aligned} \tag{93}$$

Notably, other natural communication tasks closely related to quantum state discrimination can also be expressed as SDPs. Examples of this are the quantum guesswork, where one aims to minimize the number of guesses needed to learn $x$ (Hanson *et al.*, 2022), discrimination of sets of labels (Chaturvedi, Pawłowski, and Saha, 2021), maximum confidence state discrimination (Lee *et al.*, 2022), and quantum state exclusion, where one aims to rule out the possibility that Alice selected a subset of her input alphabet (Bandyopadhyay *et al.*, 2014; Russo and Sikora, 2023). The central question then becomes to determine the relationship between the correlations $p(b|x, y)$ and the information $I(\mathcal{E})$ (or the guessing probability $P_g$). Tavakoli, Zambrini Cruzeiro *et al.* (2022) developed convex programming methods for analyzing informationally restricted classical and quantum correlations. The former are fully characterized by an LP, and the latter can be bounded by an SDP hierarchy. The key step for constructing the hierarchy is to introduce an auxiliary operator $\sigma$ when building the moment matrix. This auxiliary operator comes from the SDP dual to Eq. (93),

$$\begin{aligned} P_g = \min_{\sigma} \quad & \mathrm{tr}(\sigma) \\ \text{such that} \quad & \sigma \succeq p_x \rho_x \quad \forall\, x. \end{aligned} \tag{94}$$

Note that strong duality holds. Therefore, the properties that $\mathrm{tr}(\sigma) \leq P_g$ and that $\sigma \succeq p_x \rho_x$ are built into the moment matrix. The former is simply the linear constraint $\Gamma(\sigma, \mathbb{1}) \leq P_g$. The latter are semidefinite constraints that can be imposed through localizing matrices; see Sec. III.B. Moreover, for informationally restricted correlations one cannot restrict to pure states without loss of generality. Taking this into account also requires localizing matrices for imposing the condition that $\rho_x$ be a valid state, namely, $\rho_x - \rho_x^2 \succeq 0$. Beyond their own domain the SDP tools for informationally restricted quantum correlations can be applied to problems in quantum contextuality (Tavakoli, Zambrini Cruzeiro *et al.*, 2021) and entanglement-assisted correlations with classical or quantum messages (Tavakoli, Pauwels *et al.*, 2021). For such ends, it has the property that the complexity of the SDP is independent of the amount of information considered.

However, the convergence of the hierarchy to the quantum set is presently unknown.

A practical approach to quantum communication in the prepare-and-measure scenario is based on limiting the energy in the message from Alice to Bob. van Himbeeck *et al.* (2017) proposed limiting the nonvacuum component of a weak coherent pulse through an upper bound of the form $\langle \mathbb{1} - |0\rangle\langle 0| \rangle_{\rho_x} \leq \omega_x$. When Alice had two preparations, it was shown that the set of energy-restricted quantum correlations could be mapped into a qubit problem, which in turn permitted a complete characterization in terms of a single SDP (van Himbeeck and Pironio, 2019).

### 2. Discrimination tasks

SDP techniques are useful for determining the relevance of quantum resources in various discrimination tasks. An important class of examples is quantum state estimation problems, which can with some generality be phrased as a source generating a pure state $\phi_x$ with probability $p(x)$. The state is then encoded in another state $\varphi_x$ and given to a user who is tasked with performing a measurement $\{M_a\}$. Upon observing the outcome, he outputs a quantum state $\psi_a$ as his estimate for $\phi_x$. The average fidelity of the estimation becomes

$$F = \sum_{a,x} p(x)\mathrm{tr}(\varphi_x M_a)\mathrm{tr}(\phi_x \psi_a) = \mathrm{tr}(\rho_{AB}\Lambda_{AB}). \quad (95)$$

In the second inequality of Eq. (95), we have defined $\rho_{AB} = \sum_x p(x)\varphi_x \otimes \phi_x$ and $\Lambda_{AB} = \sum_a M_a \otimes \psi_a$ because this formulation permits us to connect the task of bounding $F$ with a separability problem (Navascués, 2008). The key observation is that $\rho_{AB}$ is known, whereas $\Lambda_{AB}$ is unknown but separable and subject to the constraint $\mathrm{tr}_B(\Lambda_{AB}) = \mathbb{1}$. In fact, any separable operation with this property corresponds to a valid state estimation strategy. Hence, one can apply PPT-symmetric extensions to the system $A$ as given by the DPS hierarchy (see Sec. IV.A) and obtain a sequence of SDP bounds on $F$ that, in the limit of a large relaxation level, converges to $F$. A relevant variation of this problem is when $\varphi_x$ itself is a bipartite state and the measurement $\{M_a\}$ is restricted to admit implementation by LOCC. Since it is difficult to mathematically characterize LOCC measurements, an often viable approach is to relax these to separable measurements. As shown by Navascués (2008), this too can be connected to the DPS hierarchy. To take the bipartite feature into account, Eq. (95) is modified by replacing $\rho_{AB}$ and $\Lambda_{AB}$ with the tripartite operators $\rho_{ABC} = \sum_x p(x)\varphi_x^{AB} \otimes \phi_x^C$ and $\Lambda_{ABC} = \sum_a M_a^{AB} \otimes \psi_a^C$. Since $\{M_a^{AB}\}$ itself is separable, one must impose the conditions that $\Lambda_{ABC}$ is fully tripartite separable and that $\mathrm{tr}_C(\Lambda_{ABC}) = \mathbb{1}$. This makes the problem amenable to the multipartite variant of the DPS hierarchy of SDPs.

Discrimination of sets of entangled states using only measurements compatible with LOCC is a rich topic, and SDPs have played a role in its recent development. The set of PPT measurements has frequently been used to bound the set of LOCC measurements in such tasks (Cosentino, 2013). This relaxation can often be useful. For instance, it is known that any set of $k > d$ orthogonal maximally entangled states on $\mathbb{C}^d \otimes \mathbb{C}^d$ cannot be perfectly distinguished by LOCC measurements (Ghosh *et al.*, 2004), and the same is also true for PPT measurements (Yu, Duan, and Ying, 2012). Using duality theory for PPT measurements, it was shown that for any $d = 2^t$ (with integers $t \geq 2$), the average success probability of discriminating $k$ orthogonal maximally entangled states is bounded by $7d/(8k)$ (Cosentino and Russo, 2014). This proves that there are cases with $k = d$ and even cases with $k < d$ for which LOCC discrimination cannot be exact; see also Yu, Duan, and Ying (2012). When similar SDP techniques were used, the case of $k = d$ was then shown for any $d \geq 4$ (Li, Wang *et al.*, 2015). A variation of this discrimination problem is to allow for some auxiliary entanglement to be consumed in the discrimination protocol. Using duality theory, Bandyopadhyay *et al.* (2015) showed that the optimal average success probability of discriminating four equiprobable Bell states via LOCC is $(1/2)(1 + \sqrt{1-\epsilon^2})$, where the auxiliary entangled state is $\sqrt{(1+\epsilon)/2}|00\rangle + \sqrt{(1-\epsilon)/2}|11\rangle$. Note that a perfect discrimination is possible only with a maximally entangled state. The latter is true also for discriminating three Bell states. In contrast, using PPT relaxations, the entanglement cost for discriminating three Bell states corresponds to only $\epsilon = 1/3$ (Yu, Duan, and Ying, 2014). Another variation of these problems is to consider having many copies of the entangled state. It is well known that having many copies of orthogonal pure states permits perfect LOCC discrimination, but that the same does not need to hold for orthogonal mixed states (Bandyopadhyay, 2011). SDP techniques have shown that this behavior for mixed states also persists under PPT measurements (Yu, Duan, and Ying, 2014; Li, Wang, and Duan, 2017).

Frequently a quantum resource can be completely characterized in terms of its ability to yield an advantage in a certain discrimination task, which thereby lends it an operational interpretation. We now discuss how SDP techniques make these connections possible. Consider quantum steering, i.e., the inability of a state assemblage $\varrho_{a|x} = \mathrm{tr}_A(A_{a|x} \otimes \mathbb{1}\rho_{AB})$ to admit a local hidden state model, which was discussed in Sec. II.B.1; see Eq. (7). Piani and Watrous (2015) showed that a necessary and sufficient condition for $\rho_{AB}$ to be steerable is that it yields an advantage over all non-entanglement-based strategies in the task of subchannel discrimination when measurements are limited to be implementable by one-way LOCC. Specifically, an instrument is defined as $\mathcal{I} = \{\Lambda_x\}$, where each $\Lambda_x$ is a completely positive and trace nonincreasing map (a subchannel). The instrument is normalized to the channel $\Lambda = \sum_x \Lambda_x$. The discrimination task is to prepare a suitable state $\sigma$, apply the instrument $\mathcal{I}$, and then perform a measurement $\{M_a\}$ with the aim of determining the specific subchannel, i.e., of outputting $a = x$. The best protocol involves an optimization over both $\sigma$ and $\{M_a\}$, leading one to define the "no entanglement" performance as $p_{\mathrm{NE}} = \max_{\sigma,M} \sum_x \mathrm{tr}(\Lambda_x[\sigma]M_x)$. This can now be compared to the best protocol using the entangled state $\rho_{AB}$, where the instrument is applied on system $B$. Let the measurements be adaptive product measurements, namely, $M_a = \sum_b A_{a|b} \otimes B_b$ for some local POVMs $\{A_{a|b}\}$ and $\{B_b\}$. One then finds that for every steerable state there exists $\mathcal{I}$ such that the success probability $p_E = \max_M \sum_x \mathrm{tr}\big[(\mathbb{1}\otimes\Lambda_x)[\rho_{AB}]M_x\big]$ exceeds

$p_{\mathrm{NE}}$. To arrive at this one studies the quantity known as the steering robustness $R(\rho_{AB})$. It is defined as a supremum over a corresponding robustness quantity defined for assemblages $R(\{\varrho_{a|x}\})$. The latter quantity is the smallest $t \geq 0$ for which the assemblage can be decomposed as $\varrho_{a|x} = (1+t)\varrho^{\mathrm{US}}_{a|x} - t\tau_{a|x}$ for some unsteerable assemblage $\{\varrho^{\mathrm{US}}_{a|x}\}$ and some arbitrary assemblage $\{\tau_{a|x}\}$. Thus, it is in a sense the smallest amount weight for a steerable assemblage necessary to recover $\{\varrho_{a|x}\}$. It can be computed as the SDP

$$\begin{aligned} 1+R(\{\varrho_{a|x}\}) = \min \quad & \sum_{\lambda} \sigma_{\lambda} \\ \text{such that} \quad & \sum_{\lambda} p(a|x,\lambda)\sigma_{\lambda} \succeq \varrho_{a|x} \quad \forall\, a,x, \\ & \sigma_{\lambda} \succeq 0 \qquad\qquad\quad \forall\, \lambda. \end{aligned} \tag{96}$$

From Eq. (96) one can show that $p_E/p_{\mathrm{NE}} \leq 1 + R(\{\varrho_{a|x}\}) \leq 1 + R(\rho_{AB})$, where the last inequality follows by definition. Piani and Watrous (2015) showed that analysis of the dual SDP allows one to strengthen this to $p_E/p_{\mathrm{NE}} = 1 + R(\rho_{AB})$. Hence, for any steerable state there are local measurements that give rise to a steerable assemblage that thus exhibits $R(\{\varrho_{a|x}\}) > 0$. This implies that there is some instrument for which the entanglement-assisted subchannel discrimination (with one-way adaptive local measurements) exceeds the entanglement-unassisted limit, i.e., $p_E > p_{\mathrm{NE}}$. We note that while the steering robustness of an assemblage is useful for understanding subchannel discrimination, there are many ways to quantify steerability via SDPs; see Skrzypczyk, Navascués, and Cavalcanti (2014), Cavalcanti and Skrzypczyk (2016), and the review by Cavalcanti and Skrzypczyk (2017).

In general quantum resources associated with convex sets (e.g. entanglement, steering and joint measurability) can be systematically associated with resource quantifiers in the spirit of Eq. (96). We already saw an example of this in the discussion around Eq. (5) for PPT states (which is a convex set). When the quantum resource does not admit an SDP characterization, the quantifiers typically also do not admit an SDP representation. Nevertheless, they can often be formulated within the more general framework of conic programming. While conic programs generally lack the important feature of being efficiently computable, they can still admit a duality theory that parallels the one discussed for SDPs. For instance, a conic programming approach to separable measurements was given by Bandyopadhyay *et al.* (2015), and constructions of robustness-type measures for arbitrary convex measurement sets was developed by Takagi *et al.* (2019) and Uola *et al.* (2019). Thus, regardless of the set admitting an SDP or a more general conic characterization, a nonzero distance (in terms of a suitable robustness measure) from such a set can often be interpreted in terms of an operational advantage in a tailored discrimination task.

Consider a quantum state discrimination task based on a predetermined set of states $\rho_{a|x}$. Alice selects $x$ from a prior $p(x)$, draws $a$ from some prior $p(a|x)$, and then sends both $x$ and $\rho_{a|x}$ to Bob. Bob's task is to learn the value $a$. There are two types of protocols permitted. In either, Bob has a predefined set of incompatible measurmements $\{M_{b|y}\}$. Based on the knowledge of $x$, he stochastically selects which measurement to perform using some distribution $p(y|x,\mu)$ with prior $p(\mu)$. The measurement outcome is then used, together with the knowledge of $(x,\mu)$, to select the final guess for $a$. In contrast, an alternative protocol is for Alice to perform in each round a single measurement on $\rho_{a|x}$ and then use $y$ to postprocess the outcome into the final guess for $a$. Carmeli, Heinosaari, and Toigo (2018) showed that $\{M_{b|y}\}$ must be incompatible in order for the first type of strategy to outperform the latter. Using the knowledge of robustness-type resource quantifiers, one can show that measurement incompatibility is in fact both necessary and sufficient (Carmeli, Heinosaari, and Toigo, 2019; Skrzypczyk, Šupić, and Cavalcanti, 2019; Uola *et al.*, 2019). That is, for every set of incompatible measurements, there is a tailored choice of a state discrimination task, of the aforementioned form, where they can outperform any protocol-based compatible measurements. The relevant quantifier of the incompatibility resource is the incompatibility robustness discussed in Sec. V.B.4, which is computable via SDP. Notably, such ideas can also be extended to discrimination tasks for witnessing the incompatibility of channels (Mori, 2020). A related but different example is when one considers measurements from a resource theory perspective. A device that maps quantum states to classical outcomes is a measurement, but not all such devices require one to actually interact with the quantum state. A trivial example is a device that bins the state and then flips a coin and outputs the result. Skrzypczyk and Linden (2019) identified such trivial measurements as POVMs of the form $\{p(a)\mathbb{1}\}_a$ for some probability distribution $\{p(a)\}$, and a robustness measure was formulated for quantifying the extent to which a given measurement deviates from such a trivial realization. This measure is computable via SDP, and, by examining its dual, one can formulate a standard quantum state discrimination problem where the degree of advantage in the nontrivial measurements corresponds exactly to their robustness.

We also mention some examples of the previous ideas being applied to convex sets that are fully characterized not by SDPs but by more general conic constraints. A prime example is the set of bipartite separable states. The previously discussed task of subchannel discrimination assumed measurements that are compatible with one-way LOCC. If one instead permits generic bipartite measurements, it can be shown that every entangled state (i.e., the unsteerable ones as well) yields an advantage in the task (Piani and Watrous, 2009). This can also be extended to high-dimensional entanglement, as quantified by the Schmidt number of $\rho_{AB}$. Bae, Chruściński, and Piani (2019) showed that every state with a Schmidt number larger than $k$ can outperform any state with a Schmidt number of at most $k$ in subchannel discrimination. Another example is witnessing the advantage of nonprojective measurements with respect to protocols based on projective measurements. The latter is a convex set but cannot be characterized as an SDP due to the projectivity condition. Nevertheless, one can always find an advantage in a tailored state discrimination task (Uola *et al.*, 2019). The same also applies to sets of quantum states, as compared to the restricted set of quantum states that can be collectively diagonalized by a single unitary (Designolle *et al.*,

2021). These ideas have also been merged with the previous discussion of LOCC discrimination of entanglement in order to link advantages to local robustness measures (Sen, Halder, and Sen, 2024).

## VII. RANDOMNESS AND QUANTUM KEY DISTRIBUTION

Quantum cryptography offers a means to execute cryptographic tasks with information-theoretic security, with randomness generation and quantum key distribution (QKD) being the most well-studied primitives in this domain. In this section we describe how SDP hierarchies can be used to quantify randomness and compute rates of QKD protocols; see Gisin *et al.* (2002), Scarani *et al.* (2009), Pirandola *et al.* (2020), Xu *et al.* (2020), and Portmann and Renner (2022) for more in-depth reviews on the topic.

A QKD protocol consists of two parties Alice and Bob who want to establish a shared random string that is unknown to any potential adversary. To do this they execute a procedure that generates a classical-classical-quantum system $\rho_{ABE}$, where $A$ and $B$ are classical systems held by Alice and Bob, respectively, and $E$ is a quantum system held by a potential adversary. From this system they can then try to postprocess the classical systems $A$ and $B$ to produce random strings $K_A = K_B$ that are not correlated with $E$. To assess the security and performance of such a protocol, one needs to compute (or at least lower bound) its asymptotic rate,[37] i.e., the number of secret key bits generated per round of the protocol as the number of rounds tends to infinity. For example, for QKD with one-way error correction against an adversary who applies the same attack each round on the protocol independently of the other rounds [an independent and identically distributed (IID) adversary], the asymptotic rate is given by the Devetak-Winter bound (Devetak and Winter, 2005)

$$\min_{\rho_{ABE}\in\mathcal{S}} H(A|E) - H(A|B), \tag{97}$$

where $H(X|Y) \coloneqq H(XY) - H(Y)$, with $H(X) \coloneqq -\mathrm{tr}(\rho_X \log_2 \rho_X)$ the von Neumann entropy and the minimization over the set $\mathcal{S}$ of all classical-classical-quantum states $\rho_{ABE}$ that are compatible with the protocol. Therefore, the exact set $\mathcal{S}$ depends on the protocol used and the statistics observed. The asymmetry in the Devetak-Winter bound comes from the restriction to protocols with one-way error correction; i.e., all the error correction is sent by Alice to Bob. It is possible to interpret the second term $H(A|B)$ as approximately the rate of bits that Alice must send to Bob for him to successfully correct his raw key to be equal to hers.

Note that, as $A$ and $B$ are observed by Alice and Bob, one can estimate $H(A|B)$ directly from the statistics of the protocol. Thus, the main task remaining is to bound from below

$$\min_{\rho_{ABE}\in\mathcal{S}} H(A|E). \tag{98}$$

There are two main difficulties to overcome in order to compute bounds on Eq. (98). First, the objective function is a nonlinear function of $\rho_{ABE}$ and, second, one needs to characterize the set $\mathcal{S}$ of possible states $\rho_{ABE}$ output by the protocol when $E$ is a system unknown to Alice and Bob. The latter depends significantly on the security model of the protocol, so in the following we consider the different approaches suited to the different security models. It is further possible to consider different adversaries. For example, one could make a restriction to classical adversaries, which forces $E$ to be a classical system, and hence Eve cannot be entangled with the initial systems of Alice and Bob.

### A. Device-independent approach

In the device-independent security model, which was pioneered by the ideas of Ekert (1991) and Mayers and Yao (1998), Alice and Bob each have an untrusted device that they use to generate nonlocal correlations; see Fig. 2. It is assumed without loss of generality that the devices produce their outcomes given their inputs by measuring some projective measurements $\{A_{a|x}\}_{a,x}$ and $\{B_{b|y}\}_{b,y}$ on a bipartite state $\rho_{Q_AQ_B}$ [see Eq. (3)], where the subindex $Q$ indicates that the system is quantum, in contrast to the classical systems $A$ and $B$ that hold the measurement outcomes of Alice and Bob. In this security model the source $\rho_{Q_AQ_B}$ is not trusted, and hence there may be an adversarial party holding a system $E$ that is potentially entangled with the systems $Q_A$ and $Q_B$. In a device-independent protocol, Alice and Bob verify that the correlations $p(a,b|x,y)$ generated by their devices satisfy some linear constraints

$$\sum_{a,b,x,y} r_{abxy,i}\, p(a,b|x,y) \geq \omega_i \quad \forall\, i, \tag{99}$$

where $r_{abxy,i}, \omega_i \in \mathbb{R}$ are specified by the protocol. They can verify that their devices achieve some sufficiently high average CHSH violation. Thus, the set of states that are required to optimize over in Eq. (98) are exactly the post-measurement states whose statistics are compatible with the corresponding version of Eq. (99) imposed by the protocol. Using the NPA hierarchy, one can in principle relax the existence of such quantum systems satisfying Eq. (99) to a hierarchy of SDPs, as detailed in Sec. V.A. What then remains is to convert the objective function $H(A|E)$ into something that can be expressed within the framework of noncommutative polynomial optimization.

#### 1. Bounding the min-entropy

For a classical-quantum state, $\rho_{XY} = \sum_x |x\rangle\langle x| \otimes \rho_Y(x)$, the conditional min-entropy of $X$ given $Y$ is defined as $H_{\min}(X|Y) \coloneqq -\log_2 P_g(X|Y)$, where

$$P_g(X|Y) \coloneqq \max_{\{M_x\}_x} \sum_x \mathrm{tr}[M_x \rho_Y(x)], \tag{100}$$

and the maximization is over all POVMs $\{M_x\}_x$ on system $Y$. Operationally the quantity $P_g(X|Y)$ corresponds to the maximum probability with which someone who has access to

[37] It is also possible to compute nonasymptotic rates from the asymptotic rates even against non-IID adversaries (Dupuis, Fawzi, and Renner, 2020).

system $Y$ can guess the value of system $X$, and hence $P_g$ is referred to as the guessing probability (König, Renner, and Schaffner, 2009). This operational interpretation also implies that the min-entropy rates for a classical adversary coincide with those of a quantum adversary. Eve effectively creates a classical system upon measuring, which implies the existence of a classical strategy achieving the same min-entropy bound.

Using the fact that $H \geq H_{\min}$, one can immediately get lower bounds on rates by lower bounding the min-entropy or, equivalently, upper bounding the guessing probability. In particular, when Alice inputs $X = x$, we have

$$P_g(A|E) = \max_{\{M_a\}} \sum_a \mathrm{tr}[(A_{a|x} \otimes \mathbb{1} \otimes M_a)\rho_{Q_A Q_B E}], \quad (101)$$

where $\{M_a\}$ is now some POVM given to the adversary (which can be assumed to be projective) (Masanes, Pironio, and Acín, 2011). When the tools of noncommutative polynomial optimization are applied, the corresponding rate optimization can be relaxed to a hierarchy of SDPs whose moment matrices are generated by the monomials $\{\mathbb{1}\} \cup \{A_{a|x}\} \cup \{B_{b|y}\} \cup \{M_a\}$, and the $k$th level relaxation is given by

$$\begin{aligned} \max \quad & \sum_a \Gamma^k(A_{a|x}, M_a) \\ \text{such that} \quad & \sum_{a,b,x,y} r_{abxy,i}\Gamma^k(A_{a|x}, B_{b|y}) \geq \omega_i \quad \forall\, i, \\ & \Gamma^k \succeq 0, \end{aligned} \quad (102)$$

where as usual we have not explicitly specified all the constraints present in Eq. (102), such as those coming from projectivity, commutativity, orthogonality, and normalization. Taking $-\log_2$ of any solution to Eq. (102) will therefore allow the rates of device-independent QKD or device-independent randomness generation protocols to be lower bounded.

By tracing out the $E$ system, one can increase the efficiency of these relaxations in terms of the dimension of the SDP (Bancal, Sheridan, and Scarani, 2014; Nieto-Silleras, Pironio, and Silman, 2014) as Eve's operators are removed from the relaxation, and subsequently the size of the moment matrix is reduced. In particular, one can view Eve's measurement, upon obtaining the outcome $c$, as preparing the subnormalized state $\rho_{Q_A Q_B}(c) = \mathrm{tr}_E[(\mathbb{1}_{Q_A Q_B} \otimes M_c)\rho_{Q_A Q_B E}]$ for Alice and Bob, which satisfies a normalization condition $\sum_c \rho_{Q_A Q_B}(c) = \rho_{Q_A Q_B}$. Thus, it is possible to create a relaxation for each of the states $\rho_{Q_A Q_B}(c)$, leading to several smaller moment matrix blocks instead of one large moment matrix for the state $\rho_{Q_A Q_B}$. In particular, one can instead write the $k$th level relaxation as

$$\begin{aligned} \max \quad & \sum_a \Gamma^k_a(A_{a|x}, \mathbb{1}) \\ \text{such that} \quad & \sum_{a,b,x,y,c} r_{abxy,i}\Gamma^k_c(A_{a|x}, B_{b|y}) \geq \omega_i \quad \forall\, i, \\ & \sum_c \Gamma^k_c(\mathbb{1}, \mathbb{1}) = 1, \\ & \Gamma^k_c \succeq 0 \qquad\qquad\qquad\qquad \forall\, c, \end{aligned} \quad (103)$$

where we have again omitted many implicit constraints.

The SDP bounds on $H_{\min}$ have been used extensively to analyze the device-independent randomness generated from different Bell inequalities in the presence of noise (Mironowicz and Pawłowski, 2013; Bancal and Scarani, 2014; Law *et al.*, 2014), from noninequality settings (Li, Pawłowski *et al.*, 2015a), in the presence of leakage (Silman, Pironio, and Massar, 2013; Tan, 2023), from postselected events (Thinh *et al.*, 2016; Xu *et al.*, 2022), from PPT states (Vértesi and Brunner, 2014), and from partially entangled states (Gómez *et al.*, 2019). The efficiency of the SDPs allows them to be used to help optimize the experimental design to maximize randomness (Máttar *et al.*, 2015), and through the dual it is possible to extract functions on which the experimental parameters can be optimized (Assad, Thearle, and Lam, 2016). The dual also provides a function on the space of correlations that lower bounds the certifiable device-independent randomness, which can then be used to create full security proofs of the corresponding protocols (Nieto-Silleras *et al.*, 2018; Brown, Ragy, and Colbeck, 2020). Employing these SDP relaxations, one can also verify that a four-outcome POVM can be utilized to produce two bits of device-independent randomness using a maximally entangled qubit pair (Acín *et al.*, 2016; Gómez *et al.*, 2016), and similar advantages from nonprojective measurements also appear in systems with higher dimensions (Tavakoli, Farkas *et al.*, 2021). The technique can also be applied to more exotic correlation scenarios like sequential measurements (Bowles, Baccari, and Salavrakos, 2020) to show robust generation of more randomness than would be possible with just a single projective measurement or within the instrumental causal structure (Agresti *et al.*, 2020). It was also used together with analytical investigations to demonstrate that a sequence of nonprojective measurements can be used to generate unbounded amounts of randomness from a single maximally entangled qubit pair (Curchod *et al.*, 2017).

### 2. Bounding the von Neumann entropy

The min-entropy approach provides a simple method to lower bound the rates of protocols. However, secure asymptotic and nonasymptotic rates are often expressed in terms of the von Neumann entropy (Arnon-Friedman *et al.*, 2018), which in general is larger than the min-entropy. Thus, to find tighter lower bounds on the rate of a protocol, it is necessary to find a way to lower bound the von Neumann entropy more accurately.

Tan *et al.* (2021) used duality relations of entropies to remove Eve from the problem, following a similar approach taken by Coles, Metodiev, and Lütkenhaus (2016) to view the measurements of Alice and Bob through the lens of an isometry. After rephrasing the problem in terms of only Alice and Bob, they provided a lower-bounding ansatz, which, after applying a Golden-Thompson inequality (Sutter, Berta, and Tomamichel, 2017), they expressed as a noncommutative polynomial optimization problem that can in turn be relaxed to a hierarchy of SDPs.

Brown, Fawzi, and Fawzi (2021) introduced a sequence of conditional Rényi entropies[38] that are all lower bounds on

[38]Rényi entropies are usually single-parameter families of entropic quantities. For an in-depth overview see Tomamichel (2015).

$H(A|E)$. Each of these entropies is defined in terms of a solution to an SDP that emerges from the SDP representability of the matrix geometric mean (Fawzi and Saunderson, 2017). Like the min-entropy, these Rényi entropies can be each used to give a hierarchy of SDPs that lower bound the rates. Gonzales-Ureta, Predojević, and Cabello (2021) used the method to derive improved device-independent QKD rates in settings with more inputs and outputs.

While the two aforementioned methods improve over the min-entropy, it is not clear that either can compute tight lower bounds on the von Neumann entropy. Brown, Fawzi, and Fawzi (2024) introduced a sequence of variational forms that converge to the von Neumann entropy from below. Let $m \in \mathbb{N}$, and let $t_1, \ldots, t_m$ and $w_1, \ldots, w_m$ be the nodes and weights of an $m$-point Gauss-Radau quadrature rule[39] on $[0,1]$ with $t_m = 1$ (Golub, 1973). For each $m \in \mathbb{N}$ the following noncommutative polynomial optimization problem is a lower bound on the rate $\inf H(A|E)$,

$$\begin{aligned} \min \quad & c_m + \textstyle\sum_{i=1}^{m-1} \frac{w_i}{t_i \log 2} \sum_a \mathrm{tr}\big(\rho_{Q_A Q_B E}\{A_{a|x}[Z_{a,i} + Z_{a,i}^\dagger + (1-t_i) Z_{a,i}^\dagger Z_{a,i}] + t_i Z_{a,i} Z_{a,i}^\dagger\}\big) \\ \text{such that} \quad & \sum_{a,b,x,y} r_{abxy,i} \mathrm{tr}(\rho_{Q_A Q_B E} A_{a|x} B_{b|y}) \geq \omega_i, \\ & Z_{a,i}^\dagger Z_{a,i} \preccurlyeq \alpha_i^2 \mathbb{1}, \\ & [A_{a|x}, B_{b|y}] = [A_{a|x}, Z_{c,i}] = [B_{b|y}, Z_{c,i}] = 0, \end{aligned} \tag{104}$$

where $\alpha_i = (3/2)\max\{t_i^{-1}, (1-t_i)^{-1}\}$, $c_m = (\log 2)^{-1} \times \sum_{i=1}^{m-1}(w_i/t_i)$, and the operators generating the noncommutative polynomial optimization are $\{A_{a|x}\} \cup \{B_{b|y}\} \cup \{Z_{c,i}, Z_{c,i}^\dagger\}$. This can then be relaxed to an SDP using the techniques detailed in Sec. III.B. In particular, the core of the relaxation consists of a moment matrix generated by the monomials $\{\mathbb{1}\} \cup \{A_{a|x}\} \cup \{B_{b|y}\} \cup \{Z_{c,i}, Z_{c,i}^\dagger\}$. Note that the $Z_{c,i}$ operators are not Hermitian, and hence their adjoint must also be included in the generating set.

The construction leads to a double hierarchy, namely, a hierarchy of variational bounds indexed by $m$ and, for each of these bounds, an SDP relaxation hierarchy. For applications given by Brown, Fawzi, and Fawzi (2024), a value of $m = 8$ or 12 was typically used alongside various tricks to speed up the computations. This method has been shown to recover the known tight bounds on rate curves. It has been used to compute randomness generation rates in mistrustful settings (Metger *et al.*, 2022), i.e., when Alice does not trust Bob, as well as for assessing the optimal randomness certifiable in the binary input and binary output scenarios (Wooltorton, Brown, and Colbeck, 2022).

When Alice and Bob have only binary inputs and outputs, the analysis of the rate can be reduced to the analysis of qubit systems through the use of Jordan's lemma (Masanes, 2006). For certain Bell inequalities it is then possible to solve the entropy optimization analytically (Pironio *et al.*, 2009). Masini, Pironio, and Woodhead (2022) introduced a hybrid analytical-numerical approach for binary settings. They showed that, after reducing to qubit systems, it is possible to use further symmetries and properties of entropies to express the rate of the problem as an analytical function of some unknown correlators. These correlators can then be bounded by a commutative polynomial optimization of just a few variables. This can then be relaxed to a hierarchy of SDPs using the Lasserre hierarchy; see Sec. III.A. Their advantage over the previously discussed techniques is that the numerical optimizations are significantly smaller (and hence faster). Furthermore, it can achieve tight bounds in certain cases.

A similar hybrid approach was taken by Schwonnek *et al.* (2021), where they analyzed key rates achievable in binary input and binary output settings when the key was extracted from different input settings. After reducing to qubit systems, they reformulated the problem as a triplet of nested optimizations, with the innermost optimization an SDP arising from the SDP formulation of the trace norm,

$$\begin{aligned} \|K\|_1 = \min \quad & \tfrac{1}{2}\mathrm{tr}(X+Y) \\ \text{such that} \quad & \begin{pmatrix} X & K \\ K^\dagger & Y \end{pmatrix} \succeq 0, \end{aligned} \tag{105}$$

where $K$ is any square matrix (Watrous, 2018).

### 3. Beyond entropy optimizations

Thus far we have focused on randomness generation and QKD with one-way error correction, the rates of which both require solving a minimization of some entropy. When one moves beyond these protocols, the relevant figure of merit will often change. Nevertheless, SDP relaxation techniques remain readily applicable to these new settings.

Two-way error correction in QKD, i.e., when both Alice and Bob can communicate in the error correction step of the protocol, is known as advantage distillation. Tan, Lim, and Renner (2020) showed that a sufficient condition for secret key generation in this binary-outcome protocol is

$$\min F(\rho_{E|00}, \rho_{E|11}) > \sqrt{\frac{\epsilon}{1-\epsilon}}, \tag{106}$$

[39] A Gaussian quadrature rule approximates an integral $\int_a^b f(x)dx$ by a finite sum $\sum_i w_i f(t_i)$, where $w_i$ are referred to as weights and $t_i$ are called nodes. See Davis and Rabinowitz (1984) for further details.

where $F(\rho,\sigma) \coloneqq \|\sqrt{\rho}\sqrt{\sigma}\|_1$ is the fidelity, $\epsilon$ is the probability that Alice and Bob's outcomes disagree on the key-generating inputs $x$ and $y$, i.e., $\epsilon \coloneqq \sum_{a\neq b} p(a,b|x,y)$, and $\rho_{E|ab} = [1/p(ab|xy)]\mathrm{tr}_{Q_AQ_B}[(M_{a|x}\otimes N_{b|y}\otimes \mathbb{1})\rho_{Q_AQ_BE}]$ is the marginal state of Eve conditioned on Alice receiving outcome $a$ and Bob receiving outcome $b$. Various approaches to compute the minimization of the fidelity have been proposed. Tan, Lim, and Renner (2020) found that the fidelity was lower bounded by a guessing probability, resulting in an optimization that could be tackled using techniques introduced by Thinh *et al.* (2016). Hahn and Tan (2022) showed that one can apply a fidelity-preserving measurement to the quantum states to reduce the objective function to just a function of probabilities and then, using techniques similar to those introduced by van Himbeeck and Pironio (2019), arbitrarily tight bounds on the fidelity can be directly computed using noncommutative polynomial optimization. A stronger sufficient condition based on the Chernoff divergence $Q(\rho,\sigma) \coloneqq \min_{0<s<1}\mathrm{tr}(\rho^s\sigma^{1-s})$ was introduced by Stasiuk, Lütkenhaus, and Tan (2022), and indirect lower bounds were analyzed using a guessing probability lower bound and the resulting SDP relaxations, in a manner similar to that of Tan, Lim, and Renner (2020).

In contrast to QKD, wherein Alice and Bob trust each other, mistrustful cryptography aims to execute a cryptographic task between two agents who do not trust each other. The relevant figures of merit for these protocols are then the probability that each agent can cheat. Bit commitment is such a protocol in which Alice commits a bit to Bob. After commitment Alice should not be able to modify the bit, and Bob should be able to learn the bit only when Alice chooses to reveal it. Aharon *et al.* (2016) introduced a device-independent bit-commitment protocol based on the CHSH game, and it was shown that the probability that Alice can cheat could be relaxed to a noncommutative polynomial optimization problem similar to a guessing probability problem. Similar SDP relaxations were also derived for the cheating probabilities of Alice and Bob in an XOR oblivious transfer protocol based on the magic square game (Kundu, Sikora, and Tan, 2022).

In both randomness generation and QKD, regardless of the security model, various classical postprocessing of the data is performed. In particular, a procedure known as randomness extraction is necessary to transform the measurement outputs of the devices into $\epsilon$-approximate secret uniform randomness. Berta, Fawzi, and Scholz (2015) showed that the condition for a procedure to be a valid randomness extractor can be recast as a quadratic program. This quadratic program can then be relaxed to an SDP, giving a certificate for a procedure to be a secure randomness extractor.

### B. Device-dependent approach

The opposite of the device-independent approach is having a full characterization of the honest parties' devices involved in a protocol. In this device-dependent scenario, Alice and Bob measure some fixed, known POVMs $\{A_{a|x}\}_{a,x}$ and $\{B_{b|y}\}_{b,y}$ on a bipartite state $\rho_{Q_AQ_B}$. As before the source is not trusted, and thus no assumptions on $\rho_{Q_AQ_B}$ are made, except that it must be compatible with the statistics measured by Alice and Bob. In particular, an adversarial party holds a quantum system $E$ that is potentially entangled with the systems $Q_A$ and $Q_B$, with the global state denoted by $\rho_{Q_AQ_BE}$. The condition that is compatible with the measured statistics is then expressed as

$$\mathrm{tr}[(W_i\otimes \mathbb{1}_E)\rho_{Q_AQ_BE}] = \omega_i \quad \forall\, i, \tag{107}$$

where $W_i = \sum_{a,b,x,y} c_{abxy,i} A_{a|x}\otimes B_{b|y}$ is specified by the protocol and $\omega_i$ is given by the measured statistics. For example, one can choose $\{A_{a|x}\}_{a,x}$ and $\{B_{b|y}\}_{b,y}$ to be mutually unbiased bases and $W_i$ to compute the probability that Alice and Bob get equal results when measuring in the same bases (Sheridan and Scarani, 2010). Equation (107) is a simple linear constraint compatible with SDP, so, in order to compute the key rate, one simply needs to convert the objective function $H(A|E)$ from Eq. (97) into an expression that can be optimized via SDPs.

#### 1. Bounding the min-entropy

As in the device-independent case, it is possible to lower bound the von Neumann entropy by the min-entropy and compute the latter from the guessing probability given by Eq. (101). The equation can be linearized in the optimization variables by absorbing the $\{M_c\}_c$ into $\rho_{Q_AQ_BE}$, that is, defining

$$\rho_{Q_AQ_B}(c) = \mathrm{tr}_E[(\mathbb{1}\otimes\mathbb{1}\otimes M_c)\rho_{Q_AQ_BE}] \tag{108}$$

so that $\rho_{Q_AQ_B} = \sum_c \rho_{Q_AQ_B}(c)$. Computing the guessing probability is done with the following SDP:

$$\begin{aligned} \max_{\{\rho_{Q_AQ_B}(a)\}} \quad & \sum_a \mathrm{tr}[(A_{a|x}\otimes\mathbb{1})\rho_{Q_AQ_B}(a)] \\ \text{such that} \quad & \sum_a \mathrm{tr}[W_i\rho_{Q_AQ_B}(a)] = \omega_i \qquad \forall\, i, \\ & \sum_a \mathrm{tr}[\rho_{Q_AQ_B}(a)] = 1, \\ & \rho_{Q_AQ_B}(a) \succeq 0 \qquad \forall\, a. \end{aligned} \tag{109}$$

Equation (109) was used by Doda *et al.* (2021) to demonstrate improved noise tolerances for QKD using high-dimensional systems. The min-entropy, however, is a loose lower bound on the von Neumann entropy, so the key rates computed in this way are unnecessarily pessimistic. The main advantage of this technique is simplicity.

#### 2. Bounding the von Neumann entropy

The variational forms converging to the von Neumann entropy introduced by Brown, Fawzi, and Fawzi (2024) can also be applied to computing the key rate in the device-dependent case (Araújo *et al.*, 2023). Having trusted measurement devices drastically simplifies the problem: for a given matrix element on Alice and Bob's side, one builds an NPA hierarchy for Eve together with the quantum state, resulting in a block matrix SDP, as done by Navascués, de la Torre, and Vértesi (2014). This NPA-type hierarchy converges at the first level because there are no commutation relations to enforce, and thus for fixed $m$ one has a single SDP.

As shown by Coles, Metodiev, and Lütkenhaus (2016), the $H(A|E)$ term in the key rate can be rewritten as $D(\mathcal{Z}[\rho_{Q_AQ_B}]||\mathcal{Z}[\mathcal{G}(\rho_{Q_AQ_B})])$, where $D(\rho\|\sigma) \coloneqq \mathrm{tr}[\rho\log_2(\rho)] - \mathrm{tr}[\rho\log_2(\sigma)]$ is the relative entropy and $\mathcal{Z}$ and $\mathcal{G}$ are quantum channels. This rewriting achieves two things: it removes Eve from the problem, and it results in an objective function that is convex in the variables $\rho_{Q_AQ_B}$. Thus, the key-rate calculation becomes a convex optimization problem. Winick, Lütkenhaus, and Coles (2018) showed that a Frank-Wolfe-type algorithm (Frank and Wolfe, 1956) can be used to solve the problem. They also provided a method to convert feasible points of the convex optimization problem into rigorous lower bounds on the key rate: when the objective is linearized at a given feasible point $\rho_{Q_AQ_B}$, the convex optimization problem becomes an SDP, and a guaranteed lower bound can be obtained using the weak duality of the SDPs. Dedicated interior-point algorithms to solve the optimization problem have also been developed (Hu *et al.*, 2022), with improved stability and convergence rates over the known Frank-Wolfe-type methods. The convex optimization can also be done using the semidefinite approximations of the matrix logarithm developed by Fawzi, Saunderson, and Parrilo (2019), who gave an alternate method that uses SDPs (Bunandar *et al.*, 2020; Hu *et al.*, 2022).

More recently effective conic methods have been developed to optimize over nonsymmetric cones (Skajaa and Ye, 2015; Papp and Yıldız, 2017; Coey, Kapelevich, and Vielma, 2023). Together with the modeling of the relative entropy as a nonsymmetric cone (Fawzi and Saunderson, 2023), this has made it possible to solve the key-rate problem directly without relying on SDP relaxations or dedicated algorithms (He, Saunderson, and Fawzi, 2024; Lorente *et al.*, 2024). Such methods offer a dramatic improvement of performance over previous techniques.

### C. Semi-device-independent approach

Semi-device-independent (SDI) protocols offer a trade-off between the high security of device independence and the ease of implementation of device-dependent protocols. Ideally one looks to add one or more easily verifiable assumptions that enable the resulting protocol to be implemented in a significantly simpler manner. Often these protocols reduce to a prepare-and-measure scenario (see Fig. 3) similar to those discussed in Sec. VI, wherein Alice randomly prepares one of the states $\{\rho_x\}_x$ and sends it to a measurement device (Bob) that performs one of several measurements to generate the data that become the source of randomness or the secret key. Different assumptions can then be placed on the source device and the measurement device to generate different SDI protocols. Note that if one has an SDP relaxation of the set of correlations achievable within this setting, then one can often optimize entropies over these sets to bound the rates of randomness generation protocols. For several assumptions these SDP relaxations of the correlation sets were already discussed in Sec. VI.

The first work to introduce SDI cryptography considered a QKD scheme in the prepare-and-measure setting that assumes that the quantum states prepared by Alice and sent to Bob are qubits (Pawłowski and Brunner, 2011). By restricting the dimension of the Hilbert space, the set of possible prepare-and-measure correlations $p(b|x,y)$ is also restricted. Note that, akin to the situation in Bell nonlocality, there are qubit correlations that cannot be realized by classical systems of dimension 2. By witnessing these correlations under the qubit assumption, Alice and Bob can verify that their systems must be acting in a nonclassical manner and, crucially, nondeterministically. Using analytical results concerning dimension witnesses and random access coding, Pawłowski and Brunner (2011) demonstrated that secret keys can be extracted from certain correlations, although their analysis was limited to an ideal protocol. Later SDI protocols for randomness generation based on dimension bounds were introduced (Li *et al.*, 2011, 2012; Mironowicz *et al.*, 2016). Mironowicz *et al.* (2016) used the dimension-restricted correlations hierarchy of Navascués and Vértesi (2015) (see also Sec. VI.B.1) to compute a lower bound on the min-entropy that can be certified from devices that achieve some minimal success probability for a quantum random access code. The issue with an upper bound on the dimension of a quantum system is that it is difficult to physically justify, hence researchers then looked for protocols that rely on other assumptions that are easier to verify.

van Himbeeck and Pironio (2019) analyzed SDI protocols for randomness generation under assumptions of bounded average and maximal energy of the quantum states sent from Alice to Bob, and a full security proof against classical adversaries is given. The resulting correlation set has an SDP representation (see Sec. VI.C.1), which van Himbeeck and Pironio used to analyze the randomness generated against a classical adversary. To achieve this they had to deal with the nonlinearity of $\sum_x p(x)h(E_x)$, where $p(x)$ is the input distribution, $h(x) \coloneqq -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy, and $E_x$ is an observed quantity in the protocol. As $h$ is concave, one can define a sequence of piecewise linear lower bounds on $h$ that approximates $h$ arbitrarily well in the limit. This led van Himbeeck and Pironio (2019) to a hierarchy of SDP bounds on the rates based on this approximation.

SDI randomness amplification protocols, i.e., SDI randomness generation with a partially trusted seed, can also be performed under the assumption of energy bounds (Senno and Acín, 2021). A similar approach was taken by Jones *et al.* (2022), who showed that the formalism developed by van Himbeeck and Pironio (2019) can also be applied to assumptions on the spacetime symmetries of the protocol, which further can be treated independently of quantum theory.

If the source is limited to the preparation of two states, then the energy bounds give a physical justification for a minimal overlap $|\langle\psi_x|\psi_y\rangle| > 0$ in the states prepared by the source. A number of researchers have also analyzed SDI randomness generation directly under the assumption of a minimal overlap between the states $\{|\psi_x\rangle\}_x$ sent by the source to the measurement device. Bohr Brask *et al.* (2017) noted that any attempt to unambiguously discriminate between $|\psi_0\rangle$ and $|\psi_1\rangle$ must contain some randomness in whether or not the discrimination is conclusive. An SDP based on $H_{\min}$ is formulated to bound the randomness generated with respect to an adversary who may share classical correlations with the measurement device. This SDP can also be generalized to more inputs and outputs to achieve higher randomness generation rates (Tebyanian *et al.*, 2021). Employing

time-bin encoding and single-photon detection, Roch i Carceller *et al.* (2024) used SDP to certify more than one bit of randomenss per round in this framework. Roch i Carceller *et al.* (2022) used the minimal overlap assumption to show that quantum devices can generate more randomness than noncontextual devices that obey an analogous assumption, and an SDP to compute the randomness for noncontextual devices was also given. Note that, since these works assume the preparation of pure states, they are able to restrict the analysis to the finite-dimensional subspace spanned by those states. As a result, the computation of the rates can be directly written as a single SDP.

An SDI randomness generation protocol under which all overlaps $\langle\psi_x|\psi_y\rangle$ are known was given by Ioannou *et al.* (2022). They also analyzed the randomness generated against a quantum adversary who has access to the quantum channel between the source and the measurement device and can use this to create entanglement between themselves and the measured states. By adapting the SDP relaxation method of Wang *et al.* (2019) [see Eq. (92)], one can then compute a hierarchy of min-entropy bounds against the adversary. A similar SDI randomness generation protocol was given by Wang, Primaatmaja *et al.* (2023) in which the source was fully characterized but the quantum channel and Bob's measurement device was untrusted. Using also the techniques of Wang *et al.* (2019) an SDP relaxation of min-entropy bounds was given and a full security analysis was provided.

An alternative bounded overlap condition was given by Tavakoli (2021), who assumed that the source prepares states that are close to some fixed set of target states; see Sec. VI.C.1. The randomness generated by the measurement device with respect to an adversary who shares classical correlations with both the source and the measurement device is then analyzed using the min-entropy and SDP relaxations of the underlying correlation set of the scenario. An alternative to the various overlap assumptions was given by Tavakoli, Zambrini Cruzeiro *et al.* (2022), who assumed a bound on the information transmitted through the prepare-and-measure channel; see also Sec. VI.C.1. The certifiable randomness was evaluated using the min-entropy for various bounds on the transmitted information, and comparisons to the dimension-bounded protocols were also given.

The setting of measurement-device-independent (MDI) QKD offers stronger security than device-dependent QKD as well as a longer distance (Lo, Curty, and Qi, 2012). Winick, Lütkenhaus, and Coles (2018) and Hu *et al.* (2022) showed that the methods developed for device-dependent QKD can also be used to compute key rates of MDI-QKD protocols and variants like twin-field QKD (Lucamarini *et al.*, 2018). Primaatmaja *et al.* (2019) derived an SDP method to bound the phase error rate of a variety of protocols that can in turn be used to compute their rates via the Shor-Preskill formula (Shor and Preskill, 2000). Other works in the setting of uncharacterized measurement devices have investigated randomness generated in steering scenarios (Passaro *et al.*, 2015) and with trusted quantum inputs (Šupić, Skrzypczyk, and Cavalcanti, 2017).

## VIII. CORRELATIONS IN NETWORKS

A line of research in quantum correlations takes the study of entanglement-based correlations beyond the traditional Bell-type scenarios and into the domain of networks. Networks are composed of a number of parties that are connected to each other through multiple independent sources that each emit physical systems. A party can then perform measurements on the shares received from several different sources; see Fig. 7. Not only is the framework of networks the appropriate one to analyze long-distance entanglement-based and communication scenarios, but it has also provided new insights into the fundamentals of quantum theory (Renou *et al.*, 2021; Abiuso *et al.*, 2022).

Characterizing classical, quantum, or no-signaling correlations in networks is a major theoretical challenge. The origin of the difficulty is that the presence of multiple independent sources renders the correlation sets nonconvex, and therefore one cannot rely on more standard tools from convex optimization theory. For this reason, relaxation hierarchies have become a useful way to approach correlations in networks. In this section we provide introductions to these methods and their applications; see Tavakoli, Pozas-Kerstjens *et al.* (2022) for in-depth discussions of these and other aspects of correlations in networks.

### A. Inflation methods

Inflation is a general framework for characterizing correlations in causal structures in general and networks in

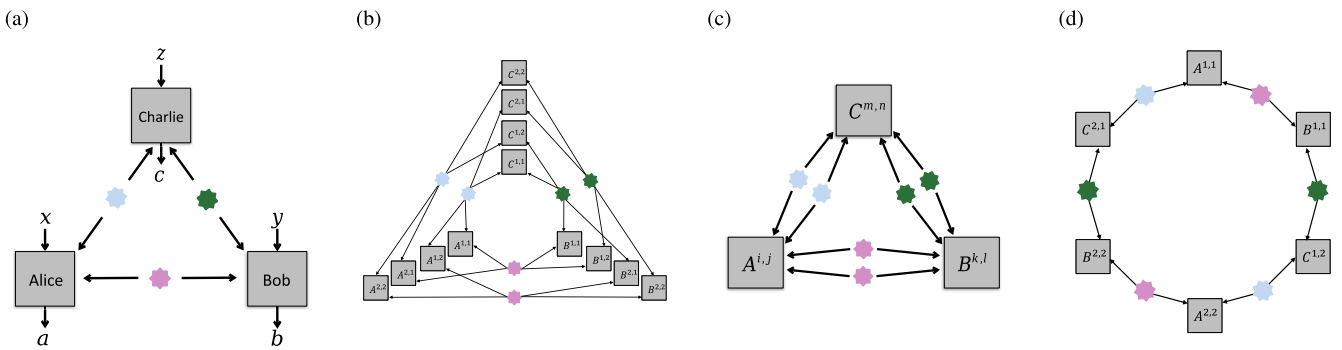


FIG. 7. (a) The triangle network and the second levels of its (b) classical, (c) quantum, and (d) NSI inflation hierarchies. Note that the inputs and outputs were omitted in (b)–(d) for clarity. The superindices denote the copies of the sources that each party acts upon.

particular via SDP or LP relaxations. The main idea in inflation is to substitute the original network and its nonconvex constraints for a larger network, created by copies of the sources and parties of the original network, in which the constraints are relaxed to linear symmetry constraints. An illustration is shown in Fig. 7, where the problem of characterizing the probability distributions $p(a,b,c|x,y,z)$ compatible with the triangle scenario in Fig. 7(a) is relaxed by the characterization of distributions $p_{\text{inf}}(\{a^{i,j}\},\{b^{k,l}\},\{c^{m,n}\}|\{x^{i,j}\},\{y^{k,l}\},\{z^{m,n}\})$ that are compatible with one of the inflations in Figs. 7(b)–7(d), where the superindices denote the copies of the sources that are used to produce a particular value. Thus, one trades a simple but technically challenging problem for one that can be solved using standard methods in a more complicated network. The construction of the inflated network strongly depends on the physical model underlying the network. The three main models of interest are (i) classical models corresponding to associating each source with an independent local variable, (ii) quantum models in which each source is associated with an independent entangled quantum state, and (iii) models constrained only by no-signaling and independence (NSI) assumptions, where each source is independently associated with a general nonlocal resource required only to respect the no-signaling principle. The key difference in the construction of the inflations stems from the fact that the case with local variables allows free copying of information, whereas the quantum and no-signaling cases do not. We now discuss the basics of the three types of inflation.

### 1. Classical inflation

In classical networks, the sources can be described by random variables and the measurement devices can without loss of generality be seen as deterministic functions of the classical variables received by a particular party. Since classical information can be copied, an inflated network may feature copies not only of the sources and measurement devices but also of the concrete values of the local variables distributed by the sources (Wolfe, Spekkens, and Fritz, 2019).

An example of classical inflation is presented in Fig. 7(b) for the triangle-shaped network of Fig. 7(a), where the parties' outputs are labeled $a$, $b$, and $c$, respectively. Since the sources and measurement devices are copies of those in the original network, the correlations $p_{\text{inf}}$ seen in the inflation must satisfy the symmetries

$$\begin{aligned} &p_{\text{inf}}(\{a^{i,j}\},\{b^{k,l}\},\{c^{m,n}\}) \\ &\quad = p_{\text{inf}}(\{a^{\pi(i),\pi'(j)}\},\{b^{\pi'(k),\pi''(l)}\},\{c^{\pi''(m),\pi(n)}\}) \end{aligned} \tag{110}$$

for independent permutations $\pi$, $\pi'$, and $\pi''$ of the different copies of the sources. Moreover, marginals of $p_{\text{inf}}$ over parties that reproduce parts of the original network can be directly associated with the probability distribution $p_{\text{orig}}$ in the original network,

$$p_{\text{inf}}(\Pi_i\{a^{i,i},b^{i,i},c^{i,i}\}) = \Pi_i p_{\text{orig}}(a^{i,i},b^{i,i},c^{i,i}). \tag{111}$$

One such constraint in the inflation in Fig. 7(b) is

$$\begin{aligned} &p_{\text{inf}}(a^{1,1},a^{2,2},b^{1,1},b^{2,2},c^{1,1},c^{2,2}) \\ &\quad = p_{\text{orig}}(a^{1,1},b^{1,1},c^{1,1})p_{\text{orig}}(a^{2,2},b^{2,2},c^{2,2}). \end{aligned} \tag{112}$$

Note that the constraints in Eq. (111) can be imposed only in feasibility problems, where $p_{\text{orig}}$ is given and thus the right-hand side is a number. When one optimizes over the set of distributions compatible with a given inflation, $p_{\text{orig}}$ are also variables, and thus the linear constraints that can be imposed are simply

$$p_{\text{inf}}(a^{i,i},b^{i,i},c^{i,i}) = p_{\text{orig}}(a^{i,i},b^{i,i},c^{i,i}) \;\forall\; i. \tag{113}$$

A third type of constraint is relevant for feasibility problems (Pozas-Kerstjens, 2019; Pozas-Kerstjens, Gisin, and Renou, 2023). These are constraints on marginals that factorize, and some of the factors can be associated with $p_{\text{orig}}$. An example illustrated in the inflation of Fig. 7(b) is

$$\begin{aligned} &p_{\text{inf}}(a^{1,1},a^{2,2},b^{1,1},b^{1,2},c^{1,1},c^{2,1}) \\ &\quad = p_{\text{orig}}(a^{2,2})p_{\text{inf}}(a^{1,1},b^{1,1},b^{1,2},c^{1,1},c^{2,1}). \end{aligned} \tag{114}$$

Since all of the discussed constraints are linear for a given $p_{\text{orig}}$, the task of finding a probability distribution $p_{\text{inf}}$ compatible with the same constraints can be cast as an LP. The inflation technique (Wolfe, Spekkens, and Fritz, 2019) provides a complete solution to the characterization of classical network correlations. This was shown by Navascués and Wolfe (2020), who identified a sequence of inflation tests that, in the limit of large inflation, converges to the set of local correlations associated with the original network. This sequence is constructed such that the $n$th test features $n$ copies of each of the sources of the original network. The inflation illustrated in Fig. 7(b) corresponds to the second step in this sequence of converging tests for the case of the triangle network. Although it guarantees convergence in the asymptotic limit, one must bear in mind that the complexity of the hierarchy of LPs (measured by the number of elements in the probability distribution $p_{\text{inf}}$) grows in $n$ as $N^{n^r}$, where $N$ is the number of outcomes for a party and $r$ is the amount of sources that send states to a party.

Inflation has become a standard tool in the analysis of network nonlocality, and it has often been employed in the depicted triangle network. For a specific inflation, Wolfe, Spekkens, and Fritz (2019) completely characterized the set of compatible no-input binary-outcome correlations. Fraser and Wolfe (2018) found that this characterization did not admit quantum violations and gave other Bell-like inequalities for the triangle scenario, with four outcomes per party, that do admit noise-robust quantum violations. Classical inflation has also been used to show that a shared random bit cannot be realized in the triangle network with classical sources (Wolfe, Spekkens, and Fritz, 2019), and to find certificates of more genuine quantum nonlocality in the four-output triangle scenario by studying the dual of an inflation LP (Pozas-Kerstjens, Gisin, and Renou, 2023). Inflation methods have also enabled examples of nonlocality that use a smaller number of outputs (Boreiri *et al.*, 2023; Pozas-Kerstjens *et al.*, 2023). Moreover, outside the domain of networks, it has been used to determine

equivalences between causal structures that produce the same correlations (Ansanelli, 2022).

### 2. Quantum inflation

In quantum networks the sources distribute entangled quantum systems and the parties perform quantum measurements on the subsystems at their disposal. In contrast to the classical case, quantum theory must respect the no-cloning theorem (Park, 1970; Dieks, 1982; Wootters and Zurek, 1982), which prevents valid inflations from copying the individual subsystems produced in the quantum sources and distributing them between additional parties. This limits the inflations allowed for a network. If we again use the triangle scenario of Fig. 7(a), Born's rule gives the quantum correlations

$$p_Q^{\triangle}(a,b,c|x,y,z) = \mathrm{tr}(A_{a|x}\otimes B_{b|y}\otimes C_{c|z}\cdot \rho_{AB}\otimes\rho_{BC}\otimes\rho_{CA}), \tag{115}$$

which is analogous to Eq. (3). Quantum inflation (Wolfe *et al.*, 2021) relaxes the fact that the global state in the scenario $\rho_{AB}\otimes\rho_{BC}\otimes\rho_{CA}$ has a tensor-product form. It does so via a gedanken experiment similar to that of Sec. VIII.A.1: if states and operators satisfying Eq. (115) exist, then one can have multiple copies of them, and thus there exist at least one state $\rho$ and operators $A_{a|x}^{i_{CA},i_{AB}}$, $B_{b|y}^{i_{AB},i_{BC}}$, and $C_{c|z}^{i_{BC},i_{CA}}$ (where the new superindices indicate which copy of the corresponding sources are acted upon) that satisfy the analogs of Eqs. (110) and (111) at the level of Born's rule, namely,

$$\mathrm{tr}[\rho\cdot Q(\{A_{a|x}^{i,j}\},\{B_{b|y}^{k,l}\},\{C_{c|z}^{m,n}\})] = \mathrm{tr}[\rho\cdot Q(\{A_{a|x}^{\pi(i),\pi'(j)}\},\{B_{b|y}^{\pi'(k),\pi''(l)}\},\{C_{c|z}^{\pi''(m),\pi(n)}\})], \tag{116}$$

for any polynomial $Q$ of the operators, and

$$\mathrm{tr}\left[\rho\cdot\bigotimes_{i=1}^{n}(A_{a_i|x_i}^{i,i}\otimes B_{b_i|y_i}^{i,i}\otimes C_{c_i|z_i}^{i,i})\right] = \Pi_{i=1}^{n} p_Q^{\triangle}(a_i,b_i,c_i|x_i,y_i,z_i), \tag{117}$$

for any $n$ and any independent permutations $\pi$, $\pi'$, and $\pi''$ of the copies of a same source. Now one can develop a hierarchy in $n$, which denotes the amount of copies of each source in the inflation network [Fig. 7(c) contains the $n=2$ quantum inflation of the triangle scenario]. For each $n$ the characterization of the states and operators that satisfy Eqs. (116) and (117) has the same form of that discussed in Sec. V.A, with some additional linear constraints at the level of expectation values. Thus, this characterization can be approximated by the NPA hierarchy.

Therefore, the implementation of quantum inflation comprises two different hierarchies. The first hierarchy is that of inflations increasing the number of copies of the sources in the network. For each inflation there is then an NPA-like hierarchy to characterize the correlations compatible with such inflation. The latter hierarchy is known to converge to the set of quantum correlations with a commutation structure (which, as explained in Sec. V.A, is a relaxation of the tensor-product structure that coincides with it for finite-dimensional Hilbert spaces). For the former it is not yet known whether the hierarchy where step $n$ represents the inflation with $n$ copies of each source [defined by Wolfe *et al.* (2021)] converges, except in the case of the bilocality network; see Fig. 8 in Sec. VIII.B.1 (Ligthart and Gross, 2023). There is another, provably convergent SDP sequence for quantum network nonlocality, namely, that of Ligthart, Gachechiladze, and Gross (2023). However, this is not a hierarchy in the standard sense, because it is not monotonic: failing a particular SDP test does not imply that the subsequent SDP tests will fail too.

Wolfe *et al.* (2021) outlined with examples various families of applications of quantum inflation. This included certifying that distributions are impossible to generate in a concrete quantum network, optimizing over distributions that can be generated in a quantum network, extracting polynomial witnesses of incompatibility, and, in a concrete practical example, bounding the information that an eavesdropper could obtain in cryptographic scenarios involving quantum repeaters. Notably, additional commutation constraints can be added to the quantum inflation SDPs in order to constrain the resulting correlations to be classical. These SDPs can be seen as semidefinite relaxations of the LPs of the classical inflation hierarchy of Sec. VIII.A.1, where one can trade off computational power for accuracy.

### 3. No-signaling and independence

Correlations in networks can be characterized subject only to minimal physical constraints, namely, only by the independence of the sources and by the no-signaling principle. While we note that other tools also apply to this task [see Renou *et al.* (2019), Beigi and Renou (2022), and Sec. VIII.B.2], inflation methods present a systematic hierarchy approach for the purpose. The principles for NSI inflation were put forward in the original work of Wolfe, Spekkens, and Fritz (2019): not only can physical systems not be cloned, but the compatibility relations between the measurements that are performed on the distributed physical states are not characterized. This means in practice that measurement devices receive only one copy of each relevant system. These two requirements significantly constrain the set of allowed inflations; see Fig. 7(d). The characterization of correlations compatible with NSI inflations can be formulated in terms of a single LP for each inflation.

NSI inflations [also known as *non–fan-out* inflations in the literature (Wolfe, Spekkens, and Fritz, 2019)] have been explicitly used in the context of extending the role of the no-signaling principle to networks, in situations where the parties do not have a choice of measurements to perform on their systems (Gisin *et al.*, 2020) and in demonstrations of nonlocality in the simplest scenario in the triangle network, namely, that in which all the parties do not have inputs and produce binary outcomes (Pozas-Kerstjens *et al.*, 2023). This has led to the definition of the analogous of a Popescu-Rohrlich box (Popescu and Rohrlich, 1994) for network correlations based on the work of Bancal and Gisin (2021). Moreover, the agnosticity of the physical model has been used as a theoretical basis for proposing a definition of genuine $n$-partite nonlocality based on the idea that correlations cannot be simulated in any network using global classical randomness and nonlocal resources shared between $n-1$ parties

(Coiteux-Roy, Wolfe, and Renou, 2021a, 2021b). However, in contrast to the classical and quantum versions of inflation, it is not true that the steps in the NSI inflation hierarchy describe sets of correlations that are contained in those corresponding to lower levels, although the behavior observed in practice is that of monotonically improving bounds. Currently how to define network correlations subject only to the existence of independent sources and no-signaling is a complicated matter (Henson, Lal, and Pusey, 2014), and in fact NSI inflations have been proposed as a definition that is physically well motivated (Beigi and Renou, 2022).

Note that the various inflation techniques can be combined in order to address correlations in networks where different sources distribute systems of different natures. This is especially easy in the case of classical and NSI inflation since both are naturally formulated in terms of LPs. For example, such hybrid inflations are useful tools for tests of full network nonlocality (Pozas-Kerstjens, Gisin, and Tavakoli, 2022; Gu *et al.*, 2023; Wang, Pozas-Kerstjens *et al.*, 2023; Luo, Yang, and Pozas-Kerstjens, 2024), where one aims to certify that every source in a network must uphold some degree of nonlocality in order to model observed correlations. However, hybrid networks are still mostly unknown territory.

#### 4. Entanglement in networks

A natural question when studying quantum networks regards what sort of entangled states can be produced in a given network. Indeed, this question has recently received considerable attention (Navascués *et al.*, 2020; Kraft, Designolle *et al.*, 2021; Kraft, Spee *et al.*, 2021; Luo, 2021). When we again take as illustration the triangle network of Fig. 7(a), if the sources distribute quantum states $\sigma \in \mathcal{H}_{A''B'}$, $\mu \in \mathcal{H}_{B''C'}$, and $\tau \in \mathcal{H}_{C''A'}$ and the parties perform local operations characterized as completely positive trace-preserving maps $\Omega_P : \mathrm{B}(\mathcal{H}_{P'} \otimes \mathcal{H}_{P''}) \to \mathrm{B}(\mathcal{H}_P)$, all states that can be produced in the triangle network take the form

$$\rho^{\triangle} = [\Omega_A \otimes \Omega_B \otimes \Omega_C](\sigma \otimes \mu \otimes \tau). \tag{118}$$

While an individual characterization of any of the components of Eq. (118) can be cast as an SDP [see the seesaw procedure in Eqs. (24) and (25)], the complete characterization of $\rho^{\triangle}$ cannot.

The problem of characterizing the quantum states that can be produced in quantum networks was addressed by Navascués *et al.* (2020) via SDP relaxations based on inflation. In a spirit similar to that described in Sec. VIII.A, these relaxations transform the conditions on the independence of the sources in the network into symmetry constraints in more complicated networks, created using copies of the original sources and operations. The main difference is that, while the symmetry constraints were enforced at the level of expectation values of operators when studying nonlocality in Sec. VIII.A, when studying network entanglement the constraints are enforced at the level of the quantum state in the inflation and its marginals. The fact that the state must be a PSD operator allows the problem to be phrased as a single SDP for a fixed inflation. Navascués *et al.* (2020) used these relaxations to bound the maximum fidelities of known multipartite states with network realizations, which were later interpreted as witnesses of genuine network entanglement. Similarly, Hansenne *et al.* (2022) and Wang, Xu, and Gühne (2024) provided no-go theorems regarding the preparation of cluster and graph states in networks.

### B. Other SDP methods in network correlations

In addition to inflation, in some specific scenarios there are other methods for characterizing network correlations. They range from analytic methods to alternative LP and SDP relaxations. We now review some of these relaxations.

#### 1. Relaxations of factorization

Particles that have never interacted can become entangled via the seminal process of entanglement swapping (Żukowski *et al.*, 1993). The simplest entanglement-swapping scenario is that in which two parties Alice and Charlie share each a bipartite physical system with a central party, Bob, that performs entangled operations on the two systems received (Pan *et al.*, 1998; Jennewein *et al.*, 2001); see Fig. 8. Recently this setting was employed for showing that real Hilbert spaces have less predictive power than the complex Hilbert spaces postulated by quantum theory (Renou *et al.*, 2021). The associated entanglement-swapping scenario assumes that the two sources share no entanglement but may be classically correlated. SDP relaxation methods based on PPT constraints compatible with the interpretation of the NPA hierarchy discussed in Sec. V.B.3 are then employed to bound the predictive power of real quantum models.

However, it is also relevant to consider entanglement swapping when the sources are also classically uncorrelated. Any correlation between Alice and Charlie must then be mediated by Bob, i.e., two-body expectation values factor as $\langle AC \rangle = \langle A \rangle \langle C \rangle$, thereby breaking the convexity of the sets of relevant correlations. This was the first network scenario considered in the literature and for which specific network Bell inequalities were developed (Branciard, Gisin, and Pironio, 2010; Branciard *et al.*, 2012).

Pozas-Kerstjens *et al.* (2019) provided SDP hierarchies that relax the nonconvex sets of probability distributions generated in networks where some parties are not connected to others. These hierarchies are modifications of the NPA hierarchy discussed in Sec. V.A. The main idea of the modification consisted of a *scalar extension* allowing the rows and columns of moment matrices to be labeled not only by operators but also by subnormalized operators that denote products of an actual normalized operator in the problem and a possibly unknown expectation value. The elements in the moment matrices that are generated from these sets of operators will

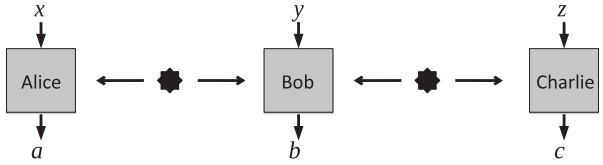


FIG. 8. The bilocality network. A central party receives shares from two independent sources, each of which sends another share to a different party. This network underlies the simplest entanglement-swapping experiments and quantum repeaters.

contain variables that represent products of expectation values and can be associated via linear constraints to other variables upon which one wants to impose factorization.

Take as an illustration the entanglement-swapping scenario with Alice and Charlie performing two dichotomic measurements each, $\{A_0, A_1\}$ and $\{C_0, C_1\}$, respectively, and the moment matrix generated[40] by the set of operators $\{\mathbb{1}, A_0A_1, C_0C_1, \langle A_0A_1\rangle\mathbb{1}\}$,

$$\Gamma = \begin{array}{c} \\ \mathbb{1} \\ (A_0A_1)^\dagger \\ (C_0C_1)^\dagger \\ \langle A_0A_1\rangle_\rho^*\mathbb{1} \end{array} \begin{array}{c} \begin{array}{cccc} \mathbb{1} & A_0A_1 & C_0C_1 & \langle A_0A_1\rangle_\rho\mathbb{1} \end{array} \\ \begin{pmatrix} 1 & v_1 & v_2 & v_2 \\ & 1 & v_4 & v_5 \\ & & 1 & v_6 \\ & & & v_7 \end{pmatrix} \end{array}. \tag{119}$$

Per the standard NPA prescription, we have $v_1 = v_3$ because they both evaluate to $\langle A_0A_1\rangle_\rho$, and $v_5 = v_7$ because both evaluate to $\langle\langle A_0A_1\rangle_\rho(A_0A_1)^\dagger\rangle_\rho = |\langle A_0A_1\rangle_\rho|^2$. Moreover, in the entanglement-swapping scenario it holds that, regardless of the particular operators and quantum state, $\langle A_0A_1C_0C_1\rangle_\rho = \langle A_0A_1\rangle_\rho\langle C_0C_1\rangle_\rho$. This constraint is enforced in Eq. (119) by setting the linear constraint $v_4 = v_6$. Since all constraints between the variables in Eq. (119) are linear, the set of distributions admitting a PSD $\Gamma$ can be characterized via SDP.

A hierarchy can then be generated by taking the levels of the associated NPA hierarchy and, for each of them, adding as many new columns as are needed to impose at least one linear constraint per element of $\Gamma$ that should factorize. For the entanglement-swapping scenario, the hierarchy constructed in such a way converges to the desired set of quantum distributions (Renou and Xu, 2022). However, the proof technique used there is difficult to generalize to more complicated networks (Tavakoli *et al.*, 2014; Mukherjee, Paul, and Sarkar, 2015), where the SDP method still applies. The method has been used to show that networks can activate the usefulness of measurement devices for detecting network nonlocality (Pozas-Kerstjens *et al.*, 2019) and to provide quantum bounds on Bell inequalities tailored to the entanglement-swapping scenario (Tavakoli, Gisin, and Branciard, 2021).

#### 2. Tests for network topology

SDP relaxations can also be used to rule out a hypothesized causal structure, i.e., a network constellation, connecting a given number of measuring parties. In some situations it is fairly easy to detect correlations that could not have been produced in a concrete network. A simple illustration is the network in Fig. 8. As discussed, if one considers the marginal distribution of Alice and Charlie, the resulting correlations must factor since there is no connection between the two parties. Thus, any nonfactoring correlations between Alice and Charlie are impossible to generate in the bilocal network. While nonlinear, these constraints can be linearized by working with the entropies of the variables instead of the probabilities (Weilenmann and Colbeck, 2017). However, in other networks like the triangle network of Fig. 7, such simple criteria do not exist, because all parties are connected to all sources.

Åberg *et al.* (2020), building on a similar characterization for correlations admitting local models in networks (Kela *et al.*, 2020), found simple criteria that allowed them to discern whether correlations admitted a realization in a particular network, regardless of the physical model of the systems distributed by the sources. The characterization is based on the covariance matrix of the variables representing the outcomes of the measurements performed by the parties. Covariance matrices are inherently PSD. The important realization is that the network structure imposes a decomposition of the covariance matrix in block matrices that are individually PSD, as they determine the correlations established by each of the sources. That is, for each source there is one PSD block matrix, that contains nonzero elements only in the rows and columns associated with the parties that receive systems from that source. This leads to a simple and efficient way to characterize the correlations that can be generated in different networks via SDP that has been found to be connected to the characterization of block coherence of quantum states (Kraft, Spee *et al.*, 2021). However, as discussed by Åberg *et al.* (2020), this characterization is not tight, in the sense that there are alternative methods that better approximate the set of relevant correlations in some situations.

## IX. FURTHER TOPICS AND METHODS

In this section we collect additional topics where SDP relaxations are relevant and methods for reducing the computational load of SDP.

### A. Classical models for quantum correlations

For some entangled states the outcome statistics from performing arbitrary local measurements in Bell-type experiments can be simulated by models based on local variables. Consequently entanglement and nonlocality are two distinct phenomena (Augusiak, Demianowicz, and Acín, 2014). The seminal example is Werner's model showing that the state $\rho_v = v|\psi^-\rangle\langle\psi^-| + [(1-v)/4]\mathbb{1}$, where $\psi^-$ is the singlet state, admits an LHV model for $v \leq 1/2$, even though the state is entangled for any $v > 1/3$ (Werner, 1989). The critical $v$ up to which the $\rho_v$ admits an LHV model for all projective measurements turns out to be equal to the inverse of the Grothendieck constant of order 3 (Acín, Gisin, and Toner, 2006).

General methods are known for deciding whether a given entangled state admits an LHV model (Cavalcanti *et al.*, 2016; Hirsch *et al.*, 2016). These methods are based on the idea of first choosing a finite collection of measurements and determining via LP how much white noise must be added to the state for there to be an LHV model of the resulting distribution. Next one can add sufficient white noise in the measurement space so that all the quantum measurements can be represented as classical postprocessings of the measurements in the selected set. In other words, the measurement space is shrunk until it is contained in the convex hull of the

[40]See footnote 21.

selected measurement set. It then follows that, for any such noisy measurement, the distribution must admit an LHV. In a final step one can pass the noise in the measurement space to the state space and obtain a generic LHV model for the final noisy state. The bottleneck here is that one must choose a large measurement set to obtain a good approximation of the quantum measurement space. This means solving an accordingly large LP or SDP. To circumvent this one can instead employ an oracle-based method known as Gilbert's algorithm (Gilbert, 1966; Brierley, Navascués, and Vértesi, 2017), which allows one to approximate the distance between a point and a convex set in real space. Hirsch *et al.* (2017) used this algorithm together with a simple heuristic for the oracle to implement a polyhedral approximation of the Bloch sphere based on 625 measurements and thereby obtain an LHV model for $\rho_v$ up to $v \approx 0.6829$. Another option is to use instead of Gilbert's algorithm the more general Frank-Wolfe algorithm (Frank and Wolfe, 1956; Bomze, Rinaldi, and Zeffiro, 2021). This has further improved the LHV threshold to $v \approx 0.6875$ (Designolle *et al.*, 2023). Notably, this work also provided an improved upper bound at $v \approx 0.6961$ using 97 local measurements. In fact, methods of this sort also work when building local hidden state models; see Eq. (7) for entangled states. The main difference is that one runs an SDP to check for the steerability of the assemblage instead of the LP for membership to the local polytope. However, when restricting to two-qubit entanglement, one can exploit geometric arguments and use increasingly large polytope circumscription and inscriptions of the Bloch sphere in order to determine bounds on the steerability of a state for infinitely many measurement settings, which can be evaluated via LP (Nguyen, Nguyen, and Gühne, 2019).

The idea of shrinking the quantum measurement space so that it can be inscribed in a polytope whose vertices comprise finitely many measurements can also be applied in other settings. For example, in the case of steering, this was done by Bavaresco *et al.* (2017). A similar approach shows that there are sets of incompatible measurements that can never be used to violate a Bell inequality (Bene and Vértesi, 2018; Hirsch, Quintino, and Brunner, 2018). This extends earlier SDP arguments that were restricted to sets of projective measurements for the uncharacterized party (Quintino *et al.*, 2016). Moreover, this type of approach can also be used in the prepare-and-measure scenario to determine whether the outcome statistics associated with performing arbitrary measurements on an ensemble of qubit states admits a classical model based on bits (de Gois *et al.*, 2021). Using Gilbert's algorithm with up to 70 measurements, nontrivial bounds have been established on the critical detection efficiency needed to violate classical constraints in the qubit prepare-and-measure scenario (Diviánszky *et al.*, 2023).

### B. Generalized Bell scenarios

A large portion of this review has focused on scenarios where all the parties share parts of the same quantum state that are known as Bell scenarios. These scenarios were generalized in Sec. VIII to account for multiple independent sources distributing systems between different collections of parties. There are further generalizations of the Bell scenario that are relevant in randomness generation and in entanglement certification, and that can be characterized via SDP.

The first generalization is that to sequential scenarios where, instead of performing only one measurement at every round, the parties perform sequences of measurements in the systems received (Gallego *et al.*, 2014; Silva *et al.*, 2015). These scenarios are conceptually interesting, including in the context of randomness generation, since it is possible to extract more randomness from a given state when performing sequences of measurements (Curchod *et al.*, 2017). It is possible to modify the NPA hierarchy (see Sec. V.A) in order to characterize the correlations that can be produced in these scenarios (Bowles, Baccari, and Salavrakos, 2020). This is achieved by considering operators that represent strings of outcomes and requiring that these operators satisfy "no signaling to the past" (i.e., that the measurement operators that define the first $k$ measurements do not depend on the $n-k$ remaining inputs, since these occur later in the sequence), which are linear constraints admitted in SDPs. The result is a convergent hierarchy that has been used to certify local randomness beyond two bits and for investigating monogamy properties of nonlocality.

The second generalization that we discuss is that known as broadcast scenarios, where the systems sent to one or several of the parties are passed through channels that prepare new systems, and the outputs are distributed to multiple new parties that measure them (Bowles, Hirsch, and Cavalcanti, 2021). When the channel prepares quantum systems, the correlations in the scenario can be characterized with a slight modification of the NPA hierarchy. This scenario has found particular interest in the activation of nonlocality. With a quantum model, it allows one to certify in a device-independent way the entanglement of Werner states in almost the entire range in which it is known to be entangled (Boghiu *et al.*, 2023).

### C. Bounding ground-state energies

A central problem in the study of many-body systems is computing or bounding the ground-state energy of the system, i.e., finding the minimal eigenvalue of its corresponding Hamiltonian. This problem is known to be computationally hard, in particular, it is in general QMA complete (Kempe, Kitaev, and Regev, 2006). Thus, computationally tractable relaxations have been sought and, in particular, several SDP approaches have been developed.

The structure of the problem naturally lends itself to a treatment in terms of noncommutative polynomial optimization. In particular, the problem takes the form $\min \mathrm{tr}(\rho H)$, where $H$ can be written as a polynomial of local operators. Thus, lower bounds can be obtained from SDP relaxation techniques similar to those mentioned in Sec. III (Barthel and Hübener, 2012; Baumgratz and Plenio, 2012).

An apparent numerical paradox can be observed when these computations are performed for bosonic systems (Navascués *et al.*, 2013). Convergence of the semidefinite hierarchies for noncommutative polynomial optimization problems is proven only when the operators are bounded (Pironio, Navascués, and Acín, 2010). Therefore, for problems involving the bosonic creation (annihilation) operators $a_i^\dagger$ $(a_i)$, the standard proof of

convergence does not hold. In fact, it can be shown that for Hamiltonians in this setting the hierarchy collapses at level 1. That is, higher levels give no improvement over level 1, and the optimal value at level 1 is not equal to the optimal value of the original problem. Nevertheless, when performing the computations numerically, one can sometimes observe improving lower bounds that converge to the actual solution. This apparent paradox is due to the finite precision of numerical computations, implying that the solver is actually solving a slightly perturbed problem. Mathematically the set of SOS polynomials is dense in the set of positive polynomials generated by the ladder operators. Note that a similar numerical paradox appeared in the setting of commutative polynomial optimization (Henrion and Lasserre, 2005), and it has a similar resolution (Lasserre, 2007).

Another approach to obtaining SDP relaxations for the ground-state energy problem was proposed by Kull *et al.* (2024). They considered the problem of computing the ground-state energy of a translation-invariant Hamiltonian with identical nearest-neighbor interactions on each pair of an infinite chain. Formally the problem can be stated as

$$\begin{aligned} \min \quad & \mathrm{tr}(H\rho^{(2)}) \\ \text{such that} \quad & \mathrm{tr}(\rho^{(2)}) = 1, \\ & \rho^{(2)} \succeq 0, \\ & \rho^{(2)} \leftarrow \psi_{\mathrm{TI}}, \end{aligned} \tag{120}$$

where $\rho^{(m)}$ denotes the density matrix corresponding to an $m$-body marginal and $\rho^{(2)} \leftarrow \psi_{\mathrm{TI}}$ is the constraint that $\rho^{(2)}$ is a two-body marginal of some translation-invariant state for the entire chain. The latter constraint is equivalent to a quantum marginal problem asking whether there is a global state consistent with the marginal states; see Sec. IV.C.2. It can be relaxed to the existence of all $m$-body marginals up to some finite $m_{\max} \in \mathbb{N}$, i.e., a collection of partial trace constraints $\rho^{(2)} \leftarrow \rho^{(3)} \leftarrow \cdots \leftarrow \rho^{(m_{\max})}$. This results in a hierarchy of SDP relaxations; however, the size of the SDPs grows exponentially in the number of sites considered. The core idea of Kull *et al.* (2024) was to apply compression maps that retain the useful aspects of the marginal constraints while reducing the dimension of the variables significantly.

### D. Rank-constrained optimization

Several problems of interest in classical and quantum information theory can be formulated as an optimization problem that includes a constraint in the rank of a matrix. These include optimization over pure quantum states, the Max-Cut problem (Goemans and Williamson, 1995), matrix completion (Candès and Tao, 2010), compressed sensing quantum state tomography (Gross *et al.*, 2010), detection of unfaithful entanglement (Weilenmann *et al.*, 2020; Gühne, Mao, and Yu, 2021), and many others (Markovsky, 2012).

The problem of optimizing under rank constraints is generally NP hard, and as such it is usually solved via heuristics or approximations (Sun and Dai, 2017). It is possible, however, to formulate it as an SDP hierarchy similar to the DPS hierarchy discussed in Sec. IV.A by reformulating it as a separability problem (Yu *et al.*, 2022). This allows one to obtain a sequence of global bounds to the problem that converge to the optimal value.

The idea is that a state $\rho$ of dimension $d$ has a rank of at most $k$ if and only if it is the partial trace of a pure state $|\phi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^k$. The set of such states is hard to characterize, but it can be handled by first noticing that one is interested only in its convex hull, and then by noticing that the convex hull is the partial trace over the last two subsystems of a state $\sigma \in \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^k \otimes \mathbb{C}^d \otimes \mathbb{C}^k)$ that respects the constraints of being separable over the bipartition $(12|34)$, which is invariant under a SWAP over the same bipartition, and recovering the initial $\rho$ through the appropriate partial trace. Exploiting these, one can use the DPS hierarchy to characterize the separability constraint, thereby obtaining the SDP hierarchy for rank-constrained optimization. Note that although the idea we have explained here is in terms of quantum states, it also applies to bound ranks of general matrices.

### E. Quantum contextuality

Quantum theory cannot be modeled with hidden variables that are both deterministic and noncontextual[41] (Bell, 1966; Kochen and Specker, 1968). This is known as contextuality (Budroni *et al.*, 2022). Contextuality scenarios can be cast in the language of graph theory, where each input-output tuple (event) is associated with a vertex, and an edge is drawn between two vertices if and only if the events can be distinguished by jointly measurable observables. While many different contextuality tests can be associated with the same graph, both the noncontextual hidden variable and the quantum bounds associated with a given graph can be bounded in terms of the graph's independence number and the Lovász theta function, respectively (Cabello, Severini, and Winter, 2014); see Eq. (81). These quantities are computable via LP and SDP, respectively. The connection with the Lovász theta function has been leveraged to self-test quantum states in contextuality scenarios by examining the dual SDP (Bharti *et al.*, 2019). Generally it is possible to adapt the NPA hierarchy to arbitrary tests of contextuality by leveraging the fact that compatible projective measurements commute, which adds constraints to the moment matrix (Acín *et al.*, 2015).

A more operational notion of contextuality has also been proposed that is not specific to quantum theory and not limited to projective measurements (Spekkens, 2005). Two preparations (measurements) are considered indistinguishable if they cannot be distinguished through any measurement (preparation) allowed in the theory. They are said to belong to the same context and are therefore assigned the same realist representation. When operationally indistinguishable preparations give rise to statistics that do not admit such a realist model, the theory is said to be contextual. This test can be cast as an LP; see Selby *et al.* (2024). The set of preparation contextual quantum correlations can be bounded by hierarchies of SDPs.

[41]This means that each projective measurement is assigned a definite value that is independent of other compatible measurements performed simultaneously.

Two different hierarchies have been proposed. One leverages the idea and SDP methods of informationally restricted correlations (Tavakoli, Zambrini Cruzeiro *et al.*, 2022) reviewed in Sec. VI.C.1 by interpreting the indistinguishability of two preparations as the impossibility of accessing any information about which preparation was selected (Tavakoli, Zambrini Cruzeiro *et al.*, 2021). The other relies on using unitaries in the monomial representation and connecting them to POVMs via the fact that every $0 \preccurlyeq M \preccurlyeq \mathbb{1}$ can be written in terms of a unitary $M = \mathbb{1}/2 + (U + U^\dagger)/4$ (Chaturvedi, Farkas, and Wright, 2021). Both methods require an extensive use of localizing matrices to deal with mixed states and nonprojective measurements. Notably, these ideas also enable the addition of measurement contextuality. The convergence of either hierarchy to the quantum set remains unknown.

Furthermore, in experimental tests of this type of contextuality, it is not the case that the relevant lab preparations are precisely indistinguishable, including when the measurements used to probe their distinguishability are a small subset of the entire measurement space. Upon accepting the latter limitation, the former issue can be resolved by means of LP by leveraging the linearity of the operational theory to postprocess the lab data into new data that correspond to exactly indistinguishable preparations (Mazurek *et al.*, 2016). Simplified variants of this approach have also been used for qutrit-based contextuality tests (Hameedi *et al.*, 2017).

### F. Symmetrization methods

Many of the most interesting problems in quantum information exhibit a degree of symmetry. Exploiting them can lead to vast computational advantages: turning an intractable problem into a tractable one, or even making it simple enough to allow for an analytical solution. Symmetries have been successfully applied to several problems, for example, polynomial optimization (Gatermann and Parrilo, 2004); nonlocal correlations (Moroder *et al.*, 2013; Fadel and Tura, 2017; Ioannou and Rosset, 2021); quantum communication (Tavakoli, Rosset, and Renou, 2019); mutually unbiased bases (Aguilar *et al.*, 2018; Gribling and Polak, 2024), port-based teleportation (Studziński *et al.*, 2017; Mozrzymas *et al.*, 2018; Mozrzymas, Studziński, and Kopszak, 2021); unitary inversion, transposition, and conjugation (Grinko and Ozols, 2022; Ebler *et al.*, 2023; Yoshida, Soeda, and Murao, 2023); rank-constrained optimization (Yu *et al.*, 2022); and measurement incompatibility (Nguyen *et al.*, 2020).

The fundamental idea behind symmetrization techniques is that, if both the objective function and the feasible set of an SDP are invariant under transformation of the variable $X$ by some function $f$, one can exploit this symmetry to eliminate redundant variables and block diagonalize $X$. Both of these reductions can drastically simplify the problem.

To be more precise we consider again an SDP in the primal form of Eq. (1). Assume that there exists a function $f$ such that $\langle C, f(X)\rangle = \langle C, X\rangle$, and furthermore that if $X$ is a feasible point, that is, $\langle A_i, X\rangle = b_i \ \ \forall \ i$ and $X \succeq 0$, then $f(X)$ is also a feasible point. For all feasible $X$ and $\lambda \in [0,1]$, the point $g(X,\lambda) = \lambda X + (1-\lambda) f(X)$ will then be feasible and attain the same value of the objective, which follows from linearity and convexity. Assume also that there exists $\lambda^*$ such that $f(g(X,\lambda^*)) = g(X,\lambda^*)$, meaning that $g(X,\lambda^*)$ is a projection of $X$ onto a fixed point of $f$. One can then add the constraint $f(X) = X$ to the SDP in Eq. (1) without loss of generality. That is, it is possible to rewrite Eq. (1) as

$$\begin{aligned} \max_X \quad & \langle C, X\rangle \\ \text{such that} \quad & \langle A_i, X\rangle = b_i \quad \forall\, i, \\ & f(X) = X, \\ & X \succeq 0. \end{aligned} \tag{121}$$

To see why consider a feasible (or optimal) point $X^*$ for the SDP in Eq. (1). From the previous argument $g(X^*,\lambda^*)$ will also be feasible for the original SDP, with the same value of the objective. Since by assumption it is a fixed point of $f$, it is also feasible for the SDP in Eq. (121).

The simplest example of symmetrization is when $C$, $A_i$, and $b_i$ are all real. Then a function $f$ that leaves the objective and feasible set of the SDP invariant is complex conjugation, and the projection onto its fixed point is taking the real part of $X$. This symmetrization often delivers significant performance improvements, as SDP solvers frequently have poor support for complex numbers.

Symmetrizing an SDP then boils down to identifying $f$, the projection onto the fixed point subspace, and using the constraint $f(X) = X$ to simplify the problem. The theory for doing so is particularly simple and well developed when $f$ is a group action (Gatermann and Parrilo, 2004; Bachoc *et al.*, 2011; Riener *et al.*, 2013), so we present it here while noting that more general techniques exist (de Klerk, Dobre, and Pasechnik, 2011; Permenter and Parrilo, 2020).

Let then $G$ be a group, and let $\rho$ be a representation of the group, that is, a function $g \mapsto \rho_g$ such that for all $g, h \in G$ we have $\rho_{gh} = \rho_g \rho_h$. Here we consider only unitary representations, which are those in which $\rho_{g^{-1}} = \rho_g^\dagger$. The group then acts on the SDP variable as $X \mapsto \rho_g X \rho_g^\dagger$. We say that the SDP is invariant under this group action if for all $g$ we have that $\langle C, \rho_g X \rho_g^\dagger\rangle = \langle C, X\rangle$ and $\langle A_i, X\rangle = b_i$ imply $\langle A_i, \rho_g X \rho_g^\dagger\rangle = b_i$ for all $i$. Note that we do not need to consider whether $\rho_g X \rho_g^\dagger \succeq 0$ for $X \succeq 0$, as this is always the case.

The projection onto the fixed point subspace is then given by the group average[42]

$$\bar{X} = \frac{1}{|G|} \sum_{g \in G} \rho_g X \rho_g^\dagger, \tag{122}$$

which can be easily verified to satisfy $\bar{X} = \rho_g \bar{X} \rho_g^\dagger$ for all $g$, so we can add that as a constraint to the SDP.

This constraint allows one not only to eliminate redundant variables but also to block diagonalize $\bar{X}$ using Schur's lemma. The main idea is that a group representation can be decomposed as a direct sum of the irreducible representations with their multiplicities, so there exists a unitary matrix $V$ such that, for all $g$,

$$V \rho_g V^\dagger = \bigoplus_i \mathbb{1}_{n_i} \otimes \rho_g^i, \tag{123}$$

[42]In the case of an infinite but compact group, this is given by $\int_G d\mu(g) \rho_g X \rho_g^\dagger$, where $\mu$ is the Haar measure on $G$.

where $\rho_g^i$ is the $i$th irreducible representation with dimension $d_i$ and multiplicity $n_i$. Now the constraint $\bar{X} = \rho_g \bar{X} \rho_g^\dagger$ is equivalent to $[\bar{X}, \rho_g] = 0$, which implies that the same $V$ also block diagonalizes $\bar{X}$,

$$V \bar{X} V^\dagger = \bigoplus_i \bar{X}^i \otimes \mathbb{1}_{d_i}, \tag{124}$$

where $X^i$ is a Hermitian matrix of dimension $n_i$.

Computing $V$ can be challenging. For small problems it can be computed analytically using computer algebra systems such as GAP (GAP Group, 2022). In the cases where the representation in question is the tensor product of $n$ unitaries of dimension $d$, the permutations between $n$ tensor factors of dimension $d$, or a combination, the Schur-Weyl duality can be used to give an explicit construction of $V$ (Bacon, Chuang, and Harrow, 2007). In general, though, it can only be computed numerically, via the use of software such as `RepLAB` (Rosset, Montealegre-Mora, and Bancal, 2021).

To illustrate how symmetrization works, we consider a simple SDP

$$\begin{aligned} \min_{x_1, x_2} \quad & x_1 + x_2 \\ \text{such that} \quad & X = \begin{pmatrix} 2 & x_1 & 1 \\ x_1 & 2 & x_2 \\ 1 & x_2 & 2 \end{pmatrix} \succeq 0. \end{aligned} \tag{125}$$

Equation (125) is invariant under permutation of the first and third rows and columns of $X$. Since this permutation is its own inverse, the underlying group is the symmetric group over two elements $G = \{e, p\}$, where $e$ is the identity and $p^2 = e$. The group representation that we need is then $\rho_e = \mathbb{1}$ and

$$\rho_p = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}. \tag{126}$$

We first eliminate variables using the group average,

$$\bar{X} = \frac{1}{2}(\rho_e X \rho_e^\dagger + \rho_p X \rho_p^\dagger) = \begin{pmatrix} 2 & y & 1 \\ y & 2 & y \\ 1 & y & 2 \end{pmatrix}, \tag{127}$$

where $y = (x_1 + x_2)/2$ is now the sole variable of the SDP. To perform the block diagonlization, we note that the symmetric group over two elements has only two irreducible representations, 1 and $-1$. The representation that we are using consists of two copies of 1 and one copy of $-1$, and the unitary that block diagonalizes it is

$$V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & -1 \\ 0 & \sqrt{2} & 0 \\ 1 & 0 & 1 \end{pmatrix}, \tag{128}$$

with which $V \rho_p V^\dagger = (1 \otimes -1) \oplus (\mathbb{1}_2 \otimes 1)$. The same unitary block diagonalizes $\bar{X}$ as $V \bar{X} V^\dagger = (\bar{X}^1 \otimes 1) \oplus (\bar{X}^2 \otimes 1)$, where $\bar{X}^1 = 1$ and $\bar{X}^2 = \left(\begin{smallmatrix} 2 & y\sqrt{2} \\ y\sqrt{2} & 3 \end{smallmatrix}\right)$. The SDP was simplified to

$$\begin{aligned} \min_{y} \quad & 2y \\ \text{such that } X = & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & y\sqrt{2} \\ 0 & y\sqrt{2} & 3 \end{pmatrix} \succeq 0. \end{aligned} \tag{129}$$

Equation (129) can now be solved as an eigenvalue problem of a $2 \times 2$ matrix, with the optimal solution being $-2\sqrt{3}$.

## X. CONCLUSIONS

Quantum theory promises many advantages in information-processing tasks. However, in general characterizing the correlations established by quantum systems is demanding, both at the complexity theory level and in practice. In this review we have shown that many questions related to quantum correlations can be written as, or relaxed to, semidefinite programming problems. This has enabled researchers to obtain approximate or exact solutions to many problems regarding entanglement, nonlocality, quantum communication, quantum networks, quantum cryptography, etc. For this reason semidefinite programming has become a central tool in the field.

## LIST OF SYMBOLS AND ABBREVIATIONS

| | |
|---|---|
| GME | genuine multipartite entanglement |
| LHV | local hidden variable |
| LP | linear program |
| LOCC | local operations and classical communication |
| MDI | measurement-device independent |
| POVM | positive operator-valued measure |
| PPT | positive partial transpose |
| PSD | positive semidefinite |
| QKD | quantum key distribution |
| QMP | quantum marginal problem |
| SDI | semi–device independent |
| SDP | semidefinite program |
| SOS | sum of squares |

## ACKNOWLEDGMENTS

We thank Kishor Bharti, Cyril Branciard, Siddharta Das, Omar Fawzi, Carlos de Gois, Sander Gribling, Otfried Gühne, Felix Huber, Ludovico Lami, Yeong-Cherng Liang, Miguel Navascués, Ties Ohst, Jef Pauwels, Stefano Pironio, Denis Rosset, Vincent Russo, Gaurav Saxena, Valerio Scarani, Marco Túlio Quintino, and Mark Wilde for their comments and feedback. A. T. is supported by the Wenner-Gren Foundations and by the Knut and Alice Wallenberg Foundation through the Wallenberg Center for Quantum Technology (WACQT). A. P.-K. is supported by the Spanish Ministry of Science and Innovation (Grants No. CEX2019-000904-S and No. PID2020–113523 GB-I00), the Spanish Ministry of Economic Affairs and Digital Transformation (project QUANTUM ENIA, as part of the Recovery, Transformation and Resilience Plan, which is

funded by the EU program NextGenerationEU), Comunidad de Madrid (QUITEMAD-CM Grant No. P2018/TCS-4342), Universidad Complutense de Madrid (Grant No. FEI-EU-22-06), the CSIC Quantum Technologies Platform PTI-001, the NCCR SwissMAP, and the Swiss National Science Foundation (Grant No. 224561). P. B. acknowledges funding from the European Union's Horizon Europe research and innovation program under the project "Quantum Secure Networks Partnership" (QSNP; Grant Agreement No. 101114043). M. A. acknowledges funding from the FWF stand-alone Project No. P 35509-N and was also supported by the European Union–Next Generation UE/MICIU/Plan de Recuperación, Transformación y Resiliencia/Junta de Castilla y León.

## APPENDIX A: IMPLEMENTATION GUIDE

In this appendix we discuss publicly available computer code packages for SDP relaxation hierarchies addressing various physics problems. We also discuss different SDP solvers and programming languages.

SDP solvers require the problem to be input in a standard form that is roughly similar to Eqs. (1) and (2) but with details that vary with the specific solver. This can be cumbersome for more complex problems. To get around this it is common to use modelers, which allow much more flexible forms of input and automatically translate them to the format required by the solvers.

The available modelers are

- `YALMIP`: open source, written in `MATLAB-Octave` (Löfberg, 2004).
- `CVX`: proprietary, written in `MATLAB` (Grant and Boyd, 2008).
- `CVXPY`: open source, written in `Python` (Diamond and Boyd, 2016).
- `PICOS`: open source, written in `Python` (Sagnol and Stahlberg, 2022).
- `JuMP`: open source, written in `Julia` (Lubin *et al.*, 2023).

There is a large number of solvers available. Here we mention only a few notable ones:

- `SeDuMi`: open source, bindings for `MATLAB-Octave`. Complex numbers can be handled natively (Sturm, 1999).
- `SDPA`: open source, bindings for `C`, `C++`, and `MATLAB`. The variants `SDPA-GMP`, `SDPA-QD`, and `SDPA-DD` can solve problems with high or arbitrary precision (Nakata *et al.*, 2001; Nakata, 2010).
- `MOSEK`: proprietary, bindings for `C`, `C++`, `Java`, `Julia`, `MATLAB`, `.NET`, `Python`, and `R`. Fast, parallelized implementation (MOSEK ApS, 2023).
- `SCS`: open source, bindings for `C`, `C++`, `Julia`, `MATLAB`, `Python`, `R`, and `Ruby`. Uses a first-order method in order to handle large-scale problems (O'Donoghue *et al.*, 2016).
- `Hypatia`: open source, bindings for `Julia`. Can handle complex numbers natively and solve problems with arbitrary precision, and supports a wide variety of cones other than the SDP one (Coey, Kapelevich, and Vielma, 2022).

There are also several software packages that implement some of the SDP relaxations discussed here. Some notable ones are

- `QETLAB`: open source, written in `MATLAB`. Works with CVX. Implements several of the algorithms discussed here, including the DPS and NPA hierarchies (Johnston, 2016).
- `Ket`: open source, written in `Julia`. Works with `JuMP`. Implements several of the algorithms discussed here, including the DPS hierarchy (Araújo *et al.*, 2024).
- `toqito`: open source, written in `Python`. Works with `CVXPY`. Implements several of the algorithms discussed here, including the DPS and NPA hierarchies (Russo, 2021).
- `MOMENT`: open source, written in `C++` with bindings for `MATLAB`. Works with `YALMIP` and `CVX`. Performs noncommutative polynomial optimization and classical inflation, with symmetrization support (Garner and Araújo, 2024).
- `Ncpol2sdpa`: open source, written in `Python`. Works with SDPA and `MOSEK`. Performs commutative and noncommutative polynomial optimization and focuses on NPA-type problems (Wittek, 2015).
- `GloptiPoly`: open source, written in `MATLAB`, works with `YALMIP`. Performs commutative polynomial optimization (Henrion, Lasserre, and Löfberg, 2009).
- `SOSTOOLS`: open source, written in `MATLAB`. Performs commutative polynomial optimization (Papachristodoulou *et al.*, 2021).
- `NCSOStools`: open source, written in `MATLAB`. Performs noncommutative polynomial optimization (Cafuta, Klep, and Povh, 2012).
- `Inflation`: open source, written in `Python`, works with `MOSEK`. It implements quantum inflation for quantum and classical correlations (Boghiu, Wolfe, and Pozas-Kerstjens, 2023).
- `RepLAB`: open source, written in `MATLAB-Octave`. Performs numerical representation theory for the purpose of symmetrization (Rosset, Montealegre-Mora, and Bancal, 2021).

## APPENDIX B: STRICT FEASIBILITY

In this appendix we prove that the unconstrained NPA hierarchy is strictly feasible by explicitly constructing a positive-definite feasible point. We thank Miguel Navascués for providing this proof.

Instead of the usual basis of projectors to represent Alice's and Bob's measurements $\{A_{a|x}\}_{a,x}$ and $\{B_{b|y}\}_{b,y}$, we instead use the unitary basis of generalized observables, which is defined as

$$A_x = \sum_{a=0}^{N-1} \omega_N^a A_{a|x}, \tag{B1}$$

$$B_y = \sum_{b=0}^{M-1} \omega_M^b B_{b|y}, \tag{B2}$$

where $\omega_N = e^{-i(2\pi/N)}$ and $\omega_M = e^{-i(2\pi/M)}$. The conditions that $\{A_{a|x}\}_{a,x}$ and $\{B_{b|y}\}_{b,y}$ are sets of projectors that sum to identity are mapped onto the condition that $A_x$ and $B_y$ are

unitary and that their $N$th and $M$th powers evaluate to identity, that is,

$$\begin{aligned} A_x A_x^\dagger &= A_x^\dagger A_x = \mathbb{1}, \\ B_y B_y^\dagger &= B_y^\dagger B_y = \mathbb{1}, \\ A_x^N &= B_y^M = \mathbb{1}. \end{aligned} \tag{B3}$$

Note that this transformation from projectors to unitaries is reversible. The inverse operation is given by

$$A_{a|x} = \frac{1}{N}\sum_{a'=0}^{N-1} \omega_N^{aa'} A_x^{a'}, \tag{B4}$$

$$B_{b|y} = \frac{1}{N}\sum_{b'=0}^{M-1} \omega_M^{bb'} B_y^{b'}. \tag{B5}$$

Now consider the set $\mathcal{A}$ of inequivalent sequences of products of elements in $\{A_x\}_x$, that is, monomials that are not equivalent under Eqs. (B3). Define then an infinite-dimensional, countable Hilbert space $\mathcal{H}_A$ with a canonical orthonormal basis whose elements are labeled by monomials of $A_1, \ldots, A_n$. That is,

$$\mathcal{H}_A = \overline{\text{span}}\{|a\rangle \colon a \in \mathcal{A}\}, \tag{B6}$$

with $\langle a|a'\rangle = \delta_{a,a'}$.

Define now the operators $\{\pi_A(A_x)\}_x \in B(\mathcal{H}_A)$ through their action on this orthonormal basis as follows:

$$\pi_A(A_x)|a\rangle = |A_x a\rangle \quad \forall\, a \in \mathcal{A}. \tag{B7}$$

For each $x$, $\pi_A(A_x)$ is a unitary operator satisfying $\pi(A_x)^N = \mathbb{1}$. The representation $\pi_A$ is known in operator algebras as the *left regular representation* of $\{A_x\}_x$ given Eqs. (B3).

Doing the analogous construction from Bob, we can now define the moment matrix

$$\begin{aligned} \Gamma_{ab,a'b'} &= \langle\psi|[\pi_A(a)^\dagger \pi_A(a') \otimes \pi_B(b)^\dagger \pi_B(b')]|\psi\rangle, \\ & a, a' \in \mathcal{A}, \qquad b, b' \in \mathcal{B}, \end{aligned} \tag{B8}$$

where $|\psi\rangle = |1\rangle_A \otimes |1\rangle_B$.

From the definition of the constructions, we have

$$\begin{aligned} \Gamma_{ab,a'b'} &= \langle 1|\pi_A(a)^\dagger \pi_A(a')|1\rangle\langle 1|\pi_B(b)^\dagger \pi_B(b')|1\rangle \\ &= \langle a|a'\rangle\langle b|b'\rangle \\ &= \delta_{a,a'}\delta_{b,b'}, \end{aligned} \tag{B9}$$

so $\Gamma = \mathbb{1}$, which is positive definite, and the NPA hierarchy without constraints is strictly feasible, as we wanted to show.

Note that from this construction one can also obtain a positive-definite feasible moment matrix in the usual basis of projectors. Using Eqs. (B4) and (B5), one constructs the linear transformation $C$ that takes monomials from the unitary basis to the projector basis. The desired moment matrix is then $\tilde{\Gamma} = C\Gamma C^\dagger = CC^\dagger$.

## REFERENCES


Åberg, Johan, Ranieri Nery, Cristhiano Duarte, and Rafael Chaves, 2020, "Semidefinite Tests for Quantum Network Topologies," Phys. Rev. Lett. **125**, 110505.

Abiuso, Paolo, Tamás Kriváchy, Emanuel-Cristian Boghiu, Marc-Olivier Renou, Alejandro Pozas-Kerstjens, and Antonio Acín, 2022, "Single-photon nonlocality in quantum networks," Phys. Rev. Res. **4**, L012041.

Acín, Antonio, Tobias Fritz, Anthony Leverrier, and Ana Belén Sainz, 2015, "A combinatorial approach to nonlocality and contextuality," Commun. Math. Phys. **334**, 533–628.

Acín, Antonio, Nicolas Gisin, and Benjamin Toner, 2006, "Grothendieck's constant and local models for noisy entangled quantum states," Phys. Rev. A **73**, 062105.

Acín, Antonio, Stefano Pironio, Tamás Vértesi, and Peter Wittek, 2016, "Optimal randomness certification from one entangled bit," Phys. Rev. A **93**, 040102.

Agresti, Iris, Davide Poderini, Leonardo Guerini, Michele Mancusi, Gonzalo Carvacho, Leandro Aolita, Daniel Cavalcanti, Rafael Chaves, and Fabio Sciarrino, 2020, "Experimental device-independent certified randomness generation with an instrumental causal structure," Commun. Phys. **3**, 110.

Aguilar, Edgar A., Jakub J. Borkała, Piotr Mironowicz, and Marcin Pawłowski, 2018, "Connections between Mutually Unbiased Bases and Quantum Random Access Codes," Phys. Rev. Lett. **121**, 050501.

Aharon, Nati, Serge Massar, Stefano Pironio, and Jonathan Silman, 2016, "Device-independent bit commitment based on the CHSH inequality," New J. Phys. **18**, 025014.

Ahrens, Johan, Piotr Badziąg, Marcin Pawłowski, Marek Żukowski, and Mohamed Bourennane, 2014, "Experimental Tests of Classical and Quantum Dimensionality," Phys. Rev. Lett. **112**, 140401.

Alizadeh, Farid, 1992, "Optimization over the positive-definite cone: Interior point methods and combinatorial applications," in *Advances in Optimization and Parallel Computing*, edited by Panos M. Pardalos (North-Holland, Amsterdam).

Almeida, Mafalda L., Jean-Daniel Bancal, Nicolas Brunner, Antonio Acín, Nicolas Gisin, and Stefano Pironio, 2010, "Guess Your Neighbor's Input: A Multipartite Nonlocal Game with No Quantum Advantage," Phys. Rev. Lett. **104**, 230404.

Aloy, Albert, Matteo Fadel, and Jordi Tura, 2021, "The quantum marginal problem for symmetric states: Applications to variational optimization, nonlocality and self-testing," New J. Phys. **23**, 033026.

Aloy, Albert, Jordi Tura, Flavio Baccari, Antonio Acín, Maciej Lewenstein, and Remigiusz Augusiak, 2019, "Device-Independent Witnesses of Entanglement Depth from Two-Body Correlators," Phys. Rev. Lett. **123**, 100507.

Ambainis, Andris, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani, 2002, "Dense quantum coding and quantum finite automata," J. Assoc. Comput. Mach. **49**, 496–511.

Ansanelli, Marina Maciel, 2022, "Observational equivalences between causal structures," master's thesis (Instituto de Física Teórica–São Paulo), http://hdl.handle.net/11449/234685.

Araújo, Mateus, 2023, "Comment on 'Geometry of the quantum set on no-signaling faces,' " Phys. Rev. A **107**, 036201.

Araújo, Mateus, Peter Brown, Sébastien Designolle, Carlos de Gois, and Lucas Porto, 2024, computer code `Ket.jl`, https://github.com/araujoms/Ket.jl.

Araújo, Mateus, Marcus Huber, Miguel Navascués, Matej Pivoluska, and Armin Tavakoli, 2023, "Quantum key distribution rates from semidefinite programming," Quantum **7**, 1019.

Arnon-Friedman, Rotem, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick, 2018, "Practical device-independent

quantum cryptography via entropy accumulation," Nat. Commun. **9**, 459.

Assad, Syed M., Oliver Thearle, and Ping Koy Lam, 2016, "Maximizing device-independent randomness from a Bell experiment by optimizing the measurement settings," Phys. Rev. A **94**, 012304.

Audenaert, Koenraad, and Bart De Moor, 2002, "Optimizing completely positive maps using semidefinite programming," Phys. Rev. A **65**, 030302.

Audenaert, Koenraad, Martin B. Plenio, and Jens Eisert, 2003, "Entanglement Cost under Positive-Partial-Transpose-Preserving Operations," Phys. Rev. Lett. **90**, 027901.

Augusiak, Remigiusz, Maciej Demianowicz, and Antonio Acín, 2014, "Local hidden-variable models for entangled quantum states," J. Phys. A **47**, 424002.

Augusiak, Remigiusz, Alexia Salavrakos, Jordi Tura, and Antonio Acín, 2019, "Bell inequalities tailored to the Greenberger-Horne-Zeilinger states of arbitrary local dimension," New J. Phys. **21**, 113001.

Baccari, Flavio, Remigiusz Augusiak, Ivan Šupić, Jordi Tura, and Antonio Acín, 2020, "Scalable Bell Inequalities for Qubit Graph States and Robust Self-Testing," Phys. Rev. Lett. **124**, 020402.

Baccari, Flavio, Daniel Cavalcanti, Peter Wittek, and Antonio Acín, 2017, "Efficient Device-Independent Entanglement Detection for Multipartite Systems," Phys. Rev. X **7**, 021042.

Bachoc, Christine, Dion C. Gijswijt, Alexander Schrijver, and Frank Vallentin, 2011, "Invariant semidefinite programs," in *Handbook on Semidefinite, Conic and Polynomial Optimization*, International Series in Operations Research & Management Science Vol. 166, edited by Miguel F. Anjos and Jean B. Lasserre (Springer, New York), pp. 219–269, 10.1007/978-1-4614-0769-0_9.

Bacon, Dave, Isaac L. Chuang, and Aram W. Harrow, 2007, "The quantum Schur transform: I. Efficient qudit circuits," in *Proceedings of the 18th annual ACM-SIAM Symposium on Discrete Algorithms (SODA), New Orleans, 2007*, edited by Harold Gabow (Association for Computing Machinery, New York), pp. 1235–1244 [arXiv:quant-ph/0601001].

Bae, Joonwoo, Dariusz Chruściński, and Marco Piani, 2019, "More Entanglement Implies Higher Performance in Channel Discrimination Tasks," Phys. Rev. Lett. **122**, 140404.

Bamps, Cédric, and Stefano Pironio, 2015, "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.

Bancal, Jean-Daniel, and Nicolas Gisin, 2021, "Nonlocal boxes for networks," Phys. Rev. A **104**, 052212.

Bancal, Jean-Daniel, Nicolas Gisin, Yeong-Cherng Liang, and Stefano Pironio, 2011, "Device-Independent Witnesses of Genuine Multipartite Entanglement," Phys. Rev. Lett. **106**, 250404.

Bancal, Jean-Daniel, Miguel Navascués, Valerio Scarani, Tamás Vértesi, and Tzyh Haur Yang, 2015, "Physical characterization of quantum devices from nonlocal correlations," Phys. Rev. A **91**, 022115.

Bancal, Jean-Daniel, and Valerio Scarani, 2014, "More randomness from noisy sources," in *Proceedings of the 9th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2014), Singapore, 2014*, Leibniz International Proceedings in Informatics (LIPIcs) Vol. 27, edited by Steven T. Flammia and Aram W. Harrow (Schloss Dagstuhl—Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany), pp. 1–6, 10.4230/LIPIcs.TQC.2014.1.

Bancal, Jean-Daniel, Lana Sheridan, and Valerio Scarani, 2014, "More randomness from the same data," New J. Phys. **16**, 033011.

Bandyopadhyay, Somshubhro, 2011, "More Nonlocality with Less Purity," Phys. Rev. Lett. **106**, 210402.

Bandyopadhyay, Somshubhro, Alessandro Cosentino, Nathaniel Johnston, Vincent Russo, John Watrous, and Nengkun Yu, 2015, "Limitations on separable measurements by convex optimization," IEEE Trans. Inf. Theory **61**, 3593–3604.

Bandyopadhyay, Somshubhro, Rahul Jain, Jonathan Oppenheim, and Christopher Perry, 2014, "Conclusive exclusion of quantum states," Phys. Rev. A **89**, 022336.

Barizien, Victor, Pavel Sekatski, and Jean-Daniel Bancal, 2024, "Custom Bell inequalities from formal sums of squares," Quantum **8**, 1333.

Barman, Siddharth, and Omar Fawzi, 2016, "Algorithmic aspects of optimal channel coding," in *Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT 2016), Barcelona, 2016* (IEEE, New York), pp. 905–909, 10.1109/ISIT.2016.7541430.

Barthel, Thomas, and Robert Hübener, 2012, "Solving Condensed-Matter Ground-State Problems by Semidefinite Relaxations," Phys. Rev. Lett. **108**, 200404.

Baumgratz, Tillmann, and Martin B. Plenio, 2012, "Lower bounds for ground states of condensed matter systems," New J. Phys. **14**, 023027.

Bäuml, Stefan, Siddhartha Das, and Mark M. Wilde, 2018, "Fundamental Limits on the Capacities of Bipartite Quantum Interactions," Phys. Rev. Lett. **121**, 250504.

Bavaresco, Jessica, Marco Túlio Quintino, Leonardo Guerini, Thiago O. Maciel, Daniel Cavalcanti, and Marcelo Terra Cunha, 2017, "Most incompatible measurements for robust steering tests," Phys. Rev. A **96**, 022110.

Bavaresco, Jessica, Natalia Herrera Valencia, Claude Klöckl, Matej Pivoluska, Paul Erker, Nicolai Friis, Mehul Malik, and Marcus Huber, 2018, "Measurements in two bases are sufficient for certifying high-dimensional entanglement," Nat. Phys. **14**, 1032–1037.

Beigi, Salman, 2010, "Entanglement-assisted zero-error capacity is upper-bounded by the Lovász $\vartheta$ function," Phys. Rev. A **82**, 010303.

Beigi, Salman, 2021, "Separation of quantum, spatial quantum, and approximate quantum correlations," Quantum **5**, 389.

Beigi, Salman, and Marc-Olivier Renou, 2022, "Covariance decomposition as a universal limit on correlations in networks," IEEE Trans. Inf. Theory **68**, 384–394.

Beigi, Salman, and Peter W. Shor, 2007, "On the complexity of computing zero-error and Holevo capacity of quantum channels," arXiv:0709.2090.

Bell, John S., 1964, "On the Einstein Podolsky Rosen paradox," Phys. Phys. Fiz. **1**, 195–200.

Bell, John S., 1966, "On the problem of hidden variables in quantum mechanics," Rev. Mod. Phys. **38**, 447–452.

Bell, John S., 1975, Ed., "The theory of local beables," in *Speakable and Unspeakable in Quantum Mechanics*, edited by Simon Capelin (Cambridge University Press, Cambridge, England), Chap. 7, pp. 52–62, 10.1017/CBO9780511815676.009.

Bene, Erika, and Tamás Vértesi, 2018, "Measurement incompatibility does not give rise to Bell violation in general," New J. Phys. **20**, 013021.

Bennett, Charles H., Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher, 1996, "Concentrating partial entanglement by local operations," Phys. Rev. A **53**, 2046–2052.

Bennett, Charles H., Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters, 1993, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," Phys. Rev. Lett. **70**, 1895–1899.

Bennett, Charles H., Igor Devetak, Aram W. Harrow, Peter W. Shor, and Andreas Winter, 2014, "The quantum reverse Shannon theorem and resource tradeoffs for simulating quantum channels," IEEE Trans. Inf. Theory **60**, 2926–2959.

Bennett, Charles H., David P. DiVincenzo, and John A. Smolin, 1997, "Capacities of Quantum Erasure Channels," Phys. Rev. Lett. **78**, 3217–3220.

Bennett, Charles H., David P. DiVincenzo, John A. Smolin, and William K. Wootters, 1996, "Mixed-state entanglement and quantum error correction," Phys. Rev. A **54**, 3824–3851.

Bennett, Charles H., Aram W. Harrow, Debbie W. Leung, and John A. Smolin, 2003, "On the capacities of bipartite Hamiltonians and unitary gates," IEEE Trans. Inf. Theory **49**, 1895–1911.

Bennett, Charles H., Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal, 1999, "Entanglement-Assisted Classical Capacity of Noisy Quantum Channels," Phys. Rev. Lett. **83**, 3081–3084.

Bennett, Charles H., Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal, 2002, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," IEEE Trans. Inf. Theory **48**, 2637–2655.

Bennett, Charles H., and Stephen J. Wiesner, 1992, "Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States," Phys. Rev. Lett. **69**, 2881–2884.

Bermejo Morán, Moisés, Alejandro Pozas-Kerstjens, and Felix Huber, 2023, "Bell Inequalities with Overlapping Measurements," Phys. Rev. Lett. **131**, 080201.

Bernards, Fabian, and Otfried Gühne, 2020, "Generalizing Optimal Bell Inequalities," Phys. Rev. Lett. **125**, 200401.

Berta, Mario, Francesco Borderi, Omar Fawzi, and Volkher B. Scholz, 2022, "Semidefinite programming hierarchies for constrained bilinear optimization," Math. Program. **194**, 781–829.

Berta, Mario, Matthias Christandl, and Renato Renner, 2011, "The quantum reverse Shannon theorem based on one-shot information theory," Commun. Math. Phys. **306**, 579–615.

Berta, Mario, Omar Fawzi, and Volkher B. Scholz, 2015, "Semidefinite programs for randomness extractors," in *Proceedings of the 10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015), Brussels, 2015*, edited by Salman Beigi and Robert König (Schloss Dagstuhl—Leibniz-Zentrum für Informatik, Dagstuhl, Germany), pp. 73–91, 10.4230/LIPIcs.TQC.2015.73.

Berta, Mario, Omar Fawzi, and Volkher B. Scholz, 2016, "Quantum bilinear optimization," SIAM J. Optim. **26**, 1529–1564.

Bertsimas, Dimitris, and Ioana Popescu, 2005, "Optimal inequalities in probability theory: A convex optimization approach," SIAM J. Optim. **15**, 780–804.

Bharti, Kishor, Maharshi Ray, Antonios Varvitsiotis, Naqueeb Ahmad Warsi, Adán Cabello, and Leong-Chuan Kwek, 2019, "Robust Self-Testing of Quantum Systems via Noncontextuality Inequalities," Phys. Rev. Lett. **122**, 250403.

Bischof, Felix, Hermann Kampermann, and Dagmar Bruß, 2019, "Resource Theory of Coherence Based on Positive-Operator-Valued Measures," Phys. Rev. Lett. **123**, 110402.

Boghiu, Emanuel-Cristian, Flavien Hirsch, Pei-Sheng Lin, Marco Túlio Quintino, and Joseph Bowles, 2023, "Device-independent and semi-device-independent entanglement certification in broadcast Bell scenarios," SciPost Phys. Core **6**, 028.

Boghiu, Emanuel-Cristian, Elie Wolfe, and Alejandro Pozas-Kerstjens, 2023, "`Inflation`: A `Python` library for classical and quantum causal compatibility," Quantum **7**, 996, https://github.com/ecboghiu/inflation.

Bohnet-Waldraff, Fabian, Daniel Braun, and Olivier Giraud, 2017, "Entanglement and the truncated moment problem," Phys. Rev. A **96**, 032312.

Bohr Brask, Jonatan, Anthony Martin, William Esposito, Raphael Houlmann, Joseph Bowles, Hugo Zbinden, and Nicolas Brunner, 2017, "Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination," Phys. Rev. Appl. **7**, 054018.

Bomze, Immanuel M., Francesco Rinaldi, and Damiano Zeffiro, 2021, "Frank-Wolfe and friends: A journey into projection-free first-order optimization methods," 4OR **19**, 313–345.

Boreiri, Sadra, Antoine Girardin, Bora Ulu, Patryk Lipka-Bartosik, Nicolas Brunner, and Pavel Sekatski, 2023, "Towards a minimal example of quantum nonlocality without inputs," Phys. Rev. A **107**, 062413.

Bourennane, Mohamed, Manfred Eibl, Christian Kurtsiefer, Sascha Gaertner, Harald Weinfurter, Otfried Gühne, Philipp Hyllus, Dagmar Bruß, Maciej Lewenstein, and Anna Sanpera, 2004, "Experimental Detection of Multipartite Entanglement Using Witness Operators," Phys. Rev. Lett. **92**, 087902.

Bowles, Joseph, Flavio Baccari, and Alexia Salavrakos, 2020, "Bounding sets of sequential quantum correlations and device-independent randomness certification," Quantum **4**, 344.

Bowles, Joseph, Flavien Hirsch, and Daniel Cavalcanti, 2021, "Single-copy activation of Bell nonlocality via broadcasting of quantum states," Quantum **5**, 499.

Bowles, Joseph, Marco Túlio Quintino, and Nicolas Brunner, 2014, "Certifying the Dimension of Classical and Quantum Systems in a Prepare-and-Measure Scenario with Independent Devices," Phys. Rev. Lett. **112**, 140407.

Bowles, Joseph, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín, 2018, "Device-Independent Entanglement Certification of All Entangled States," Phys. Rev. Lett. **121**, 180503.

Boyd, Stephen, and Lieven Vandenberghe, 2004, *Convex Optimization* (Cambridge University Press, Cambridge, England).

Branciard, Cyril, 2011, "Detection loophole in Bell experiments: How postselection modifies the requirements to observe nonlocality," Phys. Rev. A **83**, 032123.

Branciard, Cyril, Nicolas Gisin, and Stefano Pironio, 2010, "Characterizing the Nonlocal Correlations Created via Entanglement Swapping," Phys. Rev. Lett. **104**, 170401.

Branciard, Cyril, Denis Rosset, Nicolas Gisin, and Stefano Pironio, 2012, "Bilocal versus nonbilocal correlations in entanglement-swapping experiments," Phys. Rev. A **85**, 032119.

Brandão, Fernando G. S. L., 2005, "Quantifying entanglement with witness operators," Phys. Rev. A **72**, 022310.

Brandão, Fernando G. S. L., Matthias Christandl, and Jon Yard, 2011, "Faithful squashed entanglement," Commun. Math. Phys. **306**, 805.

Brandão, Fernando G. S. L., and Reinaldo O. Vianna, 2004a, "Robust semidefinite programming approach to the separability problem," Phys. Rev. A **70**, 062309.

Brandão, Fernando G. S. L., and Reinaldo O. Vianna, 2004b, "Separable Multipartite Mixed States: Operational Asymptotically Necessary and Sufficient Conditions," Phys. Rev. Lett. **93**, 220503.

Brassard, Gilles, 2003, "Quantum communication complexity," Found. Phys. **33**, 1593–1616.

Brassard, Gilles, Harry Buhrman, Noah Linden, André Allan Méthot, Alain Tapp, and Falk Unger, 2006, "Limit on Nonlocality in Any World in Which Communication Complexity is Not Trivial," Phys. Rev. Lett. **96**, 250401.

Braunstein, Samuel L., Alfred Mann, and Michael Revzen, 1992, "Maximal Violation of Bell Inequalities for Mixed States," Phys. Rev. Lett. **68**, 3259–3261.

Brierley, Stephen, Miguel Navascués, and Tamás Vértesi, 2017, "Convex separation from convex optimization for large-scale problems," arXiv:1609.05011.

Brierley, Stephen, and Stefan Weigert, 2010, "Mutually unbiased bases and semi-definite programming," J. Phys. Conf. Ser. **254**, 012008.

Brown, Peter, Hamza Fawzi, and Omar Fawzi, 2021, "Computing conditional entropies for quantum correlations," Nat. Commun. **12**, 1–12.

Brown, Peter, Hamza Fawzi, and Omar Fawzi, 2024, "Device-independent lower bounds on the conditional von Neumann entropy," Quantum **8**, 1445.

Brown, Peter J., Sammy Ragy, and Roger Colbeck, 2020, "A framework for quantum-secure device-independent randomness expansion," IEEE Trans. Inf. Theory **66**, 2964–2987.

Brunner, Nicolas, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner, 2014, "Bell nonlocality," Rev. Mod. Phys. **86**, 419–478.

Brunner, Nicolas, Miguel Navascués, and Tamás Vértesi, 2013, "Dimension Witnesses and Quantum State Discrimination," Phys. Rev. Lett. **110**, 150501.

Budroni, Costantino, Adán Cabello, Otfried Gühne, Matthias Kleinmann, and Jan-Åke Larsson, 2022, "Kochen-Specker contextuality," Rev. Mod. Phys. **94**, 045007.

Buhrman, Harry, Richard Cleve, Serge Massar, and Ronald de Wolf, 2010, "Nonlocality and communication complexity," Rev. Mod. Phys. **82**, 665–698.

Bunandar, Darius, Luke C. G. Govia, Hari Krovi, and Dirk Englund, 2020, "Numerical finite-key analysis of quantum key distribution," npj Quantum Inf. **6**, 104.

Burgdorf, Sabine, and Igor Klep, 2012, "The truncated tracial moment problem," J. Oper. Theory **68**, 141–163, http://www.mathjournals.org/jot/2012-068-001/2012-068-001-007.html.

Cabello, Adán, Simone Severini, and Andreas Winter, 2014, "Graph-Theoretic Approach to Quantum Correlations," Phys. Rev. Lett. **112**, 040401.

Cafuta, Kristijan, Igor Klep, and Janez Povh, 2012, "Constrained polynomial optimization problems with noncommuting variables," SIAM J. Optim. **22**, 363–383, https://ncsostools.fis.unm.si.

Candès, Emmanuel J., and Terence Tao, 2010, "The power of convex relaxation: Near-optimal matrix completion," IEEE Trans. Inf. Theory **56**, 2053–2080.

Carmeli, Claudio, Teiko Heinosaari, and Alessandro Toigo, 2018, "State discrimination with postmeasurement information and incompatibility of quantum measurements," Phys. Rev. A **98**, 012126.

Carmeli, Claudio, Teiko Heinosaari, and Alessandro Toigo, 2019, "Quantum Incompatibility Witnesses," Phys. Rev. Lett. **122**, 130402.

Cavalcanti, Daniel, Mafalda L. Almeida, Valerio Scarani, and Antonio Acín, 2011, "Quantum networks reveal quantum nonlocality," Nat. Commun. **2**, 184.

Cavalcanti, Daniel, Leonardo Guerini, Rafael Rabelo, and Paul Skrzypczyk, 2016, "General Method for Constructing Local Hidden Variable Models for Entangled Quantum States," Phys. Rev. Lett. **117**, 190401.

Cavalcanti, Daniel, Alejo Salles, and Valerio Scarani, 2010, "Macroscopically local correlations can violate Information Causality," Nat. Commun. **1**, 136.

Cavalcanti, Daniel, and Paul Skrzypczyk, 2016, "Quantitative relations between measurement incompatibility, quantum steering, and nonlocality," Phys. Rev. A **93**, 052112.

Cavalcanti, Daniel, and Paul Skrzypczyk, 2017, "Quantum steering: A review with focus on semidefinite programming," Rep. Prog. Phys. **80**, 024001.

Cavalcanti, Daniel, Paul Skrzypczyk, and Ivan Šupić, 2017, "All Entangled States Can Demonstrate Nonclassical Teleportation," Phys. Rev. Lett. **119**, 110501.

Chaturvedi, Anubhav, Máté Farkas, and Victoria J. Wright, 2021, "Characterising and bounding the set of quantum behaviours in contextuality scenarios," Quantum **5**, 484.

Chaturvedi, Anubhav, Marcin Pawłowski, and Debashis Saha, 2021, "Quantum description of reality is empirically incomplete," arXiv:2110.13124.

Chaturvedi, Anubhav, and Debashis Saha, 2020, "Quantum prescriptions are more ontologically distinct than they are operationally distinguishable," Quantum **4**, 345.

Chen, Shin-Liang, Costantino Budroni, Yeong-Cherng Liang, and Yueh-Nan Chen, 2016, "Natural Framework for Device-Independent Quantification of Quantum Steerability, Measurement Incompatibility, and Self-Testing," Phys. Rev. Lett. **116**, 240401.

Chen, Shin-Liang, Costantino Budroni, Yeong-Cherng Liang, and Yueh-Nan Chen, 2018, "Exploring the framework of assemblage moment matrices and its applications in device-independent characterizations," Phys. Rev. A **98**, 042127.

Chen, Shin-Liang, Nikolai Miklin, Costantino Budroni, and Yueh-Nan Chen, 2021, "Device-independent quantification of measurement incompatibility," Phys. Rev. Res. **3**, 023143.

Chiribella, Giulio, Giacomo Mauro D'Ariano, and Paolo Perinotti, 2008, "Transforming quantum operations: Quantum supermaps," Europhys. Lett. **83**, 30004.

Chitambar, Eric, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter, 2014, "Everything you always wanted to know about LOCC (but were afraid to ask)," Commun. Math. Phys. **328**, 303–326.

Choi, Man-Duen, 1975, "Completely positive linear maps on complex matrices," Linear Algebra Appl. **10**, 285–290.

Christandl, Matthias, and Andreas Winter, 2004, "Squashed entanglement: An additive entanglement measure," J. Math. Phys. (N.Y.) **45**, 829–840.

Clauser, John F., Michael A. Horne, Abner Shimony, and Richard A. Holt, 1969, "Proposed Experiment to Test Local Hidden-Variable Theories," Phys. Rev. Lett. **23**, 880–884.

Clivaz, Fabien, Marcus Huber, Ludovico Lami, and Gláucia Murta, 2017, "Genuine-multipartite entanglement criteria based on positive maps," J. Math. Phys. (N.Y.) **58**, 082201.

Coey, Chris, Lea Kapelevich, and Juan Pablo Vielma, 2022, "Solving natural conic formulations with `Hypatia.jl`," INFORMS J. Comput. **34**, 2686–2699, https://github.com/chriscoey/Hypatia.jl.

Coey, Chris, Lea Kapelevich, and Juan Pablo Vielma, 2023, "Performance enhancements for a generic conic interior point algorithm," Math. Program. Comput. **15**, 53–101.

Coiteux-Roy, Xavier, Elie Wolfe, and Marc-Olivier Renou, 2021a, "Any physical theory of nature must be boundlessly multipartite nonlocal," Phys. Rev. A **104**, 052207.

Coiteux-Roy, Xavier, Elie Wolfe, and Marc-Olivier Renou, 2021b, "No Bipartite-Nonlocal Causal Theory Can Explain Nature's Correlations," Phys. Rev. Lett. **127**, 200401.

Coladangelo, Andrea, and Jalex Stark, 2020, "An inherently infinite-dimensional quantum correlation," Nat. Commun. **11**, 3335.

Coles, Patrick J., Eric M. Metodiev, and Norbert Lütkenhaus, 2016, "Numerical approach for unstructured quantum key distribution," Nat. Commun. **7**, 11712.

Collins, Daniel, and Nicolas Gisin, 2004, "A relevant two qubit Bell inequality inequivalent to the CHSH inequality," J. Phys. A **37**, 1775.

Collins, Daniel, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu, 2002, "Bell Inequalities for Arbitrarily High-Dimensional Systems," Phys. Rev. Lett. **88**, 040404.

Colomer, Maria Prat, Luke Mortimer, Irénée Frérot, Máté Farkas, and Antonio Acín, 2022, "Three numerical approaches to find mutually unbiased bases using Bell inequalities," Quantum **6**, 778.

Cope, Thomas, 2021, "The binary-outcome detection loophole," New J. Phys. **23**, 073032.

Cosentino, Alessandro, 2013, "Positive-partial-transpose-indistinguishable states via semidefinite programming," Phys. Rev. A **87**, 012321.

Cosentino, Alessandro, and Vincent Russo, 2014, "Small sets of locally indistinguishable orthogonal maximally entangled states," Quantum Inf. Comput. **14**, 1098–1106.

Cubitt, Toby S., Debbie Leung, William Matthews, and Andreas Winter, 2010, "Improving Zero-Error Classical Communication with Entanglement," Phys. Rev. Lett. **104**, 230503.

Cubitt, Toby S., Debbie Leung, William Matthews, and Andreas Winter, 2011, "Zero-error channel capacity and simulation assisted by non-local correlations," IEEE Trans. Inf. Theory **57**, 5509–5523.

Curchod, Florian J., Markus Johansson, Remigiusz Augusiak, Matty J. Hoban, Peter Wittek, and Antonio Acín, 2017, "Unbounded randomness certification using sequences of measurements," Phys. Rev. A **95**, 020102.

D'Ariano, Giacomo Mauro, Paoloplacido Lo Presti, and Paolo Perinotti, 2005, "Classical randomness in quantum measurements," J. Phys. A **38**, 5979.

Das, Siddhartha, Stefan Bäuml, and Mark M. Wilde, 2020, "Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices," Phys. Rev. A **101**, 012344.

da Silva, Rafael A., and Breno Marques, 2023, "Semidefinite-programming-based optimization of quantum random access codes over noisy channels," Phys. Rev. A **107**, 042433.

Davis, Philip J., and Philip Rabinowitz, 1984, *Methods of Numerical Integration* (Courier Corporation, North Chelmsford, MA), 10.1016/C2013-0-10566-1.

de Gois, Carlos, George Moreno, Ranieri Nery, Samuraí Brito, Rafael Chaves, and Rafael Rabelo, 2021, "General method for classicality certification in the prepare and measure scenario," PRX Quantum **2**, 030311.

de Gois, Carlos, Martin Plávala, René Schwonnek, and Otfried Gühne, 2023, "Complete Hierarchy for High-Dimensional Steering Certification," Phys. Rev. Lett. **131**, 010201.

de Klerk, Etienne, 2002, *Aspects of Semidefinite Programming*, Applied Optimization Vol. 65 (Springer, New York), 10.1007/b105286.

de Klerk, Etienne, Cristian Dobre, and Dmitrii V. Pasechnik, 2011, "Numerical block diagonalization of matrix *-algebras with application to semidefinite programming," Math. Program. **129**, 91–111.

Designolle, Sébastien, Gabriele Iommazzo, Mathieu Besançon, Sebastian Knebel, Patrick Gelß, and Sebastian Pokutta, 2023, "Improved local models and new Bell inequalities via Frank-Wolfe algorithms," Phys. Rev. Res. **5**, 043059.

Designolle, Sébastien, Roope Uola, Kimmo Luoma, and Nicolas Brunner, 2021, "Set Coherence: Basis-Independent Quantification of Quantum Coherence," Phys. Rev. Lett. **126**, 220404.

Devetak, Igor, 2005, "The private classical capacity and quantum capacity of a quantum channel," IEEE Trans. Inf. Theory **51**, 44–55.

Devetak, Igor, and Andreas Winter, 2005, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A **461**, 207–235.

de Vicente, Julio I., 2017, "Shared randomness and device-independent dimension witnessing," Phys. Rev. A **95**, 012340.

Diamond, Steven, and Stephen Boyd, 2016, "`cvxpy`: A `Python`-embedded modeling language for convex optimization," J. Mach. Learn. Res. **17**, 1–5, https://dl.acm.org/doi/10.5555/2946645.3007036, https://www.cvxpy.org.

Dieks, Dennis, 1982, "Communication by EPR devices," Phys. Lett. **92A**, 271–272.

Ding, Dawei, Sumeet Khatri, Yihui Quek, Peter W. Shor, Xin Wang, and Mark M. Wilde, 2023, "Bounding the forward classical capacity of bipartite quantum channels," IEEE Trans. Inf. Theory **69**, 3034–3061.

Diviánszky, Péter, István Márton, Erika Bene, and Tamás Vértesi, 2023, "Certification of qubits in the prepare-and-measure scenario with large input alphabet and connections with the Grothendieck constant," Sci. Rep. **13**, 13200.

Doda, Mirdit, Marcus Huber, Gláucia Murta, Matej Pivoluska, Martin Plesch, and Chrysoula Vlachou, 2021, "Quantum Key Distribution Overcoming Extreme Noise: Simultaneous Subspace Coding Using High-Dimensional Entanglement," Phys. Rev. Appl. **15**, 034003.

Doherty, Andrew C., Yeong-Cherng Liang, Ben Toner, and Stephanie Wehner, 2008, "The quantum moment problem and bounds on entangled multi-prover games," in *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity, College Park, MD, 2008* (IEEE, New York), pp. 199–210, 10.1109/CCC.2008.26.

Doherty, Andrew C., Pablo A. Parrilo, and Federico M. Spedalieri, 2002, "Distinguishing Separable and Entangled States," Phys. Rev. Lett. **88**, 187904.

Doherty, Andrew C., Pablo A. Parrilo, and Federico M. Spedalieri, 2004, "Complete family of separability criteria," Phys. Rev. A **69**, 022308.

Doherty, Andrew C., Pablo A. Parrilo, and Federico M. Spedalieri, 2005, "Detecting multipartite entanglement," Phys. Rev. A **71**, 032333.

Donald, Matthew J., Michał Horodecki, and Oliver Rudolph, 2002, "The uniqueness theorem for entanglement measures," J. Math. Phys. (N.Y.) **43**, 4252–4272.

Drusvyatskiy, Dmitriy, and Henry Wolkowicz, 2017, "The many faces of degeneracy in conic optimization," Found. Trends Optim. **3**, 77–170.

Duan, Runyao, Simone Severini, and Andreas Winter, 2013, "Zero-error communication via quantum channels, noncommutative graphs, and a quantum Lovász number," IEEE Trans. Inf. Theory **59**, 1164–1174.

Duan, Runyao, and Andreas Winter, 2016, "No-signalling-assisted zero-error capacity of quantum channels and an information theoretic interpretation of the Lovász number," IEEE Trans. Inf. Theory **62**, 891–914.

Dupuis, Frederic, Omar Fawzi, and Renato Renner, 2020, "Entropy accumulation," Commun. Math. Phys. **379**, 867–913.

Ebler, Daniel, Michał Horodecki, Marcin Marciniak, Tomasz Młynik, Marco Túlio Quintino, and Michał Studziński, 2023, "Optimal universal quantum circuits for unitary complex conjugation," IEEE Trans. Inf. Theory **69**, 5069–5082.

Einstein, Albert, Boris Podolsky, and Nathan Rosen, 1935, "Can quantum-mechanical description of physical reality be considered complete?," Phys. Rev. **47**, 777–780.

Eisert, Jens, Philipp Hyllus, Otfried Gühne, and Marcos Curty, 2004, "Complete hierarchies of efficient approximations to problems in entanglement theory," Phys. Rev. A **70**, 062317.

Ekert, Artur K., 1991, "Quantum Cryptography Based on Bell's Theorem," Phys. Rev. Lett. **67**, 661–663.

Epping, Michael, Hermann Kampermann, and Dagmar Bruß, 2013, "Designing Bell Inequalities from a Tsirelson Bound," Phys. Rev. Lett. **111**, 240404.

Fadel, Matteo, and Jordi Tura, 2017, "Bounding the Set of Classical Correlations of a Many-Body System," Phys. Rev. Lett. **119**, 230402.

Fang, Kun, and Hamza Fawzi, 2021a, "Geometric Rényi divergence and its applications in quantum channel capacities," Commun. Math. Phys. **384**, 1615–1677.

Fang, Kun, and Hamza Fawzi, 2021b, "The sum-of-squares hierarchy on the sphere and applications in quantum information theory," Math. Program. **190**, 331–360.

Fang, Kun, Xin Wang, Marco Tomamichel, and Runyao Duan, 2019, "Non-asymptotic entanglement distillation," IEEE Trans. Inf. Theory **65**, 6454–6465.

Farkas, Máté, and Jędrzej Kaniewski, 2019, "Self-testing mutually unbiased bases in the prepare-and-measure scenario," Phys. Rev. A **99**, 032316.

Fawzi, Hamza, 2021, "The set of separable states has no finite semidefinite representation except in dimension $3 \times 2$," Commun. Math. Phys. **386**, 1319–1335.

Fawzi, Hamza, and Omar Fawzi, 2018, "Efficient optimization of the quantum relative entropy," J. Phys. A **51**, 154003.

Fawzi, Hamza, and Omar Fawzi, 2021, "Defining quantum divergences via convex optimization," Quantum **5**, 387.

Fawzi, Hamza, and Omar Fawzi, 2022, "Semidefinite programming lower bounds on the squashed entanglement," arXiv:2203.03394.

Fawzi, Hamza, and James Saunderson, 2017, "Lieb's concavity theorem, matrix geometric means, and semidefinite optimization," Linear Algebra Appl. **513**, 240–263.

Fawzi, Hamza, and James Saunderson, 2023, "Optimal self-concordant barriers for quantum relative entropies," SIAM J. Optim. **33**, 2858–2884.

Fawzi, Hamza, James Saunderson, and Pablo A. Parrilo, 2019, "Semidefinite approximations of the matrix logarithm," Found. Comput. Math. **19**, 259–296.

Fawzi, Omar, and Paul Fermé, 2024a, "Broadcast channel coding: Algorithmic aspects and non-signaling assistance," IEEE Trans. Inf. Theory **70**, 7563–7580.

Fawzi, Omar, and Paul Fermé, 2024b, "Multiple-access channel coding with non-signaling correlations," IEEE Trans. Inf. Theory **70**, 1693–1719.

Fawzi, Omar, Ala Shayeghi, and Hoang Ta, 2022, "A hierarchy of efficient bounds on quantum capacities exploiting symmetry," IEEE Trans. Inf. Theory **68**, 7346–7360.

Fine, Arthur, 1982, "Hidden Variables, Joint Probability, and the Bell Inequalities," Phys. Rev. Lett. **48**, 291–295.

Frank, Marguerite, and Philip Wolfe, 1956, "An algorithm for quadratic programming," Nav. Res. Logist. Q. **3**, 95–110.

Fraser, Thomas C., and Elie Wolfe, 2018, "Causal compatibility inequalities admitting quantum violations in the triangle structure," Phys. Rev. A **98**, 022113.

Frenkel, Péter E., and Mihály Weiner, 2015, "Classical information storage in an $n$-level quantum system," Commun. Math. Phys. **340**, 563–574.

Frérot, Irénée, Flavio Baccari, and Antonio Acín, 2022, "Unveiling quantum entanglement in many-body systems from partial information," PRX Quantum **3**, 010342.

Friis, Nicolai, Giuseppe Vitagliano, Mehul Malik, and Marcus Huber, 2019, "Entanglement certification from theory to experiment," Nat. Rev. Phys. **1**, 72–87.

Fritz, Tobias, A. Belén Sainz, Remigiusz Augusiak, Jonatan B. Brask, Rafael Chaves, Anthony Leverrier, and Antonio Acín, 2013, "Local Orthogonality as a multipartite principle for quantum correlations," Nat. Commun. **4**, 2263.

Froissart, M., 1981, "Constructive generalization of Bell's inequalities," Nuovo Cimento Soc. Ital. Fis. B **64**, 241–251.

Gallego, Rodrigo, Nicolas Brunner, Christopher Hadley, and Antonio Acín, 2010, "Device-Independent Tests of Classical and Quantum Dimensions," Phys. Rev. Lett. **105**, 230501.

Gallego, Rodrigo, Lars Erik Würflinger, Rafael Chaves, Antonio Acín, and Miguel Navascués, 2014, "Nonlocality in sequential correlation scenarios," New J. Phys. **16**, 033037.

Galvão, Ernesto F., 2001, "Feasible quantum communication complexity protocol," Phys. Rev. A **65**, 012318.

GAP Group, 2022, "GAP—Groups, algorithms, and programming: A system for computational discrete algebra," https://www.gap-system.org/.

Garner, Andrew J. P., and Mateus Araújo, 2024, "Introducing `MOMENT`: A toolkit for semi-definite programming with moment matrices," arXiv:2406.15559, https://github.com/ajpgarner/moment.

Gatermann, Karin, and Pablo A. Parrilo, 2004, "Symmetry groups, semidefinite programs, and sums of squares," J. Pure Appl. Algebra **192**, 95–128.

Genovese, Marco, 2005, "Research on hidden variable theories: A review of recent progresses," Phys. Rep. **413**, 319–396.

Gharibian, Sevag, 2010, "Strong NP-hardness of the quantum separability problem," Quantum Inf. Comput. **10**, 343–360.

Gharibian, Sevag, 2024, "The 7 faces of quantum NP," ACM SIGACT News **54**, 54–91.

Ghosh, Sibasish, Guruprasad Kar, Anirban Roy, and Debasis Sarkar, 2004, "Distinguishability of maximally entangled states," Phys. Rev. A **70**, 022304.

Gilbert, Elmer G., 1966, "An iterative procedure for computing the minimum of a quadratic form on a convex set," SIAM J. Control **4**, 61–80.

Gisin, Nicolas, 1984, "Quantum Measurements and Stochastic Processes," Phys. Rev. Lett. **52**, 1657–1660.

Gisin, Nicolas, Jean-Daniel Bancal, Yu Cai, Patrick Remy, Armin Tavakoli, Emmanuel Zambrini Cruzeiro, Sandu Popescu, and Nicolas Brunner, 2020, "Constraints on nonlocality in networks from no-signaling and independence," Nat. Commun. **11**, 2378.

Gisin, Nicolas, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, 2002, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195.

Gisin, Nicolas, and Rob Thew, 2007, "Quantum communication," Nat. Photonics **1**, 165–171.

Gittsovich, Oleg, Otfried Gühne, Philipp Hyllus, and Jens Eisert, 2008, "Unifying several separability conditions using the covariance matrix criterion," Phys. Rev. A **78**, 052319.

Gittsovich, Oleg, Philipp Hyllus, and Otfried Gühne, 2010, "Multiparticle covariance matrices and the impossibility of detecting graph-state entanglement with two-particle correlations," Phys. Rev. A **82**, 032306.

Goemans, Michel X., and David P. Williamson, 1995, "Improved approximation algorithms for maximum cut and satisfiability

problems using semidefinite programming," J. Assoc. Comput. Mach. **42**, 1115–1145.
Golub, Gene H., 1973, "Some modified matrix eigenvalue problems," SIAM Rev. **15**, 318–334.
Gómez, Esteban S., *et al.*, 2016, "Device-Independent Certification of a Nonprojective Qubit Measurement," Phys. Rev. Lett. **117**, 260401.
Gómez, Santiago, Alejandro Máttar, Italo Machuca, Esteban Sepúlveda Gómez, Daniel Cavalcanti, Osvaldo Jiménez Farías, Antonio Acín, and Gustavo Lima, 2019, "Experimental investigation of partially entangled states for device-independent randomness generation and self-testing protocols," Phys. Rev. A **99**, 032108.
Gondzio, Jacek, 2012, "Matrix-free interior point method," Comput. Optim. Appl. **51**, 457–480.
Gondzio, Jacek, Jacek A. Gruca, J. A. Julian Hall, Wiesław Laskowski, and Marek Żukowski, 2014, "Solving large-scale optimization problems related to Bell's theorem," J. Comput. Appl. Math. **263**, 392–404.
Gonzales-Ureta, Junior R., Ana Predojević, and Adán Cabello, 2021, "Device-independent quantum key distribution based on Bell inequalities with more than two inputs and two outputs," Phys. Rev. A **103**, 052436.
Gouveia, João, Pablo A. Parrilo, and Rekha R. Thomas, 2010, "Theta bodies for polynomial ideals," SIAM J. Optim. **20**, 2097–2118.
Gouveia, João, and Rekha R. Thomas, 2012, "Spectrahedral approximations of convex hulls of algebraic sets," in *Semidefinite Optimization and Convex Algebraic Geometry*, MOS-SIAM Series on Optimization, edited by Grigoriy Blekherman, Pablo A. Parrilo, and Rekha Thomas (Society for Industrial and Applied Mathematics, Philadelphia), Chap. 7, pp. 293–340, 10.1137/1.9781611972290.ch7.
Grandjean, Basile, Yeong-Cherng Liang, Jean-Daniel Bancal, Nicolas Brunner, and Nicolas Gisin, 2012, "Bell inequalities for three systems and arbitrarily many measurement outcomes," Phys. Rev. A **85**, 052113.
Grant, Michael, and Stephen Boyd, 2008, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, edited by V. Blondel, S. Boyd, and H. Kimura (Springer-Verlag, Berlin), pp. 95–110, 10.1007/978-1-84800-155-8_7, https://cvxr.com/cvx.
Gribling, Sander, David de Laat, and Monique Laurent, 2018, "Bounds on entanglement dimensions and quantum graph parameters via noncommutative polynomial optimization," Math. Program. **170**, 5–42.
Gribling, Sander, Monique Laurent, and Andries Steenkamp, 2022, "Bounding the separable rank via polynomial optimization," Linear Algebra Appl. **648**, 1–55.
Gribling, Sander, and Sven Polak, 2024, "Mutually unbiased bases: Polynomial optimization and symmetry," Quantum **8**, 1318.
Grinko, Dmitry, and Maris Ozols, 2022, "Linear programming with unitary-equivariant constraints," arXiv:2207.05713.
Gross, David, Yi-Kai Liu, Steven T. Flammia, Stephen Becker, and Jens Eisert, 2010, "Quantum State Tomography via Compressed Sensing," Phys. Rev. Lett. **105**, 150401.
Grothendieck, Alexander, 1953, "Résumé de la théorie métrique des produits tensoriels topologiques [Summary of the metric theory of topological tensor products]," Bol. Soc. Mat. São Paulo **8**, 1–79, https://www.revistas.usp.br/resenhasimeusp/article/download/74836/78406.
Gruca, Jacek, Wiesław Laskowski, and Marek Żukowski, Nikolai Kiesel, Witlef Wieczorek, Christian Schmid, and Harald Weinfurter, 2010, "Nonclassicality thresholds for multiqubit states: Numerical analysis," Phys. Rev. A **82**, 012118.
Gu, Xue-Mei, *et al.*, 2023, "Experimental Full Network Nonlocality with Independent Sources and Strict Locality Constraints," Phys. Rev. Lett. **130**, 190201.
Gühne, Otfried, Erkka Haapasalo, Tristan Kraft, Juha-Pekka Pellonpää, and Roope Uola, 2023, "Colloquium: Incompatible measurements in quantum information science," Rev. Mod. Phys. **95**, 011003.
Gühne, Otfried, Yuanyuan Mao, and Xiao-Dong Yu, 2021, "Geometry of Faithful Entanglement," Phys. Rev. Lett. **126**, 140503.
Gühne, Otfried, and Géza Tóth, 2009, "Entanglement detection," Phys. Rep. **474**, 1–75.
Gurvits, Leonid, 2003, "Classical deterministic complexity of Edmonds' problem and quantum entanglement," in *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing (STOC '03), San Diego, 2003* (Association for Computing Machinery, New York), Chap. 1, pp. 10–19, 10.1145/780542.780545.
Gyongyosi, László, Sandor Imre, and Hung Viet Nguyen, 2018, "A survey on quantum channel capacities," IEEE Commun. Surv. Tutor. **20**, 1149–1205.
Haapasalo, Erkka, 2015, "Robustness of incompatibility for quantum devices," J. Phys. A **48**, 255303.
Haapasalo, Erkka, Tristan Kraft, Nikolai Miklin, and Roope Uola, 2021, "Quantum marginal problem and incompatibility," Quantum **5**, 476.
Häffner, Hartmut, *et al.*, 2005, "Scalable multiparticle entanglement of trapped ions," Nature (London) **438**, 643–646.
Hahn, Thomas A., and Ernest Y.-Z. Tan, 2022, "Fidelity bounds for device-independent advantage distillation," npj Quantum Inf. **8**, 145.
Hall, William, 2007, "Compatibility of subsystem states and convex geometry," Phys. Rev. A **75**, 032102.
Hameedi, Alley, Armin Tavakoli, Breno Marques, and Mohamed Bourennane, 2017, "Communication Games Reveal Preparation Contextuality," Phys. Rev. Lett. **119**, 220402.
Hansenne, Kiara, Zhen-Peng Xu, Tristan Kraft, and Otfried Gühne, 2022, "Symmetries in quantum networks lead to no-go theorems for entanglement distribution and to verification techniques," Nat. Commun. **13**, 496.
Hanson, Eric P., Vishal Katariya, Nilanjana Datta, and Mark M. Wilde, 2022, "Guesswork with quantum side information," IEEE Trans. Inf. Theory **68**, 322–338.
Harrow, Aram W., Anand Natarajan, and Xiaodi Wu, 2017, "An improved semidefinite programming hierarchy for testing entanglement," Commun. Math. Phys. **352**, 881–904.
Hastings, Matthew B., 2009, "Superadditivity of communication capacity using entangled inputs," Nat. Phys. **5**, 255–257.
Hayashi, Masahito, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita, 2006, "$(4,1)$-quantum random access coding does not exist—One qubit is not enough to recover one of four bits," New J. Phys. **8**, 129.
Hayden, Patrick M., Michal Horodecki, and Barbara M. Terhal, 2001, "The asymptotic entanglement cost of preparing a quantum state," J. Phys. A **34**, 6891.
He, Kerry, James Saunderson, and Hamza Fawzi, 2024, "Exploiting structure in quantum relative entropy programs," arXiv:2407.00241.
Heinosaari, Teiko, Takayuki Miyadera, and Mário Ziman, 2016, "An invitation to quantum incompatibility," J. Phys. A **49**, 123001.
Heisenberg, Werner, 1925, "Über quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen [Quantum-theoretical reinterpretation of kinematic and mechanical relations]," Z. Phys. **33**, 879–893; translated in *Sources of Quantum Mechanics*, edited by B. L. van der Waerden (Dover, New York), ISBN 0-486-61881-1, pp. 261–276.

Henrion, Didier, and Andrea Garulli, 2005, Eds., *Positive Polynomials in Control*, Lecture Notes in Control and Information Sciences Vol. 312 (Springer, New York), 10.1007/b96977.

Henrion, Didier, and Jean-Bernard Lasserre, 2005, "Detecting global optimality and extracting solutions in GloptiPoly," in *Positive Polynomials in Control*, Lecture Notes in Control and Information Sciences Vol. 312, edited by Didier Henrion and Andrea Garulli (Springer, Berlin), Chap. 15, pp. 293–310, 10.1007/10997703_15.

Henrion, Didier, Jean-Bernard Lasserre, and Johan Löfberg, 2009, "GloptiPoly 3: Moments, optimization and semidefinite programming," Optim. Method Software **24**, 761–779, https://homepages.laas.fr/henrion/software/gloptipoly3.

Henson, Joe, Raymond Lal, and Matthew F. Pusey, 2014, "Theory-independent limits on correlations from generalized Bayesian networks," New J. Phys. **16**, 113043.

Hirsch, Flavien, Marco Túlio Quintino, and Nicolas Brunner, 2018, "Quantum measurement incompatibility does not imply Bell nonlocality," Phys. Rev. A **97**, 012129.

Hirsch, Flavien, Marco Túlio Quintino, Tamás Vértesi, Miguel Navascués, and Nicolas Brunner, 2017, "Better local hidden variable models for two-qubit Werner states and an upper bound on the Grothendieck constant $K_G(3)$," Quantum **1**, 3.

Hirsch, Flavien, Marco Túlio Quintino, Tamás Vértesi, Matthew F. Pusey, and Nicolas Brunner, 2016, "Algorithmic Construction of Local Hidden Variable Models for Entangled Quantum States," Phys. Rev. Lett. **117**, 190402.

Holdsworth, Tharon, Vishal Singh, and Mark M. Wilde, 2023, "Quantifying the performance of approximate teleportation and quantum error correction via symmetric 2-PPT-extendible channels," Phys. Rev. A **107**, 012428.

Holevo, Alexander S., 1973, "Bounds for the quantity of information transmitted by a quantum communication channel," Probl. Inf. Transm. **9**, 177–183, https://www.mathnet.ru/eng/ppi903.

Holevo, Alexander S., 1998, "The capacity of the quantum channel with general signal states," IEEE Trans. Inf. Theory **44**, 269–273.

Holevo, Alexander S., 2020, "Quantum channel capacities," Quantum Electron. **50**, 440.

Holevo, Alexander S., and Vittorio Giovannetti, 2012, "Quantum channels and their entropic characteristics," Rep. Prog. Phys. **75**, 046001.

Hopkins, Samuel B., Tselil Schramm, Jonathan Shi, and David Steurer, 2016, "Fast spectral algorithms from sum-of-squares proofs: Tensor decomposition and planted sparse vectors,"in *Proceedings of the Forth-Eighth Annual ACM Symposium on Theory of Computing (STOC '16), Cambridge, MA, 2016*, edited by Daniel Wichs and Yishay Mansour (Association for Computing Machinery, New York), pp. 178–191, 10.1145/2897518.2897529.

Horodecki, Michał, Paweł Horodecki, and Ryszard Horodecki, 1996, "Separability of mixed states: Necessary and sufficient conditions," Phys. Lett. A **223**, 1–8.

Horodecki, Michał, Paweł Horodecki, and Ryszard Horodecki, 1998, "Mixed-State Entanglement and Distillation: Is There a 'Bound' Entanglement in Nature?," Phys. Rev. Lett. **80**, 5239–5242.

Horodecki, Michał, Paweł Horodecki, and Ryszard Horodecki, 1999, "General teleportation channel, singlet fraction, and quasidistillation," Phys. Rev. A **60**, 1888–1898.

Horodecki, Michał, Paweł Horodecki, and Ryszard Horodecki, 2000, "Limits for Entanglement Measures," Phys. Rev. Lett. **84**, 2014–2017.

Horodecki, Michał, Aditi Sen(De), and Ujjwal Sen, 2003, "Rates of asymptotic entanglement transformations for bipartite mixed states: Maximally entangled states are not special," Phys. Rev. A **67**, 062314.

Horodecki, Ryszard, Paweł Horodecki, Michał Horodecki, and Karol Horodecki, 2009, "Quantum entanglement," Rev. Mod. Phys. **81**, 865–942.

Hsieh, Chung-Yun, Matteo Lostaglio, and Antonio Acín, 2022, "Quantum channel marginal problem," Phys. Rev. Res. **4**, 013249.

Hu, Hao, Jiyoung Im, Jie Lin, Norbert Lütkenhaus, and Henry Wolkowicz, 2022, "Robust interior point method for quantum key distribution rate computation," Quantum **6**, 792.

Hu, Xiao-Min, *et al.*, 2021, "Optimized Detection of High-Dimensional Entanglement," Phys. Rev. Lett. **127**, 220501.

Huang, Chang-Jiang, Guo-Yong Xiang, Yu Guo, Kang-Da Wu, Bi-Heng Liu, Chuan-Feng Li, Guang-Can Guo, and Armin Tavakoli, 2021, "Nonlocality, Steering, and Quantum State Tomography in a Single Experiment," Phys. Rev. Lett. **127**, 020401.

Huang, Yichen, 2014, "Computing quantum discord is NP-complete," New J. Phys. **16**, 033027.

Huber, Felix, Igor Klep, Victor Magron, and Jurij Volčič, 2022, "Dimension-free entanglement detection in multipartite Werner states," Commun. Math. Phys. **396**, 1051–1070.

Huber, Felix, and Nikolai Wyderka, 2022, "Refuting spectral compatibility of quantum marginals," arXiv:2211.06349.

Huber, Marcus, and Ritabrata Sengupta, 2014, "Witnessing Genuine Multipartite Entanglement with Positive Maps," Phys. Rev. Lett. **113**, 100501.

Hughston, Lane P., Richard Jozsa, and William K. Wootters, 1993, "A complete classification of quantum ensembles having a given density matrix," Phys. Lett. A **183**, 14–18.

Hulpke, Florian, Dagmar Bruß, Maciej Lewenstein, and Anna Sanpera, 2004, "Simplifying Schmidt number witnesses via higher-dimensional embeddings," Quantum Inf. Comput. **4**, 207–221.

Ioannou, Marie, and Denis Rosset, 2021, "Noncommutative polynomial optimization under symmetry," arXiv:2112.10803.

Ioannou, Marie, Pavel Sekatski, Alastair A. Abbott, Denis Rosset, Jean-Daniel Bancal, and Nicolas Brunner, 2022, "Receiver-device-independent quantum key distribution protocols," New J. Phys. **24**, 063006.

Ishizaka, Satoshi, 2020, "Geometrical self-testing of partially entangled two-qubit states," New J. Phys. **22**, 023022.

Ishizaka, Satoshi, and Tohya Hiroshima, 2008, "Asymptotic Teleportation Scheme as a Universal Programmable Quantum Processor," Phys. Rev. Lett. **101**, 240501.

Ishizaka, Satoshi, and Martin B. Plenio, 2005, "Multiparticle entanglement manipulation under positive partial transpose preserving operations," Phys. Rev. A **71**, 052303.

Ivanović, Igor D., 1981, "Geometrical description of quantal state determination," J. Phys. A **14**, 3241.

Jamiołkowski, Andrzej, 1972, "Linear transformations which preserve trace and positive semidefiniteness of operators," Rep. Math. Phys. **3**, 275–278.

Jee, Hyejung H., Carlo Sparaciari, Omar Fawzi, and Mario Berta, 2021, "Quasi-polynomial time algorithms for free quantum games in bounded dimension," in *48th International Colloquium on Automata, Languages, and Programming (ICALP 2021)*, Leibniz International Proceedings in Informatics (LIPIcs) Vol. 198, edited by Nikhil Bansal, Emanuela Merelli, and James Worrell (Schloss Dagstuhl—Leibniz-Zentrum für Informatik, Dagstuhl, Germany), pp. 82:1–82:20, 10.4230/LIPIcs.ICALP.2021.82.

Jennewein, Thomas, Gregor Weihs, Jian-Wei Pan, and Anton Zeilinger, 2001, "Experimental Nonlocality Proof of Quantum Teleportation and Entanglement Swapping," Phys. Rev. Lett. **88**, 017903.

Ji, Zhengfeng, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen, 2020, "MIP* = RE," arXiv:2001.04383.
Johnston, Nathaniel, 2016, computer code QETLAB, http://qetlab.com.
Johnston, Nathaniel, Benjamin Lovitz, and Aravindan Vijayaraghavan, 2022, "Complete hierarchy of linear systems for certifying quantum entanglement of subspaces," Phys. Rev. A **106**, 062443.
Jones, Caroline L., Stefan L. Ludescher, Albert Aloy, and Markus P. Mueller, 2022, "Theory-independent randomness generation with spacetime symmetries," arXiv:2210.14811.
Jungnitsch, Bastian, Tobias Moroder, and Otfried Gühne, 2011a, "Taming Multiparticle Entanglement," Phys. Rev. Lett. **106**, 190502.
Jungnitsch, Bastian, Tobias Moroder, and Otfried Gühne, 2011b, "Entanglement witnesses for graph states: General theory and examples," Phys. Rev. A **84**, 032310.
Kamath, Anil P., and Narendra K. Karmarkar, 1991, "A continuous approach to compute upper bounds in quadratic maximization problems with integer constraints," in *Recent Advances in Global Optimization*, Princeton Series in Computer Science, Christodoulos A. Floudas and Panos M. Pardalos (Princeton University Press, Princeton, NJ), pp. 125–140, 10.1515/9781400862528.125.
Kamath, Anil P., and Narendra K. Karmarkar, 1993, "An $O(nL)$ iteration algorithm for computing bounds in quadratic optimization problems," in *Complexity in Numerical Optimization*, edited by Panos M. Pardalos (World Scientific, Singapore), pp. 254–268, 10.1142/9789814354363_0012.
Kaniewski, Jędrzej, Ivan Šupić, Jordi Tura, Flavio Baccari, Alexia Salavrakos, and Remigiusz Augusiak, 2019, "Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems," Quantum **3**, 198.
Karmarkar, Narendra K., 1984, "A new polynomial-time algorithm for linear programming," Combinatorica **4**, 373–395.
Karp, Richard M., 1972, "Reducibility among combinatorial problems," in *Complexity of Computer Computations. The IBM Research Symposia Series*, edited by Raymond E. Miller, James W. Thatcher, and Jean D. Bohlinger (Springer, Boston), Chap. 9, pp. 85–103, 10.1007/978-1-4684-2001-2_9.
Kaur, Eneet, Siddhartha Das, Mark M. Wilde, and Andreas Winter, 2019, "Extendibility Limits the Performance of Quantum Processors," Phys. Rev. Lett. **123**, 070502.
Kaur, Eneet, Siddhartha Das, Mark M. Wilde, and Andreas Winter, 2021, "Resource theory of unextendibility and nonasymptotic quantum capacity," Phys. Rev. A **104**, 022401.
Kela, Aditya, Kai Von Prillwitz, Johan Åberg, Rafael Chaves, and David Gross, 2020, "Semidefinite tests for latent causal structures," IEEE Trans. Inf. Theory **66**, 339–349.
Kempe, Julia, Alexei Kitaev, and Oded Regev, 2006, "The complexity of the local Hamiltonian problem," SIAM J. Comput. **35**, 1070–1097.
Kempe, Julia, Oded Regev, and Ben Toner, 2010, "Unique games with entangled provers are easy," SIAM J. Comput. **39**, 3207–3229.
Khalfin, Leonid A., and Boris S. Tsirelson, 1985, "Quantum and quasi-classical analogs of Bell inequalities," in *Symposium on the Foundations of Modern Physics*, edited by P. Lahti and P. Mittelstaedt (World Scientific, Singapore), pp. 441–460.
King, Christopher, 2002, "Additivity for unital qubit channels," J. Math. Phys. (N.Y.) **43**, 4641–4653.
King, Christopher, 2003, "The capacity of the quantum depolarizing channel," IEEE Trans. Inf. Theory **49**, 221–229.
Kitaev, Alexei Y., Alexander H. Shen, and Mikhail N. Vyalyi, 2002, *Classical and Quantum Computation*, Graduate Studies in Mathematics Vol. 47 (American Mathematical Society, Providence), 10.1090/gsm/047.
Klep, Igor, Victor Magron, and Jurij Volčič, 2022, "Optimization over trace polynomials," Ann. Henri Poincaré **23**, 67–100.
Koashi, Masato, and Andreas Winter, 2004, "Monogamy of quantum entanglement and other correlations," Phys. Rev. A **69**, 022309.
Kochen, Simon, and Ernst Specker, 1968, "The problem of hidden variables in quantum mechanics," Indiana Univ. Math. J. **17**, 59–87, http://www.jstor.org/stable/24902153.
Kogias, Ioannis, Paul Skrzypczyk, Daniel Cavalcanti, Antonio Acín, and Gerardo Adesso, 2015, "Hierarchy of Steering Criteria Based on Moments for All Bipartite Quantum Systems," Phys. Rev. Lett. **115**, 210401.
Kondra, Tulja Varun, Chandan Datta, and Alexander Streltsov, 2023, "Real quantum operations and state transformations," New J. Phys. **25**, 093043.
König, Robert, Renato Renner, and Christian Schaffner, 2009, "The operational meaning of min- and max-entropy," IEEE Trans. Inf. Theory **55**, 4337–4347.
König, Robert, and Stephanie Wehner, 2009, "A Strong Converse for Classical Channel Coding Using Entangled Inputs," Phys. Rev. Lett. **103**, 070504.
Kraft, Tristan, Sébastien Designolle, Christina Ritz, Nicolas Brunner, Otfried Gühne, and Marcus Huber, 2021, "Quantum entanglement in the triangle network," Phys. Rev. A **103**, L060401.
Kraft, Tristan, Cornelia Spee, Xiao-Dong Yu, and Otfried Gühne, 2021, "Characterizing quantum networks: Insights from coherence theory," Phys. Rev. A **103**, 052405.
Kull, Ilya, Norbert Schuch, Ben Dive, and Miguel Navascués, 2024, "Lower Bounding Ground-State Energies of Local Hamiltonians through the Renormalization Group," Phys. Rev. X **14**, 021008.
Kundu, Srijita, Jamie Sikora, and Ernest Y.-Z. Tan, 2022, "A device-independent protocol for XOR oblivious transfer," Quantum **6**, 725.
Lami, Ludovico, and Bartosz Regula, 2023, "No second law of entanglement manipulation after all," Nat. Phys. **19**, 184–189.
Lami, Ludovico, Bartosz Regula, and Gerardo Adesso, 2019, "Generic Bound Coherence under Strictly Incoherent Operations," Phys. Rev. Lett. **122**, 150402.
Lami, Ludovico, Bartosz Regula, Xin Wang, Rosanna Nichols, Andreas Winter, and Gerardo Adesso, 2018, "Gaussian quantum resource theories," Phys. Rev. A **98**, 022335.
Lancien, Cécilia, Otfried Gühne, Ritabrata Sengupta, and Marcus Huber, 2015, "Relaxations of separability in multipartite systems: Semidefinite programs, witnesses and volumes," J. Phys. A **48**, 505302.
Landau, Lawrence J., 1988, "Empirical two-point correlation functions," Found. Phys. **18**, 449–460.
Lang, Ben, Tamás Vértesi, and Miguel Navascués, 2014, "Closed sets of correlations: Answers from the zoo," J. Phys. A **47**, 424029.
Lasserre, Jean B., 2001, "Global optimization with polynomials and the problem of moments," SIAM J. Optim. **11**, 796–817.
Lasserre, Jean B., 2007, "A sum of squares approximation of nonnegative polynomials," SIAM Rev. **49**, 651–669.
Laudisa, Federico, 2023, "How and when did locality become 'local realism'? A historical and critical analysis (1963–1978)," Stud. Hist. Philos. Sci. **97**, 44–57.
Laurent, Monique, 2009, "Sums of squares, moment matrices and optimization over polynomials," in *Emerging Applications of Algebraic Geometry*, edited by Mihai Putinar and Seth Sullivant (Springer, New York), Chap. 7, pp. 157–270, 10.1007/978-0-387-09686-5_7.

Law, Yun Zhi, Le Puc Thinh, Jean-Daniel Bancal, and Valerio Scarani, 2014, "Quantum randomness extraction for various levels of characterization of the devices," J. Phys. A **47**, 424028.

Lee, Hanwool, Kieran Flatt, Carles Roch i Carceller, Jonatan B. Brask, and Joonwoo Bae, 2022, "Maximum-confidence measurement for qubit states," Phys. Rev. A **106**, 032422.

Leibfried, Didi, *et al.*, 2005, "Creation of a six-atom 'Schrödinger cat' state," Nature (London) **438**, 639–642.

Leung, Debbie, Laura Mančinska, William Matthews, Maris Ozols, and Aidan Roy, 2012, "Entanglement can increase asymptotic rates of zero-error classical communication over classical channels," Commun. Math. Phys. **311**, 97–111.

Leung, Debbie, and William Matthews, 2015, "On the power of PPT-preserving and non-signalling codes," IEEE Trans. Inf. Theory **61**, 4486–4499.

Lewenstein, Maciej, Barbara Kraus, J. Ignacio Cirac, and Paweł Horodecki, 2000, "Optimization of entanglement witnesses," Phys. Rev. A **62**, 052310.

Li, Hong-Wei, Marcin Pawłowski, Ramij Rahaman, Guang-Can Guo, and Zheng-Fu Han, 2015, "Device- and semi–device-independent random numbers based on noninequality paradox," Phys. Rev. A **92**, 022327.

Li, Hong-Wei, Marcin Pawłowski, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Han, 2012, "Semi-device-independent randomness certification using $n \to 1$ quantum random access codes," Phys. Rev. A **85**, 052308.

Li, Hong-Wei, Zhen-Qiang Yin, Yu-Chun Wu, Xu-Bo Zou, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han, 2011, "Semi-device-independent random-number expansion without entanglement," Phys. Rev. A **84**, 034301.

Li, Mao-Sheng, Yan-Ling Wang, Shao-Ming Fei, and Zhu-Jun Zheng, 2015, "$d$ locally indistinguishable maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$," Phys. Rev. A **91**, 042318.

Li, Xinhui, Yukun Wang, Yunguang Han, Sujuan Qin, Fei Gao, and Qiaoyan Wen, 2020, "Self-testing of symmetric three-qubit states," IEEE J. Sel. Areas Commun. **38**, 589–597.

Li, Yinan, Xin Wang, and Runyao Duan, 2017, "Indistinguishability of bipartite states by positive-partial-transpose operations in the many-copy scenario," Phys. Rev. A **95**, 052346.

Liang, Yeong-Cherng, and Andrew C. Doherty, 2007, "Bounds on quantum correlations in Bell-inequality experiments," Phys. Rev. A **75**, 042103.

Liang, Yeong-Cherng, Chu-Wee Lim, and Dong-Ling Deng, 2009, "Reexamination of a multisetting Bell inequality for qudits," Phys. Rev. A **80**, 052116.

Liang, Yeong-Cherng, Denis Rosset, Jean-Daniel Bancal, Gilles Pütz, Tomer Jack Barnea, and Nicolas Gisin, 2015, "Family of Bell-like Inequalities as Device-Independent Witnesses for Entanglement Depth," Phys. Rev. Lett. **114**, 190401.

Ligthart, Laurens T., Mariami Gachechiladze, and David Gross, 2023, "A convergent inflation hierarchy for quantum causal structures," Commun. Math. Phys. **401**, 2673–2714.

Ligthart, Laurens T., and David Gross, 2023, "The inflation hierarchy and the polarization hierarchy are complete for the quantum bilocal scenario," J. Math. Phys. (N.Y.) **64**, 072201.

Lin, Pei-Sheng, Jui-Chen Hung, Ching-Hsu Chen, and Yeong-Cherng Liang, 2019, "Exploring Bell inequalities for the device-independent certification of multipartite entanglement depth," Phys. Rev. A **99**, 062338.

Lin, Pei-Sheng, Tamás Vértesi, and Yeong-Cherng Liang, 2022, "Naturally restricted subsets of nonsignaling correlations: Typicality and convergence," Quantum **6**, 765.

Linden, Noah, Sandu Popescu, Anthony J. Short, and Andreas Winter, 2007, "Quantum Nonlocality and Beyond: Limits from Nonlocal Computation," Phys. Rev. Lett. **99**, 180502.

Lipka-Bartosik, Patryk, and Paul Skrzypczyk, 2020, "Operational advantages provided by nonclassical teleportation," Phys. Rev. Res. **2**, 023029.

Liu, Yi-Kai, Matthias Christandl, and Frank Verstraete, 2007, "Quantum Computational Complexity of the $N$-Representability Problem: QMA Complete," Phys. Rev. Lett. **98**, 110503.

Lloyd, Seth, 1997, "Capacity of the noisy quantum channel," Phys. Rev. A **55**, 1613–1622.

Lo, Hoi-Kwong, Marcos Curty, and Bing Qi, 2012, "Measurement-Device-Independent Quantum Key Distribution," Phys. Rev. Lett. **108**, 130503.

Löfberg, Johan, 2004, "`YALMIP`: A toolbox for modeling and optimization in `MATLAB`," in *Proceedings of the IEEE International Symposium on Computer-Aided Control Systems Design, Taipei, 2004* (IEEE, New York), pp. 284–289, 10.1109/CACSD.2004.1393890, https://yalmip.github.io.

López-Rosa, Sheila, Zhen-Peng Xu, and Adán Cabello, 2016, "Maximum nonlocality in the $(3, 2, 2)$ scenario," Phys. Rev. A **94**, 062121.

Lorente, Andrés González, Pablo V. Parellada, Miguel Castillo-Celeita, and Mateus Araújo, 2024, "Quantum key distribution rates from non-symmetric conic optimization," arXiv:2407.00152.

Lovász, László, 1979, "On the Shannon capacity of a graph," IEEE Trans. Inf. Theory **25**, 1–7.

Lu, Chao-Yang, Xiao-Qi Zhou, Otfried Gühne, Wei-Bo Gao, Jin Zhang, Zhen-Sheng Yuan, Alexander Goebel, Tao Yang, and Jian-Wei Pan, 2007, "Experimental entanglement of six photons in graph states," Nat. Phys. **3**, 91–95.

Lubin, Miles, Oscar Dowson, Joaquim Dias Garcia, Joey Huchette, Benoît Legat, and Juan Pablo Vielma, 2023, "`JuMP 1.0`: Recent improvements to a modeling language for mathematical optimization," Math. Program. Comput. **15**, 581–589, https://jump.dev/JuMP.jl/stable.

Lucamarini, Marco, Zhiliang L. Yuan, James F. Dynes, and Andrew J. Shields, 2018, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature (London) **557**, 400–403.

Luo, Ming-Xing, 2021, "New genuinely multipartite entanglement," Adv. Quantum Technol. **4**, 2000123.

Luo, Ming-Xing, Xue Yang, and Alejandro Pozas-Kerstjens, 2024, "Hierarchical certification of non-classical network correlations," Phys. Rev. A **110**, 022617.

Markovsky, Ivan, 2012, *Low Rank Approximation: Algorithms, Implementation, Applications* (Springer, New York), 10.1007/978-1-4471-2227-2.

Martínez, Daniel, Esteban S. Gómez, Jaime Cariñe, Luciano Pereira, Aldo Delgado, Stephen P. Walborn, Armin Tavakoli, and Gustavo Lima, 2023, "Certification of a non-projective qudit measurement using multiport beamsplitters," Nat. Phys. **19**, 190–195.

Martínez, Daniel, Armin Tavakoli, Mauricio Casanova, Gustavo Cañas, Breno Marques, and Gustavo Lima, 2018, "High-Dimensional Quantum Communication Complexity beyond Strategies Based on Bell's Theorem," Phys. Rev. Lett. **121**, 150504.

Masanes, Lluís, 2003, "Necessary and sufficient condition for quantum-generated correlations," arXiv:quant-ph/0309137.

Masanes, Lluís, 2005, "Extremal quantum correlations for $N$ parties with two dichotomic observables per site," arXiv:quant-ph/0512100.

Masanes, Lluís, 2006, "Asymptotic Violation of Bell Inequalities and Distillability," Phys. Rev. Lett. **97**, 050503.

Masanes, Lluís, Stefano Pironio, and Antonio Acín, 2011, "Secure device-independent quantum key distribution with causally independent measurement devices," Nat. Commun. **2**, 238.

Masini, Michele, Stefano Pironio, and Erik Woodhead, 2022, "Simple and practical DIQKD security analysis via BB84-type uncertainty relations and Pauli correlation constraints," Quantum **6**, 843.

Matsumoto, Keiji, 2018, "A new quantum version of $f$-divergence," in *Reality and Measurement in Algebraic Quantum Theory*, edited by Masanao Ozawa, Jeremy Butterfield, Hans Halvorson, Miklós Rédei, Yuichiro Kitajima, and Francesco Buscemi (Springer, Singapore), pp. 229–273, 10.1007/978-981-13-2487-1_10.

Máttar, Alejandro, Paul Skrzypczyk, Jonatan B. Brask, Daniel Cavalcanti, and Antonio Acín, 2015, "Optimal randomness generation from optical Bell experiments," New J. Phys. **17**, 022003.

Matthews, William, 2012, "A linear program for the finite block length converse of Polyanskiy-Poor-Verdú via nonsignaling codes," IEEE Trans. Inf. Theory **58**, 7036–7044.

Matthews, William, and Stephanie Wehner, 2014, "Finite blocklength converse bounds for quantum channels," IEEE Trans. Inf. Theory **60**, 7317–7329.

Mayers, Dominic, and Andrew Yao, 1998, "Quantum cryptography with imperfect apparatus," in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280), Palo Alto, 1998* (IEEE, New York), pp. 503–509, 10.1109/SFCS.1998.743501.

Mayers, Dominic, and Andrew Yao, 2004, "Self testing quantum apparatus," Quantum Inf. Comput. **4**, 273–286.

Mazurek, Michael D., Matthew F. Pusey, Ravi Kunjwal, Kevin J. Resch, and Robert W. Spekkens, 2016, "An experimental test of noncontextuality without unphysical idealizations," Nat. Commun. **7**, 11780.

Metger, Tony, Omar Fawzi, David Sutter, and Renato Renner, 2022, "Generalised entropy accumulation," in *Proceedings of the IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS), Denver, 2022* (IEEE, New York), pp. 844–850, 10.1109/FOCS54457.2022.00085.

Mihaescu, Tatiana, Hermann Kampermann, Giulio Gianfelici, Aurelian Isar, and Dagmar Bruß, 2020, "Detecting entanglement of unknown continuous variable states with random measurements," New J. Phys. **22**, 123041.

Miklin, Nikolai, Jakub J. Borkała, and Marcin Pawłowski, 2020, "Semi-device-independent self-testing of unsharp measurements," Phys. Rev. Res. **2**, 033014.

Mikos-Nuszkiewicz, Antoni, and Jędrzej Kaniewski, 2023, "Extremal points of the quantum set in the Clauser-Horne-Shimony-Holt scenario: Conjectured analytical solution," Phys. Rev. A **108**, 012212.

Milazzo, Nadia, Daniel Braun, and Olivier Giraud, 2020, "Truncated moment sequences and a solution to the channel separability problem," Phys. Rev. A **102**, 052406.

Mironowicz, Piotr, 2024, "Semi-definite programming and quantum information," J. Phys. A **57**, 163002.

Mironowicz, Piotr, Hong-Wei Li, and Marcin Pawłowski, 2014, "Properties of dimension witnesses and their semidefinite programming relaxations," Phys. Rev. A **90**, 022322.

Mironowicz, Piotr, and Marcin Pawłowski, 2013, "Robustness of quantum-randomness expansion protocols in the presence of noise," Phys. Rev. A **88**, 032319.

Mironowicz, Piotr, and Marcin Pawłowski, 2019, "Experimentally feasible semi-device-independent certification of four-outcome positive-operator-valued measurements," Phys. Rev. A **100**, 030301.

Mironowicz, Piotr, Armin Tavakoli, Alley Hameedi, Breno Marques, Marcin Pawłowski, and Mohamed Bourennane, 2016, "Increased certification of semi-device independent random numbers using many inputs and more post-processing," New J. Phys. **18**, 065004.

Mohan, Karthik, Armin Tavakoli, and Nicolas Brunner, 2019, "Sequential random access codes and self-testing of quantum measurement instruments," New J. Phys. **21**, 083034.

Morelli, Simon, Hayata Yamasaki, Marcus Huber, and Armin Tavakoli, 2022, "Entanglement Detection with Imprecise Measurements," Phys. Rev. Lett. **128**, 250501.

Mori, Junki, 2020, "Operational characterization of incompatibility of quantum channels with quantum state discrimination," Phys. Rev. A **101**, 032331.

Moroder, Tobias, Jean-Daniel Bancal, Yeong-Cherng Liang, Martin Hofmann, and Otfried Gühne, 2013, "Device-Independent Entanglement Quantification and Related Applications," Phys. Rev. Lett. **111**, 030501.

MOSEK ApS, 2023, computer code `MOSEK`, version 10.1.11, https://docs.mosek.com/latest/intro/index.html.

Mozrzymas, Marek, Michał Studziński, and Piotr Kopszak, 2021, "Optimal multi-port-based teleportation schemes," Quantum **5**, 477.

Mozrzymas, Marek, Michał Studziński, Sergii Strelchuk, and Michał Horodecki, 2018, "Optimal port-based teleportation," New J. Phys. **20**, 053006.

Mukherjee, Kaushiki, Biswajit Paul, and Debasis Sarkar, 2015, "Correlations in $n$-local scenario," Quantum Inf. Process. **14**, 2025–2042.

Müller-Hermes, Alexander, David Reeb, and Michael M. Wolf, 2016, "Positivity of linear maps under tensor powers," J. Math. Phys. (N.Y.) **57**, 015202.

Nakata, Maho, 2010, "A numerical evaluation of highly accurate multiple-precision arithmetic version of semidefinite programming solver: SDPA-GMP, -QD and -DD," in *Proceedings of the 2010 IEEE International Symposium on Computer-Aided Control System Design, Yokohama, Japan, 2010* (IEEE, New York), pp. 29–34, 10.1109/CACSD.2010.5612693, https://github.com/nakatamaho/sdpa-gmp, https://github.com/nakatamaho/sdpa-qd, https://github.com/nakatamaho/sdpa-dd.

Nakata, Maho, Hiroshi Nakatsuji, Masahiro Ehara, Mitsuhiro Fukuda, Kazuhide Nakata, and Katsuki Fujisawa, 2001, "Variational calculations of fermion second-order reduced density matrices by semidefinite programming algorithm," J. Chem. Phys. **114**, 8282–8292.

Napoli, Carmine, Thomas R. Bromley, Marco Cianciaruso, Marco Piani, Nathaniel Johnston, and Gerardo Adesso, 2016, "Robustness of Coherence: An Operational and Observable Measure of Quantum Coherence," Phys. Rev. Lett. **116**, 150502.

Navascués, Miguel, 2008, "Pure State Estimation and the Characterization of Entanglement," Phys. Rev. Lett. **100**, 070503.

Navascués, Miguel, Flavio Baccari, and Antonio Acín, 2021, "Entanglement marginal problems," Quantum **5**, 589.

Navascués, Miguel, Adrien Feix, Mateus Araújo, and Tamás Vértesi, 2015, "Characterizing finite-dimensional quantum behavior," Phys. Rev. A **92**, 042117.

Navascués, Miguel, Artur García-Sáez, Antonio Acín, Stefano Pironio, and Martin B. Plenio, 2013, "A paradox in bosonic energy computations via semidefinite programming relaxations," New J. Phys. **15**, 023026.

Navascués, Miguel, Yelena Guryanova, Matty J. Hoban, and Antonio Acín, 2015, "Almost quantum correlations," Nat. Commun. **6**, 6288.

Navascués, Miguel, Masaki Owari, and Martin B. Plenio, 2009a, "Complete Criterion for Separability Detection," Phys. Rev. Lett. **103**, 160404.

Navascués, Miguel, Masaki Owari, and Martin B. Plenio, 2009b, "Power of symmetric extensions for entanglement detection," Phys. Rev. A **80**, 052306.

Navascués, Miguel, Stefano Pironio, and Antonio Acín, 2007, "Bounding the Set of Quantum Correlations," Phys. Rev. Lett. **98**, 010401.

Navascués, Miguel, Stefano Pironio, and Antonio Acín, 2008, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," New J. Phys. **10**, 073013.

Navascués, Miguel, Sukhbinder Singh, and Antonio Acín, 2020, "Connector Tensor Networks: A Renormalization-Type Approach to Quantum Certification," Phys. Rev. X **10**, 021064.

Navascués, Miguel, Gonzalo de la Torre, and Tamás Vértesi, 2014, "Characterization of Quantum Correlations with Local Dimension Constraints and Its Device-Independent Applications," Phys. Rev. X **4**, 011011.

Navascués, Miguel, and Tamás Vértesi, 2015, "Bounding the Set of Finite Dimensional Quantum Correlations," Phys. Rev. Lett. **115**, 020501.

Navascués, Miguel, and Elie Wolfe, 2020, "The inflation technique completely solves the causal compatibility problem," J. Causal Inference **8**, 70–91.

Navascués, Miguel, Elie Wolfe, Denis Rosset, and Alejandro Pozas-Kerstjens, 2020, "Genuine Network Multipartite Entanglement," Phys. Rev. Lett. **125**, 240505.

Navascués, Miguel, and Harald Wunderlich, 2010, "A glance beyond the quantum model," Proc. R. Soc. A **466**, 881–890.

Nayak, Ashwin, 1999, "Optimal lower bounds for quantum automata and random access codes," in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039), New York, 1999* (IEEE, New York), pp. 369–376, 10.1109/SFFCS.1999.814608.

Nesterov, Yurii, 2000, "Squared functional systems and optimization problems," in *High Performance Optimization*, Applied Optimization, edited by Hans Frenk, Kees Roos, Tamás Terlaky, and Shuzhong Zhang (Springer, New York), pp. 405–440, 10.1007/978-1-4757-3216-0_17.

Nesterov, Yurii, and Arkadii Nemirovskii, 1994, *Interior-Point Polynomial Algorithms in Convex Programming* (Society for Industrial and Applied Mathematics, Philadelphia), 10.1137/1.9781611970791.

Nguyen, H. Chau, Sébastien Designolle, Mohamed Barakat, and Otfried Gühne, 2020, "Symmetries between measurements in quantum mechanics," arXiv:2003.12553.

Nguyen, H. Chau, Huy-Viet Nguyen, and Otfried Gühne, 2019, "Geometry of Einstein-Podolsky-Rosen correlations," Phys. Rev. Lett. **122**, 240401.

Nie, Jiawang, and Xinzhen Zhang, 2016, "Positive maps and separable matrices," SIAM J. Optim. **26**, 1236–1256.

Nielsen, Michael A., and Isaac L. Chuang, 2010, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, England), 10.1017/CBO9780511976667.

Nieto-Silleras, Olmo, Cédric Bamps, Jonathan Silman, and Stefano Pironio, 2018, "Device-independent randomness generation from several Bell estimators," New J. Phys. **20**, 023049.

Nieto-Silleras, Olmo, Stefano Pironio, and Jonathan Silman, 2014, "Using complete measurement statistics for optimal device-independent randomness evaluation," New J. Phys. **16**, 013035.

O'Donoghue, Brendan, Eric Chu, Neal Parikh, and Stephen Boyd, 2016, "Conic optimization via operator splitting and homogeneous self-dual embedding," J. Optim. Theory Appl. **169**, 1042–1068, https://www.cvxgrp.org/scs.

Ogawa, Tomohiro, and Hiroshi Nagaoka, 1999, "Strong converse to the quantum channel coding theorem," IEEE Trans. Inf. Theory **45**, 2486–2489.

Ohst, Ties-Albrecht, Xiao-Dong Yu, Otfried Gühne, and Chau H. Nguyen, 2024, "Certifying quantum separability with adaptive polytopes," SciPost Phys. **16**, 063.

Pál, Károly F., and Tamás Vértesi, 2009, "Quantum bounds on Bell inequalities," Phys. Rev. A **79**, 022120.

Pál, Károly F., and Tamás Vértesi, 2010, "Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems," Phys. Rev. A **82**, 022116.

Pál, Károly F., Tamás Vértesi, and Miguel Navascués, 2014, "Device-independent tomography of multipartite quantum states," Phys. Rev. A **90**, 042340.

Pan, Jian-Wei, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger, 1998, "Experimental Entanglement Swapping: Entangling Photons That Never Interacted," Phys. Rev. Lett. **80**, 3891–3894.

Papachristodoulou, Antonis, James Anderson, Giorgio Valmorbida, Stephen Prajna, Peter Seiler, Pablo A. Parrilo, Matthew M. Peet, and Declan Jagt, 2021, computer code SOSTOOLS, https://www.cds.caltech.edu/sostools/.

Papp, Dávid, and Sercan Yıldız, 2017, "On 'A homogeneous interior-point algorithm for non-symmetric convex conic optimization,' " arXiv:1712.00492.

Pappa, Anna, Niraj Kumar, Thomas Lawson, Miklos Santha, Shengyu Zhang, Eleni Diamanti, and Iordanis Kerenidis, 2015, "Nonlocality and Conflicting Interest Games," Phys. Rev. Lett. **114**, 020401.

Park, James L., 1970, "The concept of transition in quantum mechanics," Found. Phys. **1**, 23–33.

Parrilo, Pablo A., 2000, Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization, Ph.D. thesis (California Institute of Technology), 10.7907/2K6Y-CH43.

Passaro, Elsa, Daniel Cavalcanti, Paul Skrzypczyk, and Antonio Acín, 2015, "Optimal randomness certification in the quantum steering and prepare-and-measure scenarios," New J. Phys. **17**, 113010.

Pauwels, Jef, Stefano Pironio, Erik Woodhead, and Armin Tavakoli, 2022, "Almost Qudits in the Prepare-and-Measure Scenario," Phys. Rev. Lett. **129**, 250504.

Pauwels, Jef, Stefano Pironio, Emmanuel Zambrini Cruzeiro, and Armin Tavakoli, 2022, "Adaptive Advantage in Entanglement-Assisted Communications," Phys. Rev. Lett. **129**, 120504.

Pauwels, Jef, Armin Tavakoli, Erik Woodhead, and Stefano Pironio, 2022, "Entanglement in prepare-and-measure scenarios: Many questions, a few answers," New J. Phys. **24**, 063015.

Pawłowski, Marcin, and Nicolas Brunner, 2011, "Semi-device-independent security of one-way quantum key distribution," Phys. Rev. A **84**, 010302.

Pawłowski, Marcin, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Żukowski, 2009, "Information Causality as a physical principle," Nature (London) **461**, 1101–1104.

Pawłowski, Marcin, and Marek Żukowski, 2010, "Entanglement-assisted random access codes," Phys. Rev. A **81**, 042326.

Peres, Asher, 1996, "Separability Criterion for Density Matrices," Phys. Rev. Lett. **77**, 1413–1415.

Permenter, Frank, and Pablo A. Parrilo, 2020, "Dimension reduction for semidefinite programs via Jordan algebras," Math. Program. **181**, 51–84.

Piani, Marco, Marco Cianciaruso, Thomas R. Bromley, Carmine Napoli, Nathaniel Johnston, and Gerardo Adesso, 2016, "Robustness of asymmetry and coherence of quantum states," Phys. Rev. A **93**, 042107.

Piani, Marco, and John Watrous, 2009, "All Entangled States Are Useful for Channel Discrimination," Phys. Rev. Lett. **102**, 250501.

Piani, Marco, and John Watrous, 2015, "Necessary and Sufficient Quantum Information Characterization of Einstein-Podolsky-Rosen Steering," Phys. Rev. Lett. **114**, 060404.

Pirandola, Stefano, *et al.*, 2020, "Advances in quantum cryptography," Adv. Opt. Photonics **12**, 1012–1236.

Pironio, Stefano, 2005, "Lifting Bell inequalities," J. Math. Phys. (N.Y.) **46**, 062112.

Pironio, Stefano, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani, 2009, "Device-independent quantum key distribution secure against collective attacks," New J. Phys. **11**, 045021.

Pironio, Stefano, Miguel Navascués, and Antonio Acín, 2010, "Convergent relaxations of polynomial optimization problems with noncommuting variables," SIAM J. Optim. **20**, 2157–2180.

Pironio, Stefano, Valerio Scarani, and Thomas Vidick, 2016, "Focus on device independent quantum information," New J. Phys. **18**, 100202.

Plenio, Martin B., and Shashank Virmani, 2007, "An introduction to entanglement measures," Quantum Inf. Comput. **7**, 1–51.

Polyanskiy, Yury, H. Vincent Poor, and Sergio Verdú, 2010, "Channel coding rate in the finite blocklength regime," IEEE Trans. Inf. Theory **56**, 2307–2359.

Popescu, Sandu, and Daniel Rohrlich, 1992, "Which states violate Bell's inequality maximally?," Phys. Lett. A **169**, 411–414.

Popescu, Sandu, and Daniel Rohrlich, 1994, "Quantum nonlocality as an axiom," Found. Phys. **24**, 379–385.

Portmann, Christopher, and Renato Renner, 2022, "Security in quantum cryptography," Rev. Mod. Phys. **94**, 025008.

Pozas-Kerstjens, Alejandro, 2019, "Quantum information outside quantum information," Ph.D. thesis (Universitat Politècnica de Catalunya).

Pozas-Kerstjens, Alejandro, Antoine Girardin, Tamás Kriváchy, Armin Tavakoli, and Nicolas Gisin, 2023, "Post-quantum nonlocality in the minimal triangle scenario," New J. Phys. **25**, 113037.

Pozas-Kerstjens, Alejandro, Nicolas Gisin, and Marc-Olivier Renou, 2023, "Proofs of Network Quantum Nonlocality in Continuous Families of Distributions," Phys. Rev. Lett. **130**, 090201.

Pozas-Kerstjens, Alejandro, Nicolas Gisin, and Armin Tavakoli, 2022, "Full Network Nonlocality," Phys. Rev. Lett. **128**, 010403.

Pozas-Kerstjens, Alejandro, Rafael Rabelo, Łukasz Rudnicki, Rafael Chaves, Daniel Cavalcanti, Miguel Navascués, and Antonio Acín, 2019, "Bounding the Sets of Classical and Quantum Correlations in Networks," Phys. Rev. Lett. **123**, 140503.

Prevedel, Robert, Yang Lu, William Matthews, Rainer Kaltenbaek, and Kevin J. Resch, 2011, "Entanglement-Enhanced Classical Communication over a Noisy Classical Channel," Phys. Rev. Lett. **106**, 110505.

Primaatmaja, Ignatius William, Asaph Ho, and Valerio Scarani, 2021, "Optimal single-shot discrimination of optical modes," Phys. Rev. A **103**, 052410.

Primaatmaja, Ignatius William, Emilien Lavie, Koon Tong Goh, Chao Wang, and Charles C.-W. Lim, 2019, "Versatile security analysis of measurement-device-independent quantum key distribution," Phys. Rev. A **99**, 062332.

Pusey, Matthew F., 2013, "Negativity and steering: A stronger Peres conjecture," Phys. Rev. A **88**, 032313.

Quintino, Marco Túlio, Joseph Bowles, Flavien Hirsch, and Nicolas Brunner, 2016, "Incompatible quantum measurements admitting a local-hidden-variable model," Phys. Rev. A **93**, 052115.

Quintino, Marco Túlio, Costantino Budroni, Erik Woodhead, Adán Cabello, and Daniel Cavalcanti, 2019, "Device-Independent Tests of Structures of Measurement Incompatibility," Phys. Rev. Lett. **123**, 180401.

Quintino, Marco Túlio, Tamás Vértesi, and Nicolas Brunner, 2014, "Joint Measurability, Einstein-Podolsky-Rosen Steering, and Bell Nonlocality," Phys. Rev. Lett. **113**, 160402.

Rains, E. M., 1999, "Rigorous treatment of distillable entanglement," Phys. Rev. A **60**, 173–178.

Rains, Eric M., 2001, "A semidefinite program for distillable entanglement," IEEE Trans. Inf. Theory **47**, 2921–2933.

Regula, Bartosz, Kun Fang, Xin Wang, and Mile Gu, 2019, "One-shot entanglement distillation beyond local operations and classical communication," New J. Phys. **21**, 103017.

Renes, Joseph M., Robin Blume-Kohout, Andrew J. Scott, and Carlton M. Caves, 2004, "Symmetric informationally complete quantum measurements," J. Math. Phys. (N.Y.) **45**, 2171–2180.

Renou, Marc-Olivier, David Trillo, Mirjam Weilenmann, Thinh P. Le, Armin Tavakoli, Nicolas Gisin, Antonio Acín, and Miguel Navascués, 2021, "Quantum theory based on real numbers can be experimentally falsified," Nature (London) **600**, 625–629.

Renou, Marc-Olivier, Yuyi Wang, Sadra Boreiri, Salman Beigi, Nicolas Gisin, and Nicolas Brunner, 2019, "Limits on Correlations in Networks for Quantum and No-Signaling Resources," Phys. Rev. Lett. **123**, 070403.

Renou, Marc-Olivier, and Xiangling Xu, 2022, "Two convergent NPA-like hierarchies for the quantum bilocal scenario," arXiv:2210.09065.

Riener, Cordian, Thorsten Theobald, Lina Jansson Andŕn, and Jean B. Lasserre, 2013, "Exploiting symmetries in SDP-relaxations for polynomial optimization," Math. Oper. Res. **38**, 122–141.

Roch i Carceller, Carles, Lucas Nunes Faria, Zheng-Hao Liu, Nicolò Sguerso, Ulrik Lund Andersen, Jonas Schou Neergaard-Nielsen, and Jonatan B. Brask, 2024, "Improving semi-device-independent randomness certification by entropy accumulation," arXiv:2405.04244.

Roch i Carceller, Carles, Kieran Flatt, Hanwool Lee, Joonwoo Bae, and Jonatan B. Brask, 2022, "Quantum vs Noncontextual Semi-Device-Independent Randomness Certification," Phys. Rev. Lett. **129**, 050501.

Rosset, Denis, 2018, "`SymDPoly`: Symmetry-adapted moment relaxations for noncommutative polynomial optimization," arXiv:1808.09598.

Rosset, Denis, Felipe Montealegre-Mora, and Jean-Daniel Bancal, 2021, "`RepLAB`: A computational/numerical approach to representation theory," in *Quantum Theory and Symmetries*, CRM Series in Mathematical Physics, edited by M. B. Paranjape, Richard MacKenzie, Zora Thomova, Pavel Winternitz, and William Witczak-Krempa (Springer International Publishing, Cham, Switzerland), pp. 643–653, 10.1007/978-3-030-55777-5_60, https://github.com/ecboghiu/inflation.

Rozpędek, Filip, Thomas Schiet, Le Phuc Thinh, David Elkouss, Andrew C. Doherty, and Stephanie Wehner, 2018, "Optimizing practical entanglement distillation," Phys. Rev. A **97**, 062333.

Russo, Vincent, 2021, computer code `toqito`, version 1.0.0, https://github.com/vprusso/toqito.

Russo, Vincent, and Jamie Sikora, 2023, "Inner products of pure states and their antidistinguishability," Phys. Rev. A **107**, L030202.

Sagnol, Guillaume, and Maximilian Stahlberg, 2022, "`PICOS`: A `Python` interface to conic optimization solvers," J. Open Source Software **7**, 3915, https://picos-api.gitlab.io/picos.

Sainz, Ana Belén, Nicolas Brunner, Daniel Cavalcanti, Paul Skrzypczyk, and Tamás Vértesi, 2015, "Postquantum Steering," Phys. Rev. Lett. **115**, 190403.

Sainz, Ana Belén, Yelena Guryanova, Antonio Acín, and Miguel Navascués, 2018, "Almost-Quantum Correlations Violate the No-Restriction Hypothesis," Phys. Rev. Lett. **120**, 200402.

Salavrakos, Alexia, Remigiusz Augusiak, Jordi Tura, Peter Wittek, Antonio Acín, and Stefano Pironio, 2017, "Bell Inequalities Tailored to Maximally Entangled States," Phys. Rev. Lett. **119**, 040402.

Scarani, Valerio, 2019, *Bell Nonlocality* (Oxford University Press, New York), 10.1093/oso/9780198788416.001.0001.

Scarani, Valerio, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, 2009, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350.

Scholz, Volkher B., and Reinhard F. Werner, 2008, "Tsirelson's problem," arXiv:0812.4305.

Schrödinger, Erwin, 1935, "Discussion of probability relations between separated systems," Math. Proc. Cambridge Philos. Soc. **31**, 555–563.

Schumacher, Benjamin, and Michael D. Westmoreland, 1997, "Sending classical information via noisy quantum channels," Phys. Rev. A **56**, 131–138.

Schwonnek, René, Koon Tong Goh, Ignatius William Primaatmaja, Ernest Y.-Z. Tan, Ramona Wolf, Valerio Scarani, and Charles C.-W. Lim, 2021, "Device-independent quantum key distribution with random key basis," Nat. Commun. **12**, 2880.

Selby, John H., Elie Wolfe, David Schmid, Ana Belén Sainz, and Vinicius P. Rossi, 2024, "Linear Program for Testing Nonclassicality and an Open-Source Implementation," Phys. Rev. Lett. **132**, 050202.

Sen, Kornikar, Saronath Halder, and Ujjwal Sen, 2024, "Incompatibility of local measurements providing an advantage in local quantum state discrimination," Phys. Rev. A **109**, 012415.

Sen(De), Aditi, Ujjwal Sen, Časlav Brukner, Vladimír Bužek, and Marek Żukowski, 2005, "Entanglement swapping of noisy states: A kind of superadditivity in nonclassicality," Phys. Rev. A **72**, 042310.

Senno, Gabriel, and Antonio Acín, 2021, "Semi-device-independent full randomness amplification based on energy bounds," arXiv:2108.09100.

Shannon, Claude, 1956, "The zero error capacity of a noisy channel," IRE Trans. Inf. Theory **2**, 8–19.

Shannon, Claude E., 1948, "A mathematical theory of communication," Bell Syst. Tech. J. **27**, 379–423.

Shannon, Claude E., Robert G. Gallager, and Elwyn R. Berlekamp, 1967, "Lower bounds to error probability for coding on discrete memoryless channels. I," Inf. Control **10**, 65–103.

Sheridan, Lana, and Valerio Scarani, 2010, "Security proof for quantum key distribution using qudit systems," Phys. Rev. A **82**, 030301(R).

Shi, Weixu, Yu Cai, Jonatan B. Brask, Hugo Zbinden, and Nicolas Brunner, 2019, "Semi-device-independent characterization of quantum measurements under a minimum overlap assumption," Phys. Rev. A **100**, 042108.

Shor, Peter W., 2004, "Equivalence of additivity questions in quantum information theory," Commun. Math. Phys. **246**, 453–472.

Shor, Peter W., and John Preskill, 2000, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys. Rev. Lett. **85**, 441–444.

Siddiqui, Aliza U., and Mark M. Wilde, 2023, "Quantifying the performance of bidirectional quantum teleportation," AVS Quantum Sci. **5**, 011407.

Sikora, Jamie, and Antonios Varvitsiotis, 2017, "Linear conic formulations for two-party correlations and values of nonlocal games," Math. Program. **162**, 431–463.

Silman, J., S. Pironio, and S. Massar, 2013, "Device-Independent Randomness Generation in the Presence of Weak Cross-Talk," Phys. Rev. Lett. **110**, 100504.

Silva, Ralph, Nicolas Gisin, Yelena Guryanova, and Sandu Popescu, 2015, "Multiple Observers Can Share the Nonlocality of Half of an Entangled Pair by Using Optimal Weak Measurements," Phys. Rev. Lett. **114**, 250401.

Skajaa, Anders, and Yinyu Ye, 2015, "A homogeneous interior-point algorithm for nonsymmetric convex conic optimization," Math. Program. **150**, 391–422.

Skrzypczyk, Paul, and Daniel Cavalcanti, 2023, *Semidefinite Programming in Quantum Information Science* (IOP Publishing, Bristol, England), 10.1088/978-0-7503-3343-6.

Skrzypczyk, Paul, and Noah Linden, 2019, "Robustness of Measurement, Discrimination Games, and Accessible Information," Phys. Rev. Lett. **122**, 140403.

Skrzypczyk, Paul, Miguel Navascués, and Daniel Cavalcanti, 2014, "Quantifying Einstein-Podolsky-Rosen Steering," Phys. Rev. Lett. **112**, 180404.

Skrzypczyk, Paul, Ivan Šupić, and Daniel Cavalcanti, 2019, "All Sets of Incompatible Measurements Give an Advantage in Quantum State Discrimination," Phys. Rev. Lett. **122**, 130403.

Slater, Morton, 1950, "Lagrange multipliers revisited," in *Traces and Emergence of Nonlinear Programming*, 2014 reprint (Springer, New York), pp. 293–306, 10.1007/978-3-0348-0439-4_14.

Śliwa, Cezary, 2003, "Symmetries of the Bell correlation inequalities," Phys. Lett. A **317**, 165–168.

Smania, Massimiliano, Piotr Mironowicz, Mohamed Nawareg, Marcin Pawłowski, Adán Cabello, and Mohamed Bourennane, 2020, "Experimental certification of an informationally complete quantum measurement in a device-independent protocol," Optica **7**, 123–128.

Sørensen, Anders S., and Klaus Mølmer, 2001, "Entanglement and Extreme Spin Squeezing," Phys. Rev. Lett. **86**, 4431–4434.

Spekkens, Robert W., 2005, "Contextuality for preparations, transformations, and unsharp measurements," Phys. Rev. A **71**, 052108.

Stasiuk, Mikka, Norbert Lütkenhaus, and Ernest Y.-Z. Tan, 2022, "The quantum Chernoff divergence in advantage distillation for QKD and DIQKD," arXiv:2212.06975.

Studziński, Michał, Sergii Strelchuk, Marek Mozrzymas, and Michał Horodecki, 2017, "Port-based teleportation in arbitrary dimension," Sci. Rep. **7**, 10871.

Sturm, Jos F., 1999, "Using `SeDuMi 1.02`, a `MATLAB` toolbox for optimization over symmetric cones," Optim. Method Software **11**, 625–653, https://github.com/sqlp/sedumi (it is recommended to use this fork, as the original is unmaintained).

Summers, Stephen J., and Reinhard F. Werner, 1987, "Maximal violation of Bell's inequalities is generic in quantum field theory," Commun. Math. Phys. **110**, 247–259.

Sun, Chuangchuang, and Ran Dai, 2017, "Rank-constrained optimization and its applications," Automatica **82**, 128–136.

Šupić, Ivan, Remigiusz Augusiak, Alexia Salavrakos, and Antonio Acín, 2016, "Self-testing protocols based on the chained Bell inequalities," New J. Phys. **18**, 035013.

Šupić, Ivan, and Joseph Bowles, 2020, "Self-testing of quantum systems: A review," Quantum **4**, 337.

Šupić, Ivan, Paul Skrzypczyk, and Daniel Cavalcanti, 2017, "Measurement-device-independent entanglement and randomness estimation in quantum networks," Phys. Rev. A **95**, 042340.

Šupić, Ivan, Paul Skrzypczyk, and Daniel Cavalcanti, 2019, "Methods to estimate entanglement in teleportation experiments," Phys. Rev. A **99**, 032334.

Sutter, David, Mario Berta, and Marco Tomamichel, 2017, "Multivariate trace inequalities," Commun. Math. Phys. **352**, 37–58.

Szangolies, Jochen, Hermann Kampermann, and Dagmar Bruß, 2015, "Detecting entanglement of unknown quantum states with random measurements," New J. Phys. **17**, 113051.

Szangolies, Jochen, Hermann Kampermann, and Dagmar Bruß, 2017, "Device-Independent Bounds on Detection Efficiency," Phys. Rev. Lett. **118**, 260401.

Tabia, Gelo Noel M., Kai-Siang Chen, Chung-Yun Hsieh, Yu-Chun Yin, and Yeong-Cherng Liang, 2022, "Entanglement transitivity problems," npj Quantum Inf. **8**, 98.

Takagi, Ryuji, Bartosz Regula, Kaifeng Bu, Zi-Wen Liu, and Gerardo Adesso, 2019, "Operational Advantage of Quantum Resources in Subchannel Discrimination," Phys. Rev. Lett. **122**, 140402.

Tan, Ernest Y.-Z., 2023, "Robustness of implemented device-independent protocols against constrained leakage," arXiv:2302.13928.

Tan, Ernest Y.-Z., Charles C.-W. Lim, and Renato Renner, 2020, "Advantage Distillation for Device-Independent Quantum Key Distribution," Phys. Rev. Lett. **124**, 020502.

Tan, Ernest Y.-Z., René Schwonnek, Koon Tong Goh, Ignatius William Primaatmaja, and Charles C.-W. Lim, 2021, "Computing secure key rates for quantum cryptography with untrusted devices," npj Quantum Inf. **7**, 1–6.

Tavakoli, Armin, 2020, "Semi-Device-Independent Certification of Independent Quantum State and Measurement Devices," Phys. Rev. Lett. **125**, 150503.

Tavakoli, Armin, 2021, "Semi-Device-Independent Framework Based on Restricted Distrust in Prepare-and-Measure Experiments," Phys. Rev. Lett. **126**, 210503.

Tavakoli, Armin, Emmanuel Zambrini Cruzeiro, Jonatan B. Brask, Nicolas Gisin, and Nicolas Brunner, 2020, "Informationally restricted quantum correlations," Quantum **4**, 332.

Tavakoli, Armin, Emmanuel Zambrini Cruzeiro, Roope Uola, and Alastair A. Abbott, 2021, "Bounding and simulating contextual correlations in quantum theory," PRX Quantum **2**, 020334.

Tavakoli, Armin, Emmanuel Zambrini Cruzeiro, Erik Woodhead, and Stefano Pironio, 2022, "Informationally restricted correlations: A general framework for classical and quantum systems," Quantum **6**, 620.

Tavakoli, Armin, Máté Farkas, Denis Rosset, Jean-Daniel Bancal, and Jędrzej Kaniewski, 2021, "Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments," Sci. Adv. **7**, eabc3847.

Tavakoli, Armin, and Nicolas Gisin, 2020, "The Platonic solids and fundamental tests of quantum mechanics," Quantum **4**, 293.

Tavakoli, Armin, Nicolas Gisin, and Cyril Branciard, 2021, "Bilocal Bell Inequalities Violated by the Quantum Elegant Joint Measurement," Phys. Rev. Lett. **126**, 220401.

Tavakoli, Armin, Alley Hameedi, Breno Marques, and Mohamed Bourennane, 2015, "Quantum Random Access Codes Using Single *d*-Level Systems," Phys. Rev. Lett. **114**, 170502.

Tavakoli, Armin, Jędrzej Kaniewski, Tamás Vértesi, Denis Rosset, and Nicolas Brunner, 2018, "Self-testing quantum states and measurements in the prepare-and-measure scenario," Phys. Rev. A **98**, 062307.

Tavakoli, Armin, Breno Marques, Marcin Pawłowski, and Mohamed Bourennane, 2016, "Spatial versus sequential correlations for random access coding," Phys. Rev. A **93**, 032336.

Tavakoli, Armin, Jef Pauwels, Erik Woodhead, and Stefano Pironio, 2021, "Correlations in entanglement-assisted prepare-and-measure scenarios," PRX Quantum **2**, 040357.

Tavakoli, Armin, Marcin Pawłowski, Marek Żukowski, and Mohamed Bourennane, 2017, "Dimensional discontinuity in quantum communication complexity at dimension seven," Phys. Rev. A **95**, 020302.

Tavakoli, Armin, Alejandro Pozas-Kerstjens, Ming-Xing Luo, and Marc-Olivier Renou, 2022, "Bell nonlocality in networks," Rep. Prog. Phys. **85**, 056001.

Tavakoli, Armin, Denis Rosset, and Marc-Olivier Renou, 2019, "Enabling Computation of Correlation Bounds for Finite-Dimensional Quantum Systems via Symmetrization," Phys. Rev. Lett. **122**, 070501.

Tavakoli, Armin, Paul Skrzypczyk, Daniel Cavalcanti, and Antonio Acín, 2014, "Nonlocal correlations in the star-network configuration," Phys. Rev. A **90**, 062109.

Tavakoli, Armin, Massimiliano Smania, Tamás Vértesi, Nicolas Brunner, and Mohamed Bourennane, 2020, "Self-testing nonprojective quantum measurements in prepare-and-measure experiments," Sci. Adv. **6**, eaaw6664.

Tebyanian, Hamid, Mujtaba Zahidy, Marco Avesani, Andrea Stanco, Paolo Villoresi, and Giuseppe Vallone, 2021, "Semi-device independent randomness generation based on quantum state's indistinguishability," Quantum Sci. Technol. **6**, 045026.

Terhal, Barbara M., 2000, "Bell inequalities and the separability criterion," Phys. Lett. A **271**, 319–326.

Terhal, Barbara M., and Paweł Horodecki, 2000, "Schmidt number for density matrices," Phys. Rev. A **61**, 040301.

Thinh, Le Phuc, Gonzalo de la Torre, Jean-Daniel Bancal, Stefano Pironio, and Valerio Scarani, 2016, "Randomness in post-selected events," New J. Phys. **18**, 035007.

Tomamichel, Marco, 2015, *Quantum Information Processing with Finite Resources: Mathematical Foundations*, SpringerBriefs in Mathematical Physics Vol. 5 (Springer, New York), 10.1007/978-3-319-21891-5.

Tomamichel, Marco, Mario Berta, and Joseph M. Renes, 2016, "Quantum coding with finite resources," Nat. Commun. **7**, 11419.

Tomamichel, Marco, Mark M. Wilde, and Andreas Winter, 2017, "Strong converse rates for quantum communication," IEEE Trans. Inf. Theory **63**, 715–727.

Tomiyama, Jun, 1985, "On the geometry of positive maps in matrix algebras. II," Linear Algebra Appl. **69**, 169–177.

Tóth, Géza, and Otfried Gühne, 2005, "Detecting Genuine Multipartite Entanglement with Two Local Measurements," Phys. Rev. Lett. **94**, 060501.

Tóth, Géza, Christian Knapp, Otfried Gühne, and Hans J. Briegel, 2009, "Spin squeezing and entanglement," Phys. Rev. A **79**, 042334.

Tóth, Géza, Tobias Moroder, and Otfried Gühne, 2015, "Evaluating Convex Roof Entanglement Measures," Phys. Rev. Lett. **114**, 160501.

Tsirelson, Boris S., 1980, "Quantum generalizations of Bell's inequality," Lett. Math. Phys. **4**, 93–100.

Tsirelson, Boris S., 1987, "Quantum analogues of the Bell inequalities. The case of two spatially separated domains," J. Sov. Math. **36**, 557–570.

Tsirelson, Boris S., 1993, "Some results and problems on quantum Bell-type inequalities," Hadronic J. Suppl. **8**, 329–345, http://www.tau.ac.il/~tsirel/download/hadron.pdf.

Tura, Jordi, Albert Aloy, Flavio Baccari, Antonio Acín, Maciej Lewenstein, and Remigiusz Augusiak, 2019, "Optimization of

device-independent witnesses of entanglement depth from two-body correlators," Phys. Rev. A **100**, 032307.
Uhlmann, Armin, 1976, "The 'transition probability' in the state space of a *-algebra," Rep. Math. Phys. **9**, 273–279.
Uola, Roope, Costantino Budroni, Otfried Gühne, and Juha-Pekka Pellonpää, 2015, "One-to-One Mapping between Steering and Joint Measurability Problems," Phys. Rev. Lett. **115**, 230402.
Uola, Roope, Ana C. S. Costa, H. Chau Nguyen, and Otfried Gühne, 2020, "Quantum steering," Rev. Mod. Phys. **92**, 015001.
Uola, Roope, Tristan Kraft, Jiangwei Shang, Xiao-Dong Yu, and Otfried Gühne, 2019, "Quantifying Quantum Resources with Conic Programming," Phys. Rev. Lett. **122**, 130404.
Vaisakh, Mannalath, Ram krishna Patra, Mukta Janpandit, Samrat Sen, Manik Banik, and Anubhav Chaturvedi, 2021, "Mutually unbiased balanced functions and generalized random access codes," Phys. Rev. A **104**, 012420.
Valcarce, Xavier, Pavel Sekatski, Davide Orsucci, Enky Oudot, Jean-Daniel Bancal, and Nicolas Sangouard, 2020, "What is the minimum CHSH score certifying that a state resembles the singlet?," Quantum **4**, 246.
Vallins, James, Ana Belén Sainz, and Yeong-Cherng Liang, 2017, "Almost-quantum correlations and their refinements in a tripartite Bell scenario," Phys. Rev. A **95**, 022111.
van Dam, Wim, 1999, "Nonlocality and communication complexity," Ph.D. thesis (University of California, Santa Barbara).
Vandenberghe, Lieven, and Stephen Boyd, 1996, "Semidefinite programming," SIAM Rev. **38**, 49–95.
van Himbeeck, Thomas, and Stefano Pironio, 2019, "Correlations and randomness generation based on energy constraints," arXiv:1905.09117.
van Himbeeck, Thomas, Erik Woodhead, Nicolas J. Cerf, Raúl García-Patrón, and Stefano Pironio, 2017, "Semi-device-independent framework based on natural physical assumptions," Quantum **1**, 33.
Verstraete, Frank, and Henri Verschelde, 2003, "Optimal Teleportation with a Mixed State of Two Qubits," Phys. Rev. Lett. **90**, 097901.
Vértesi, Tamás, 2008, "More efficient Bell inequalities for Werner states," Phys. Rev. A **78**, 032112.
Vértesi, Tamás, and Nicolas Brunner, 2014, "Disproving the Peres conjecture by showing Bell nonlocality from bound entanglement," Nat. Commun. **5**, 5297.
Vértesi, Tamás, and Károly F. Pál, 2011, "Nonclassicality threshold for the three-qubit Greenberger-Horne-Zeilinger state," Phys. Rev. A **84**, 042122.
Vértesi, Tamás, Stefano Pironio, and Nicolas Brunner, 2010, "Closing the Detection Loophole in Bell Experiments Using Qudits," Phys. Rev. Lett. **104**, 060401.
Vidal, Guifré, and J. Ignacio Cirac, 2001, "Irreversibility in Asymptotic Manipulations of Entanglement," Phys. Rev. Lett. **86**, 5803–5806.
Vidal, Guifré, and Rolf Tarrach, 1999, "Robustness of entanglement," Phys. Rev. A **59**, 141–155.
Vidal, Guifré, and Reinhard F. Werner, 2002, "Computable measure of entanglement," Phys. Rev. A **65**, 032314.
Vieira, Carlos, Carlos de Gois, Lucas Pollyceno, and Rafael Rabelo, 2023, "Interplays between classical and quantum entanglement-assisted communication scenarios," New J. Phys. **25**, 113004.
Wang, Chao, Ignatius William Primaatmaja, Hong Jie Ng, Jing Yan Haw, Raymond Ho, Jianran Zhang, Gong Zhang, and Charles C.-W. Lim, 2023, "Provably-secure quantum randomness expansion with uncharacterised homodyne detection," Nat. Commun. **14**, 316.
Wang, Ning-Ning, Alejandro Pozas-Kerstjens, Chao Zhang, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, Nicolas Gisin, and Armin Tavakoli, 2023, "Certification of non-classicality in all links of a photonic star network without assuming quantum mechanics," Nat. Commun. **14**, 2153.
Wang, Xi-Lin, *et al.*, 2016, "Experimental Ten-Photon Entanglement," Phys. Rev. Lett. **117**, 210502.
Wang, Xin, and Runyao Duan, 2016a, "Improved semidefinite programming upper bound on distillable entanglement," Phys. Rev. A **94**, 050301.
Wang, Xin, and Runyao Duan, 2016b, "A semidefinite programming upper bound of quantum capacity," in *Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, 2016* (IEEE, New York), pp. 1690–1694, 10.1109/ISIT.2016.7541587.
Wang, Xin, and Runyao Duan, 2017a, "Irreversibility of Asymptotic Entanglement Manipulation under Quantum Operations Completely Preserving Positivity of Partial Transpose," Phys. Rev. Lett. **119**, 180506.
Wang, Xin, and Runyao Duan, 2017b, "Nonadditivity of Rains' bound for distillable entanglement," Phys. Rev. A **95**, 062322.
Wang, Xin, Kun Fang, and Runyao Duan, 2019, "Semidefinite programming converse bounds for quantum communication," IEEE Trans. Inf. Theory **65**, 2583–2592.
Wang, Xin, and Mark M. Wilde, 2020, "Cost of Quantum Entanglement Simplified," Phys. Rev. Lett. **125**, 040502.
Wang, Xin, Wei Xie, and Runyao Duan, 2018, "Semidefinite programming strong converse bounds for classical capacity," IEEE Trans. Inf. Theory **64**, 640–653.
Wang, Yi-Xuan, Zhen-Peng Xu, and Otfried Gühne, 2024, "Quantum LOSR networks cannot generate graph states with high fidelity," npj Quantum Inf. **10**, 11.
Wang, Yukun, Ignatius William Primaatmaja, Emilien Lavie, Antonios Varvitsiotis, and Charles C.-W. Lim, 2019, "Characterising the correlations of prepare-and-measure quantum networks," npj Quantum Inf. **5**, 17.
Watrous, John, 2009, "Semidefinite programs for completely bounded norms," Theory Comput. **5**, 217–238.
Watrous, John, 2013, "Simpler semidefinite programs for completely bounded norms," Chicago J. Theor. Comput. Sci. **8**, 1–19.
Watrous, John, 2018, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, England), 10.1017/9781316848142.
Wehner, Stephanie, 2006, "Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities," Phys. Rev. A **73**, 022110.
Wei, Tzu-Chieh, and Paul M. Goldbart, 2003, "Geometric measure of entanglement and applications to bipartite and multipartite quantum states," Phys. Rev. A **68**, 042307.
Weilenmann, Mirjam, Edgar A. Aguilar, and Miguel Navascués, 2021, "Analysis and optimization of quantum adaptive measurement protocols with the framework of preparation games," Nat. Commun. **12**, 4553.
Weilenmann, Mirjam, Costantino Budroni, and Miguel Navascués, 2024, "Optimization of time-ordered processes in the finite and asymptotic regimes," PRX Quantum **5**, 020351.
Weilenmann, Mirjam, and Roger Colbeck, 2017, "Analysing causal structures with entropy," Proc. R. Soc. A **473**, 20170483.
Weilenmann, Mirjam, Benjamin Dive, David Trillo, Edgar A. Aguilar, and Miguel Navascués, 2020, "Entanglement Detection beyond Measuring Fidelities," Phys. Rev. Lett. **124**, 200502.
Werner, Reinhard F., 1989, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," Phys. Rev. A **40**, 4277–4281.
Werner, Reinhard F., and Michael M. Wolf, 2001, "Bell inequalities and entanglement," Quantum Inf. Comput. **1**, 1–25.
Wiesner, Stephen, 1983, "Conjugate coding," ACM SIGACT News **15**, 78–88.

Wilde, Mark M., 2013, *Quantum Information Theory* (Cambridge University Press, Cambridge, England), 10.1017/CBO9781139525343.

Wilde, Mark M., Andreas Winter, and Dong Yang, 2014, "Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy," Commun. Math. Phys. **331**, 593–622.

Winick, Adam, Norbert Lütkenhaus, and Patrick J. Coles, 2018, "Reliable numerical key rates for quantum key distribution," Quantum **2**, 77.

Winter, Andreas, 1999, "Coding theorem and strong converse for quantum channels," IEEE Trans. Inf. Theory **45**, 2481–2485.

Wiseman, Howard M., Steven J. Jones, and Andrew C. Doherty, 2007, "Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox," Phys. Rev. Lett. **98**, 140402.

Wittek, Peter, 2015, "Algorithm 950: `Ncpol2sdpa`—Sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables," ACM Trans. Math. Software **41**, 1–12, https://github.com/peterjbrown519/ncpol2sdpa (it is recommended to use this fork, as the original is unmaintained).

Wolfe, Elie, Alejandro Pozas-Kerstjens, Matan Grinberg, Denis Rosset, Antonio Acín, and Miguel Navascués, 2021, "Quantum Inflation: A General Approach to Quantum Causal Compatibility," Phys. Rev. X **11**, 021043.

Wolfe, Elie, Robert W. Spekkens, and Tobias Fritz, 2019, "The inflation technique for causal inference with latent variables," J. Causal Inference **7**, 20170020.

Wolkowicz, Henry, Romesh Saigal, and Lieven Vandenberghe, 2000, *Handbook of Semidefinite Programming* (Springer, New York).

Wooltorton, Lewis, Peter Brown, and Roger Colbeck, 2022, "Tight Analytic Bound on the Trade-Off between Device-Independent Randomness and Nonlocality," Phys. Rev. Lett. **129**, 150403.

Wootters, William K., 1998, "Entanglement of Formation of an Arbitrary State of Two Qubits," Phys. Rev. Lett. **80**, 2245–2248.

Wootters, William K., and Brian D. Fields, 1989, "Optimal state-determination by mutually unbiased measurements," Ann. Phys. (N.Y.) **191**, 363–381.

Wootters, William K., and Wojciech H. Zurek, 1982, "A single quantum cannot be cloned," Nature (London) **299**, 802–803.

Wu, Xingyao, Yu Cai, Tzyh Haur Yang, Huy Nguyen Le, Jean-Daniel Bancal, and Valerio Scarani, 2014, "Robust self-testing of the three-qubit *W* state," Phys. Rev. A **90**, 042339.

Wyderka, Nikolai, Giovanni Chesi, Hermann Kampermann, Chiara Macchiavello, and Dagmar Bruß, 2023, "Construction of efficient Schmidt-number witnesses for high-dimensional quantum states," Phys. Rev. A **107**, 022431.

Xu, Feihu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan, 2020, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002.

Xu, Feihu, Yu-Zhe Zhang, Qiang Zhang, and Jian-Wei Pan, 2022, "Device-Independent Quantum Key Distribution with Random Postselection," Phys. Rev. Lett. **128**, 110506.

Yang, Tzyh Haur, and Miguel Navascués, 2013, "Robust self-testing of unknown quantum systems into any entangled two-qubit states," Phys. Rev. A **87**, 050102.

Yang, Tzyh Haur, Miguel Navascués, Lana Sheridan, and Valerio Scarani, 2011, "Quantum Bell inequalities from Macroscopic Locality," Phys. Rev. A **83**, 022105.

Yang, Tzyh Haur, Tamás Vértesi, Jean-Daniel Bancal, Valerio Scarani, and Miguel Navascués, 2014, "Robust and Versatile Black-Box Certification of Quantum Devices," Phys. Rev. Lett. **113**, 040401.

Yoshida, Satoshi, Akihito Soeda, and Mio Murao, 2023, "Reversing Unknown Qubit-Unitary Operation, Deterministically and Exactly," Phys. Rev. Lett. **131**, 120602.

Yu, Nengkun, Runyao Duan, and Mingsheng Ying, 2012, "Four Locally Indistinguishable Ququad-Ququad Orthogonal Maximally Entangled States," Phys. Rev. Lett. **109**, 020506.

Yu, Nengkun, Runyao Duan, and Mingsheng Ying, 2014, "Distinguishability of quantum states by positive operator-valued measures with positive partial transpose," IEEE Trans. Inf. Theory **60**, 2069–2079.

Yu, Xiao-Dong, Timo Simnacher, H. Chau Nguyen, and Otfried Gühne, 2022, "Quantum-inspired hierarchy for rank-constrained optimization," PRX Quantum **3**, 010340.

Yu, Xiao-Dong, Timo Simnacher, Nikolai Wyderka, H. Chau Nguyen, and Otfried Gühne, 2021, "A complete hierarchy for the pure state marginal problem in quantum mechanics," Nat. Commun. **12**, 1012.

Zhang, Chengjie, Sophia Denker, Ali Asadian, and Otfried Gühne, 2024, "Analyzing Quantum Entanglement with the Schmidt Decomposition in Operator Space," Phys. Rev. Lett. **133**, 040203.

Żukowski, Marek, Anton Zeilinger, Michael A. Horne, and Artur K. Ekert, 1993, "'Event-Ready-Detectors' Bell Experiment via Entanglement Swapping," Phys. Rev. Lett. **71**, 4287–4290.