Self-testing of quantum systems: a review

Ivan Šupić[1] and Joseph Bowles[2]

[1]Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland

[2]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain

September 21, 2020

Self-testing is a method to infer the underlying physics of a quantum experiment in a black box scenario. As such it represents the strongest form of certification for quantum systems. In recent years a considerable self-testing literature has developed, leading to progress in related device-independent quantum information protocols and deepening our understanding of quantum correlations. In this work we give a thorough and self-contained introduction and review of self-testing and its application to other areas of quantum information.

1 Introduction

In contrast to classical theories, states in quantum physics can be entangled and sets of measurements can be incompatible. As shown by Bell in 1964 [Bel64], these features imply striking observable phenomena. In particular, the outcomes of incompatible measurements made on the local subsystems of an entangled quantum state can exhibit correlations that are provably stronger than any resulting from a classical theory, a phenomenon known as Bell nonlocality. The field of Bell nonlocality has since grown considerably (see [BCP+14] for a recent review article), and the existence of Bell nonlocal correlations in nature is now a well established fact [HBD+15, GVW+15, SMSC+15].

As more was understood about Bell nonlocality, a number of works [SW87, PR92, BMR92, Tsi93] eventually pointed out that there exist Bell nonlocal correlations that—as well as requiring entanglement and incompatibility—can only be produced by making *particular* sets of incompatible measurements on *particular* entangled states. These works have since given birth to the field of self-testing, which broadly speaking aims to understand the structure of the set of quantum correlations and identify those correlations that admit a unique physical realisation.

An important milestone in the development of self-testing was the 2004 work of Mayers and Yao [MY04]. This work set the terminology and formalism that was to be adopted by later works, and includes the first usage of the term 'self-testing' in this context. A similar idea was already present in [MY98] in a cryptographic context, using the term 'self-checking' instead of 'self-testing'. These early works also introduced the paradigm of *device-independence*, to which self-testing is intimately related. In particular, a self-testing protocol can be seen as a device-independent—or black box—certification of a quantum system, assuming that the system can be prepared many times in an independent, identically distributed manner. Self-testing is consequently relevant to many device-independent quantum information protocols and has led to related progress in this area. More recently, self-testing has become synonymous with any protocol for certifying any type of quantum system under a small set of assumptions.

In this work we give a up-to-date review of the field of self-testing. We hope that it will be of use to people both unfamiliar with the field, as well as serving as a reference for those within it. The review is organised as follows. In section 2 we give a gentle introduction to device-independence and its connection to self-testing. We then formally introduce self-testing, giving the mathematical definitions in section 3 and a simple example in section 4 that illustrates many important concepts. Sections 5 to 8 are a thorough literature review of state and measurement self-testing, explaining the tools and techniques that are commonly used along the way. In section 9 we review extensions of self-testing to other

scenarios, and in section 10 the application of self-testing to other fields in quantum information theory. In section 11 we cover experimental realisations of self-testing protocols. Finally, in section 12 we discuss some possible future directions for the field and a number of open problems.

We point the reader to the related review articles [MdW16] and [Sca12] where discussions about self-testing can also be found. [MdW16] deals with the classical and quantum certification of both classical and quantum properties of an object, with self-testing being identified as classical certification of quantum properties. [Sca12] provides a pedagogical review of the device-independent approach to quantum physics. Self-testing is discussed as one of device-independent protocols. We also recommend [McK10, Kan17, Kan16] as valuable texts for first time readers.

Contents

2 Self-testing as a device-independent protocol

The treatment of complex systems as black boxes is a powerful tool in many scientific domains, providing a minimalist level of abstraction that allows one to focus on *what* a device or system does without the need to model precisely *how* this is achieved. In quantum information theory, this approach is known as the *device-independent* (DI) approach.

In order to explain the idea of the device-independent approach we imagine the following scenario. Consider two laboratories, run by two experimenters called Carmela and Deng. In their laboratories (let's imagine they are quantum optics laboratories) both Carmela and Deng have access to some equipment (e.g. lasers, beamsplitters, waveplates, photon detectors,...) which they can use to perform different experiments. A given experiment consists of a choice of *settings* (e.g. laser intensity, angle of the waveplates, type of beamsplitter,...) that after a run of the experiment provides a *result* (e.g. photon detection location, time of detection,...). Furthermore, a source is positioned between the laboratories and emits physical systems (e.g. photons) that are sent to Carmela's and Deng's laboratories; see figure 1, left.

Suppose that Carmela and Deng would like to learn if the source is emitting entangled particles (where the entanglement is with respect to the two laboratories). One way to achieve this is to use their equipment to perform tomography of the state of the source, i.e. Carmela and Deng perform a number of experiments each with different settings, collect statistics of the results, and use quantum state tomography to reconstruct the density matrix of the state, which can then be checked to determine if it is entangled (for instance using an entanglement witness). This is indeed what is done in many experiments around the world.

Imagine now however that two computer scientists—called Alice and Bob—are visiting each of the labs. Despite knowing the mathematical definition of entanglement, they will have problems convincing themselves that the source is producing entanglement. Firstly, they do not understand the experimental setup, so they do not know what the different settings do. Moreover, even if they were told what the settings do, they do not have a good understanding of quantum optics. As a result, they will not be able to reconstruct the state of the source in order to check if it is entangled, as was the case for Carmela and Deng.

Alice, however, proposes the following: even though they do not understand what the settings do, they can still change them and observe *something*. That is, they can simply model their laboratories as black boxes. Each laboratory is treated as a device (a black box) that takes an input (the settings) and returns and output (the result), but the physical mechanism behind how this occurs is unknown (see figure 1, centre). Similarly, they do not assume anything about the source; all they know is that it is distributing some physical systems that may or may not be entangled. Alice denotes each of her possible settings as $x = 0, 1, \ldots$ and Bob denotes each of his possible settings as $y = 0, 1, \ldots$. Similarly Alice and Bob denote the possible results of their experiments by $a = 0, 1, \ldots$ and $b = 0, 1, \ldots$.

After trying the different settings sufficiently many times and collecting statistics, Alice and Bob can estimate the probabilities (also called the *correlations*)

$$p(a, b|x, y), \tag{1}$$

that is, the probabilities to see the results a and b given that the settings x and y are used. It is important here to stress that although Alice and Bob can estimate these probabilities, they are ignorant about the underlying physics; from their perspective the experiments could have been made on atoms, electrons, neutrinos or any other physical system. This scenario is called the *device-independent* scenario. Remarkably, even with such little knowledge, Alice and Bob can still conclude that the source emits entangled states.

The trick to achieving this is to use *Bell nonlocality*, a counter-intuitive phenomenon discovered by John Bell in 1964 [Bel64] (see also box 3.1). At the heart of Bell nonlocality are objects called *Bell inequalities*. A Bell inequality consists of a function $\mathcal{I}$ of the probabilities $\{p(a, b|x, y)\}$ such that, for a source producing separable (i.e non-entangled) states one has

$$\mathcal{I}(\{p(a, b|x, y)\}) \leq \beta. \tag{2}$$

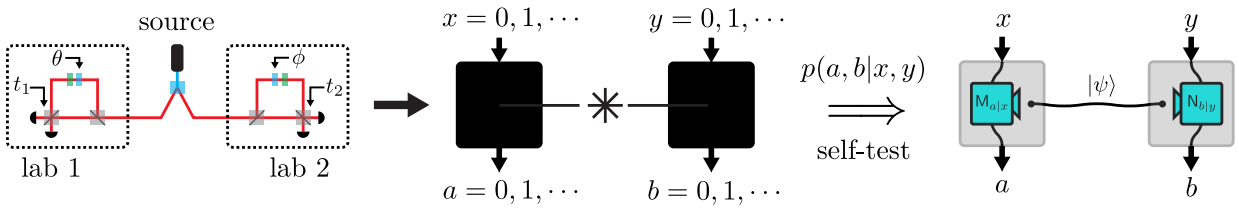


Figure 1: (left) A source produces systems and distributes them between two laboratories that can perform different local experiments by varying the settings of their equipment. (centre) In the device-independent approach, each local laboratory is treated as a black box that takes as input a label that corresponds to a particular choice of settings for the experiment, and outputs a label that denotes the corresponding result. After repeating the experiments sufficiently many times, the probabilities $p(a, b|x, y)$ can be estimated. (right) When self-testing a state and measurements, one aims to infer the form of the state of the source and measurement operators describing the laboratories from knowledge of the probabilities alone, i.e. in a black box scenario.

Importantly, the bound β holds for *any* source producing *any* kind of physical systems, provided that these systems are not entangled. This is a consequence of the fact that the definition of separability is independent of the physical system in question. Interestingly, Bell inequalities can be violated by entangled sources. That is, for some entangled sources one can achieve $\mathcal{I}(p(a, b|x, y)) > \beta$. This situation can be understood geometrically in the vector space of probabilities, where Bell inequalities are defined by linear hyperplanes; see Fig. 2.

Alice and Bob can therefore do the following. They compare their probabilities against as many Bell inequalities as they know. If they see that one is violated, then it must be that the source is entangled! Moreover, they are able to conclude this despite knowing nothing about how the experiment was actually performed; all the information that was needed was the probabilities $\{p(a, b|x, y)\}$. Such a procedure is called a *device-independent certification of entanglement*.

Suppose now that we change the task: instead of only detecting entanglement, Alice and Bob want to know the particular entangled state of the source. Due to the device-independent scenario, they cannot know the type of physical system that the source is producing. However, they may hope to write down the state vector $|\psi\rangle$ of the source, without specifying which types of physical degrees of freedom it describes. This often turns out to be possible (up to some local transformations, see the definitions in the following section), as long as one observes the *maximum* possible violation achievable in quantum theory of a corresponding Bell inequality. Such a procedure is called a *device-independent self-test* or simply a *self-test* of the state. Often, this maximal violation also allows one to self-test the measurements, i.e. to determine the form of the measurement operators that describe how the outcomes a and b are produced in the local laboratories.

Alice and Bob will nevertheless face a problem: they will never see the maximum violation of a Bell inequality due to experimental noise and finite statistics. At best, they will be able to lower bound the violation up to some statistical confidence. To become a practically relevant protocol, self-testing therefore has to be combined with two other tools: (i) noise-resistant self-testing methods (called *robust self-testing*; see section 3.6) which give distance upper bounds to the desired state and/or measurements as a function of experimental noise; and (ii) tools of statistical analysis (such as Chernoff bounds) that allow for statistically valid estimations of probabilities and corresponding confidence levels. Self-testing can thus be seen as a theoretical tool that, when augmented by statistical techniques, can be transformed into a protocol for device-independent state and measurement certification.

A number of remarks are in order before proceeding to formal definitions of self-testing in the next section. First, one may wonder whether self-testing is possible using only a single device. That is, given a single device from which one observes the conditional probabilities $p(a|x)$, is it possible to determine the quantum state $|\psi\rangle$ inside? Notice that one possibility is that there is a pre-programmed classical computer inside the device that simply simulates the statistics $p(a|x)$. In the device-independent scenario one cannot rule out this possibility. Thus, one cannot hope to certify any non-classical properties of $|\psi\rangle$ with only

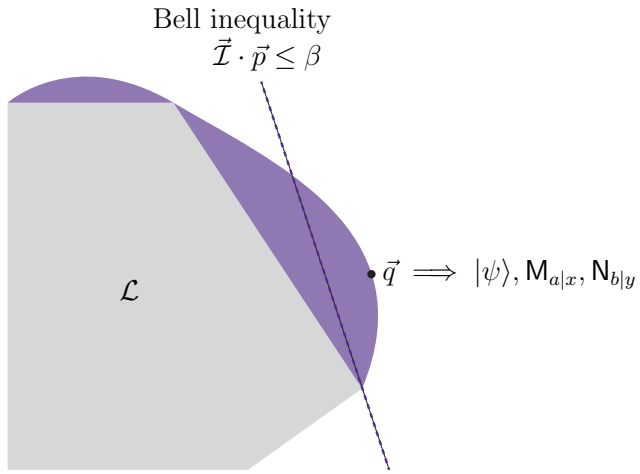


Figure 2: Geometric representation of self-testing. The figure is a 2-dimensional representation of the space of probability vectors $\vec{p} = (p(00|00), p(01|00), \dots)$. The grey area $\mathcal{L}$ is the set of probability vectors that are obtainable with separable states (commonly called the 'local set'). A Bell inequality (dotted line) consists of a pair $(\vec{\mathcal{I}}, \beta)$ such that the half space $\vec{\mathcal{I}} \cdot \vec{p} \leq \beta$ contains $\mathcal{L}$. Entangled quantum states are capable of producing probability vectors that lie outside of $\mathcal{L}$ (purple area) and thus violate Bell inequalities. Often, extremal points (e.g. $\vec{q}$) of the quantum set, which maximally violate some Bell inequality, admit—up to local transformations—a unique realisation in terms of a particular entangled state and measurements. Self-testing involves identifying such probability distributions and proving their unique realisation.

a single device. It is for this reason that it is crucial to move to a multipartite scenario in order to certify non-classical states. Indeed, it is precisely the phenomenon of Bell nonlocality that forbids an explanation using local pre-programmed classical devices.

Second, it is worth mentioning some practical advantages of the device-independent scenario. Suppose Alice and Bob are sold two devices that are claimed to contain a particular entangled state and perform certain measurements on it. Using self-testing, they will be able to conclude that the devices are indeed working correctly without having to understand precisely how they operate. This is clearly desirable from the perspective of Alice and Bob, especially for cryptographic applications where one would prefer not to trust the devices. From a more experimental perspective, the device-independent scenario naturally treats experimental errors at the level of the observed statistics, meaning for example, that a false positive detection of entanglement will never occur. Being the strongest form of device-independent certification, self-testing has proven to be useful for many device-independent protocols; see section 10 for more information.

Third, we note that the notion of device-independence referred to by the large majority of self-testing works assumes independent, identically distributed (i.i.d.) rounds of the experiment, i.e. the state and the measurements are assumed to be the same in each round and do not depend on past measurement results or choices. Such an assumption allows us to talk about the probability distribution $p(a, b|x, y)$ that is valid in every experimental round. This however is not the strongest possible notion of device-independence where one further drops the i.i.d. assumption (typically used in the field of quantum cryptography). Self-testing under this more stringent notion of device-independence is little explored (although arguably relevant); see the concluding remarks in section 12 for further discussion.

Finally, we note that aside from its motivation for device-independent certification, self-testing can also be viewed as part of the general study of quantum correlations. In particular, quantum correlations are defined via the Born rule, whereby a state and measurement operators are mapped to a probability distribution. Generally, this map does not have an inverse, since many combinations of state and measurements can lead to the same probabilities. Self-testing identifies those points of the set of quantum probability distributions for which such an inverse exists, up to the local transformations defined in the next section. That is, it associates some (extremal) probability distributions with a unique realisation using a particular state and measurements. For this reason self-testing has been used to derive important results about the set of quantum correlations.

3 Definitions

3.1 Notation

We first introduce some notation. $\mathcal{L}(\mathcal{H})$ denotes the set of linear operators acting on Hilbert space $\mathcal{H}$. Uppercase Roman letters denote a local party, most often either Alice, A, or Bob, B. Roman letters in either subscript or superscript denote the Hilbert space in which a state lives or on which

an operator acts e.g. $|\psi\rangle_{\mathrm{A}} \in \mathcal{H}_{\mathrm{A}}$. Consecutive labels denote tensor products of Hilbert spaces, e.g. $|\psi\rangle_{\mathrm{AB}} \in \mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$. Labels containing the same letter are implicitly assumed to refer to different local Hilbert spaces of a single subsystem, e.g. A and A′ refer to two Hilbert spaces of Alice.

As a result, self-testing is often a useful tool in a variety of device-independent protocols (see section 10 for explicit examples). In the following section, we formalise these ideas and define precisely what it means to self-test a state and measurements.

3.2 The self-testing scenario

The device-independent scenario described in the previous section is commonly called a *Bell test*, and the probabilities $p(a, b|x, y)$ are called *correlations*. From quantum theory, we know that there exist measurement operators $\mathsf{M}_{a|x} \in \mathcal{L}(\mathcal{H}_{\mathrm{A}})$ acting on Alice's local Hilbert space and satisfying

$$\mathsf{M}_{a|x} \succcurlyeq 0 \quad \forall x, a, \quad \sum_a \mathsf{M}_{a|x} = \mathbb{1}_{\mathrm{A}} \quad \forall x \tag{3}$$

that describe how the outcomes a are obtained given settings x. Similarly there exist measurement operators $\mathsf{N}_{b|y} \in \mathcal{L}(\mathcal{H}_{\mathrm{B}})$ for Bob acting on his local Hilbert space. From here on we work with a Naimark dilation of each of the measurements. The measurement operators are therefore projective:

$$\begin{aligned} \mathsf{M}_{a|x}\mathsf{M}_{a'|x} &= \delta_{a,a'}\mathsf{M}_{a|x} && \forall x, a, a' \,, \\ \mathsf{N}_{b|y}\mathsf{N}_{b'|y} &= \delta_{b,b'}\mathsf{N}_{b|y} && \forall y, b, b'. \end{aligned} \tag{4}$$

This can be justified if one takes the position that projective measurements and unitary evolution are the only fundamental operations in quantum theory. From this perspective, any measurement necessarily involves a projective measurement over a dilated space, the degrees of freedom of which belong to Alice and Bob's local Hilbert spaces. For further discussion on this assumption, see Appendix B.

Now, from the Born rule, there must exist some quantum state $\rho_{\mathrm{AB}} \in \mathcal{L}(\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}) \succcurlyeq 0$, $\mathrm{tr}\,\rho_{\mathrm{AB}} = 1$ such that

$$p(a, b|x, y) = \mathrm{tr}\left[\rho_{\mathrm{AB}}\, \mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y}\right]. \tag{5}$$

In self-testing, one aims to infer the form of the state and the measurements in (5) from knowledge of the correlations $p(a, b|x, y)$ alone; i.e. in the device-independent scenario.

In order to write (5), one nevertheless needs to make some basic physical assumptions that constitute the definition of the device-independent scenario in most self-testing works. These are

1. The experiment admits a quantum description; i.e. there exists a quantum state and measurement operators that lead to the observed outcomes via the Born rule.

2. The laboratories of Alice and Bob are located at separate locations in space and there is no communication between the laboratories; e.g. Alice cannot send the choice of setting x to Bob or vice-versa.

3. The settings x and y are chosen freely and independently of all other systems in the experiment. For example, the physical system used to generate x does not have any correlations (quantum or classical) with the particles or the source or the laboratory of Bob.

4. Each round of the experiment is independent from all other rounds and physically equivalent to all others. That is, there exists a single density matrix and measurement operators that are valid in every round. The statistics of all the rounds are thus independent and identically distributed (i.i.d.), so that we may consider $p(a, b|x, y)$ only.

Following the majority of self-testing works, we will often choose to work with a purification $|\psi\rangle_{\mathrm{ABP}}$ of ρ_{AB}, where the purification space $\mathcal{H}_{\mathrm{P}}$ is external to both Alice's and Bob's laboratories. This will be quite convenient mathematically, since working with state vectors over density matrices will significantly shorten the length of some equations. We stress that we do not assume that the state shared between Alice and Bob is pure; indeed it is given by $\mathrm{tr}_{\mathrm{P}}[|\psi\rangle\langle\psi|_{\mathrm{ABP}}] = \rho_{\mathrm{AB}}$. Furthermore, our definitions of self-testing will be such that the purification space is untouched by the self-testing protocol. Hence, working with $|\psi\rangle_{\mathrm{ABP}}$ and tracing out the purification space is equivalent to working with ρ_{AB}. For this reason, the definitions in the following section can be equivalently phrased using ρ_{AB} by simply discarding the purification space. Using such a purification, the probabilities (5) can be written

$$p(a, b|x, y) = \langle\psi|\mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y} \otimes \mathbb{1}_{\mathrm{P}}\, |\psi\rangle_{\mathrm{ABP}} \,, \tag{6}$$

where $\mathbb{1}_{\mathrm{P}}$ is the identity operator on the purification space.

Now, let's imagine we have in mind a particular pure state[1] $|\psi'\rangle_{\mathrm{A'B'}}$ and projective measurements $\{\mathsf{M}'_{a|x}\}, \{\mathsf{N}'_{b|y}\}$ that we would like to self-test. We call this state and measurements the *reference state* and *reference measurements*. The state ρ_{AB} and measurements $\{\mathsf{M}_{a|x}\}, \{\mathsf{N}_{b|y}\}$ that correspond to the actual experiment are called the *physical state* and *physical measurements*. Similarly, the realisation $\{|\psi'\rangle_{\mathrm{A'B'}}, \{\mathsf{M}'_{a|x}\}, \{\mathsf{N}'_{b|y}\}\}$ is called the *reference experiment* and $\{\rho_{\mathrm{AB}}, \{\mathsf{M}_{a|x}\}, \{\mathsf{N}_{b|y}\}\}$ the *physical experiment*.

Note that it will not be possible to infer exactly the reference state and measurements from the correlations alone. This is for the following two reasons:

i Due to the unitary invariance of the trace, one can reproduce the statistics of any state $|\psi'\rangle$ and measurements $\{\mathsf{M}'_{a|x}\}$, $\{\mathsf{N}'_{b|y}\}$ by instead using the rotated state $U \otimes V |\psi'\rangle$ and measurements $\{U\mathsf{M}'_{a|x}U^\dagger\}$, $\{V\mathsf{N}'_{b|y}V^\dagger\}$, where U and V are unitary transformations. Hence, one can never conclude that the state is $|\psi'\rangle$ since it may in fact be $U \otimes V |\psi'\rangle$.

ii One cannot rule out additional degrees of freedom on which the measurement operators act trivially. That is, a state $|\psi'\rangle \otimes |\xi\rangle$ and measurements $\{\mathsf{M}'_{a|x} \otimes \mathbb{1}\}$, $\{\mathsf{N}'_{b|y} \otimes \mathbb{1}\}$ (where the identity operators act on the local spaces of $|\xi\rangle$) gives the same correlations as $|\psi'\rangle$ and $\{\mathsf{M}'_{a|x}\}$, $\{\mathsf{N}'_{b|y}\}$.

To be able to define what it means to infer a particular state in the device-independent scenario, we thus need to define an equivalence between states that takes into account the above unknowns (that is, local unitary transformations and additional unused degrees of freedom). To do this, we make use of the concept of a *local isometry*.

An isometry $\Phi : \mathcal{H}_{\mathrm{A}_1} \to \mathcal{H}_{\mathrm{A}_2}$ is a linear transformation on quantum states that preserves the inner product, and can thus be seen as a unitary operator that can increase the dimension of the space. A general isometry on a state $|\psi\rangle_{\mathrm{A}_1}$ can be achieved by embedding $|\psi\rangle_{\mathrm{A}_1}$ in a larger Hilbert space $\mathcal{H}_{\mathrm{A}_2}$ and performing a unitary transformation; i.e. $\Phi[|\psi\rangle_{\mathrm{A}_1}] = U |\psi\rangle_{\mathrm{A}_2}$. A *local isometry*

$$\Phi_{\mathrm{A}_1} \otimes \Phi_{\mathrm{B}_1} : \mathcal{H}_{\mathrm{A}_1} \otimes \mathcal{H}_{\mathrm{B}_1} \to \mathcal{H}_{\mathrm{A}_2} \otimes \mathcal{H}_{\mathrm{B}_2} \qquad (7)$$

is an isometry that can be realised with local quantum operations; i.e. it is a tensor product of isometries acting locally. One way to implement a local isometry—often used in self-testing works—is to embed the initial state using local ancilla states $|00\rangle_{\mathrm{A'B'}}$, and then perform a local unitary transformation (see figure 3):

$$\Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}[|\psi\rangle_{\mathrm{AB}}] = U_{\mathrm{A'A}} \otimes V_{\mathrm{B'B}} \left[|00\rangle_{\mathrm{A'B'}} \otimes |\psi\rangle_{\mathrm{AB}}\right].$$

In the following sections we will use $\Phi[|\psi\rangle]$ to denote the action of an isometry on the pure state $|\psi\rangle$ and use $\Phi[\rho]$ to denote the corresponding transformation on a density matrix. As we will see, the notion of a local isometry will be central to our definitions of self-testing.

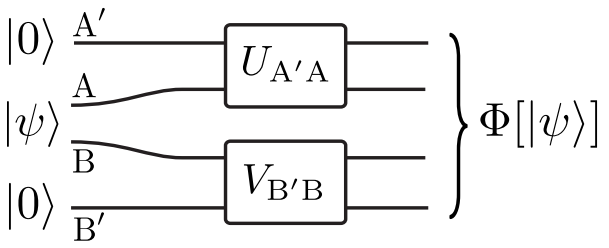


Figure 3: A local isometry applied to a quantum state. Local ancillas are added to the state and unitary transformations are applied locally.

3.3 Self-testing of states

We are now ready to define what it means to self-test a quantum state.

Definition 1. *(self-testing of pure states)*

The correlations $p(a, b|x, y)$ self-test the state $|\psi'\rangle_{\mathrm{A'B'}}$ if for any state ρ_{AB} compatible with $p(a, b|x, y)$ (for some choice of local measurements) and for any purification $|\psi\rangle_{\mathrm{ABP}}$ of ρ_{AB} there exists a local isometry

$$\Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}} : \mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}} \to \mathcal{H}_{\mathrm{A'\bar{A}}} \otimes \mathcal{H}_{\mathrm{B'\bar{B}}}$$

such that

$$\Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}} \otimes \mathbb{1}_{\mathrm{P}}[|\psi\rangle_{\mathrm{ABP}}] = |\psi'\rangle_{\mathrm{A'B'}} \otimes |\xi\rangle_{\mathrm{\bar{A}\bar{B}P}} \qquad (8)$$

for some state $|\xi\rangle_{\mathrm{\bar{A}\bar{B}P}}$.

[1] self-testing of mixed states will not be possible; see section 3.5

The above can be understood via the idea of *extraction*. If we trace out the purification space in (8) then we have

$$\Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}} \left[\rho_{\mathrm{AB}}\right] = |\psi'\rangle\langle\psi'|_{\mathrm{A'B'}} \otimes \sigma_{\bar{\mathrm{A}}\bar{\mathrm{B}}}, \quad (9)$$

where $\sigma_{\bar{\mathrm{A}}\bar{\mathrm{B}}} = \mathrm{tr}_{\mathrm{P}} |\xi\rangle\langle\xi|$. Thus, if one self-tests the state $|\psi'\rangle_{\mathrm{A'B'}}$, then there necessarily exists a local channel (given by the isometry) that allows one to extract $|\psi'\rangle_{\mathrm{A'B'}}$ from ρ_{AB} into the ancilla space. The state $|\xi\rangle_{\bar{\mathrm{A}}\bar{\mathrm{B}}\mathrm{P}}$ in (8), which contains everything else from $|\psi\rangle_{\mathrm{AB}}$ after the reference state has been extracted, is called a *junk state*. We note that it is not necessary that one actually perform the isometry in the laboratory; all that is needed is a mathematical proof that such as procedure exists in principle. In section 4 we will see how this is possible with an explicit example.

Definition 1 is the definition that is most commonly used in self-testing works, although the identity channel on the purification space is often left implicit. Note that it is important that the isometry does not act on the purification space since, for example, the purification of a mixed separable state would result in an entangled state, which would give the devices access to entanglement for free. Finally, the above definitions can be straightforwardly generalised to define self-testing of multipartite states; one simply uses an isometry that is local with respect to the subsystems of the multipartite state to be self-tested.

3.4 Self-testing of measurements

The correlations that are used to self-test the reference state often allow one to identify the measurements that were performed. Since our physical measurements are projective, this definition will apply to self-testing of projective measurements only. The idea is to prove that under the action of the isometry, the physical measurements map to the reference measurements acting on the reference state. More specifically,

---

Definition 2. (*self-testing of states and measurements)*

The correlations $p(a,b|x,y)$ self-test the state and measurements $|\psi'\rangle_{\mathrm{A'B'}}, \{\mathsf{M}'_{a|x}\}, \{\mathsf{N}'_{b|y}\}$ if for any state and measurements $\rho_{\mathrm{AB}}, \{\mathsf{M}_{a|x}\}, \{\mathsf{N}_{b|y}\}$ compatible with $p(a,b|x,y)$ and for any purification $|\psi\rangle_{\mathrm{ABP}}$ of ρ_{AB} there exists a local isometry $\Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}$ such that

$$\Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}} \otimes \mathbb{1}_{\mathrm{P}} \left[\mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y} \otimes \mathbb{1}_{\mathrm{P}} |\psi\rangle_{\mathrm{ABP}}\right] = \left(\mathsf{M}'_{a|x} \otimes \mathsf{N}'_{b|y} |\psi'\rangle_{\mathrm{A'B'}}\right) \otimes |\xi\rangle_{\bar{\mathrm{A}}\bar{\mathrm{B}}\mathrm{P}}$$

for all a, x, b, y, for some state $|\xi\rangle_{\bar{\mathrm{A}}\bar{\mathrm{B}}\mathrm{P}}$.

If we wish to make a statement solely involving the measurements, we will only be able to say something about the part of the measurement that acts on the support of the physical state. Some recent works (see e.g. [Kan17]) adopt this approach and use a definition of measurement self-testing in the following spirit (for example, for Alice's measurements).

Definition 3. (*self-testing of measurements)*

The correlations $p(a,b|x,y)$ self-test the measurements $\{\mathsf{M}'_{a|x}\}$ for Alice if for any measurements $\{\mathsf{M}_{a|x}\}$ and state ρ_{AB} compatible with $p(a,b|x,y)$ there exists a unitary operator U such that

$$U_{\mathrm{A}}[\tilde{\mathsf{M}}_{a|x}]U_{\mathrm{A}}^{\dagger} = \mathsf{M}'_{a|x} \otimes \mathbb{1}$$

for all a, x, where $\tilde{\mathsf{M}}_{a|x} = \Pi\, \mathsf{M}_{a|x}\, \Pi$ and Π is the projector onto the support of $\rho_{\mathrm{A}} = \mathrm{tr}_{\mathrm{B}}\, \rho_{\mathrm{AB}}$.

3.5 Self-testing via a Bell inequality and the geometry of the set of quantum correlations

It is known that only those correlations that are extremal points of the quantum set of correlations and are achievable with finite dimensional quantum systems can be used to self-test both a state and measurements [GKW+18]. Such points can often be witnessed by the maximum violation of some Bell inequality over the set of quantum correlations. As a result, one often does not need the full set of probabilities $p(a,b|x,y)$ in order to prove self-testing statements; the maximum quantum violation of a Bell inequality may already imply the existence of the desired isometry. One can thus consider self-testing relative to a Bell inequality by replacing the observation of the correlations by the value of a Bell inequality $\mathcal{I}[p(a,b|x,y)]$ in the previous definitions. Many of the well known Bell inequalities, such as CHSH and CGLMP have been used to this effect (see section 5 for such results).

In this light one might ask if the maximal violation of every nontrivial Bell inequality, *i.e.* one

which can be violated in quantum theory, is also a self-test of some entangled state. Or even more generally, do all extremal points of the set of quantum correlations self-test some state? These questions are examined in [GKW+18] where it was shown that the relation between self-testing, maximisers of non-trivial Bell inequalities and the boundary of the quantum set is not as simple as one might hope for.

We also note here that bipartite mixed state correlations can always be reproduced by a pure state of the *same* dimension [SVW16]. This implies that self-testing of bipartite mixed states following the same spirit as definition 1 above is impossible. Since the isometry preserves the purity of the input, applying the isometry to the pure state that gives the same correlations cannot result in the desired mixed state in tensor product with a junk state.

3.6 Robust self-testing

One encounters two problems when trying to prove self-testing statements as defined above from experimental data: (i) the experiment will inevitably contain some level of noise that will dampen the correlations, and (ii) the precise values of $p(a,b|x,y)$ will be uncertain due to a finite sample size. In practice, this will mean that proving perfect self-testing of states and measurements is impossible. Point (ii) can be addressed using tools of statistical inference [LRZ+18]. Point (i) can be tackled by proving approximate self-testing statements, and is known as robust self-testing. In short, the aim of robust self-testing is to prove that if the correlations are sufficiently close to the ideal correlations, then the state and measurements must be close (in some well-defined sense) to the desired ones.

We will focus on two notions of 'closeness' that are frequently used in the literature. Our first definition is as follows. Imagine we have identified an isometry that allows us to prove a self-testing statement as in definition 1. If the correlations are close to the ideal then one would expect that the two vectors appearing on either side of (8) be approximately equal up to some vector norm. This leads to the following.

Definition 4. *(robust self-testing of states, vector norm)*

The correlations $p(a,b|x,y)$ self-test the state $|\psi'\rangle_{\mathrm{A'B'}}$ with distance δ in the vector norm $||\cdot||$ if for any state ρ_{AB} compatible with $p(a,b|x,y)$ and for any purification $|\psi\rangle_{\mathrm{ABP}}$ of ρ_{AB} there exists a local isometry $\Phi = \Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}$ such that

$$||\Phi \otimes \mathbb{1}_{\mathrm{P}}[|\psi\rangle_{\mathrm{ABP}}] - |\psi'\rangle_{\mathrm{A'B'}} \otimes |\xi\rangle_{\bar{\mathrm{A}}\bar{\mathrm{B}}\mathrm{P}}|| \leq \delta$$

for some state $|\xi\rangle_{\bar{\mathrm{A}}\bar{\mathrm{B}}\mathrm{P}}$.

This definition was used as the first definition of robust self-testing.

Our second definition follows the intuition that if in the ideal case one can extract the reference state $|\psi'\rangle$, then in the noisy case one should be able to extract something close to $|\psi'\rangle$. Here, it is usually easiest to adopt the fidelity, defined as $F(|\psi\rangle, \rho) = \langle\psi|\rho|\psi\rangle$ as the notion of closeness. First, define ρ^{EXT} as the extracted state of the ancillas after the application of the isometry, that is,

$$\rho^{\mathrm{EXT}}_{\mathrm{A'B'}} = \mathrm{tr}_{\bar{\mathrm{A}}\bar{\mathrm{B}}}\Phi[\rho_{\mathrm{AB}}]. \tag{10}$$

We then have the following definition.

Definition 5. *(robust self-testing of states, fidelity)*

The correlations $p(a,b|x,y)$ self-test the state $|\psi'\rangle_{\mathrm{A'B'}}$ with fidelity f if for any state ρ_{AB} compatible with $p(a,b|x,y)$ there exists a local isometry $\Phi = \Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}$ such that

$$F\left(|\psi'\rangle_{\mathrm{A'B'}}, \rho^{\mathrm{EXT}}_{\mathrm{A'B'}}\right) \geq f. \tag{11}$$

Ideally, one would like replace the fidelity in the above definition by the trace distance $T(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_1 = \frac{1}{2}\mathrm{tr}[\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}]$, since the trace distance is both a metric (unlike the fidelity) and relates directly to the probability of distinguishing the two states. The fact that the fidelity is much more commonly used is because its linearity in the state ρ makes bounds generally much easier to compute. One can nevertheless prove an upper bound to $T(\rho^{\mathrm{EXT}}, |\psi'\rangle\langle\psi'|)$ from a bound on the fidelity using the relation $T \leq \sqrt{1-F}$ [NC18]. We point the reader to [BLM+09] where a useful discussion about appropriate figures of merit for robust self-testing can be found.

Note that a local isometry can always prepare any pure product state of the ancillas for free by simply ignoring the physical state and applying the necessary unitaries on the ancilla space.

Hence, the best bound achievable via this strategy defines a *trivial bound* that can always be achieved. As an example, consider the task of self-testing the state $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ for some $\theta \in (0, \pi/4)$. This state has fidelity $\cos^2(\theta)$ and euclidean distance $\sqrt{2-2\cos\theta}$ to the state $|00\rangle$. Thus a self-tested fidelity or distance is interesting only if it surpasses the corresponding bound. Taking definition 5, this trivial fidelity is equal to the square of the largest Schmidt coefficient of the state.

3.6.1 Extractability relative to a Bell inequality

As with ideal self-testing statements, it is most common to consider robust self-testing relative to a Bell inequality $\mathcal{I}$. For example, taking definition 5 as the figure of merit, one aims to find a function $f(\beta)$ that gives a lower bound on the fidelity as a function of the Bell inequality violation $\mathcal{I}(p(a,b|x,y)) = \beta$. This can be linked to the notion of *extractability* of the physical state with respect to the reference state for the Bell inequality $\mathcal{I}$. Note that any CPTP map can be realised by performing an isometry and discarding some degrees of freedom [Sti55]. Thus the map $\mathrm{tr}_{\bar{A}\bar{B}}\Phi[\rho_{AB}]$ is equivalent to a general local CPTP map $\Lambda_A \otimes \Lambda_B : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ applied to ρ_{AB}. Given a physical state ρ, the extractability Ξ is the maximum fidelity of $\Lambda_A \otimes \Lambda_B[\rho]$ and $|\psi'\rangle$ over all CPTP maps:

$$\Xi(\rho \to |\psi'\rangle) = \max_{\Lambda_A, \Lambda_B} F(\Lambda_A \otimes \Lambda_B[\rho], |\psi'\rangle). \quad (12)$$

To get optimal robust self-testing statements for a given inequality $\mathcal{I}$ one therefore needs to minimise the extractability over all states compatible with $\mathcal{I} = \beta$ for all values of β. This leads to the extractability-violation trade-off function

$$\mathcal{Q}_{\psi,\mathcal{B}_\mathcal{I}} = \inf_{\rho|\mathrm{tr}[\mathcal{B}_\mathcal{I}\rho]=\beta} \Xi(\rho \to |\psi'\rangle). \quad (13)$$

Finding the extractability-violation trade-off function for a given Bell inequality is a difficult task since it involves a minimisation of the fidelity over all compatible states and a maximisation over all possible CPTP maps. Moreover, the optimal CPTP map (or equivalently, isometry) generally depends on the observed violation. More commonly, one fixes a single isometry for all violations and minimises the fidelity only, leading to a sub-optimal curve.

Finally, one can use similar ideas to the above to define the robust self-testing of measurements. We do not give any definition here, but point the reader to section 8.3 for work in this direction.

3.7 Generalisations and alternative definitions

3.7.1 The issue of complex conjugation

When self-testing quantum states in the bipartite scenario, it is sufficient to consider real reference states only, i.e. states such that $|\psi'\rangle = |\psi'\rangle^*$, where $*$ denotes complex conjugation with respect to a fixed basis. This follows since all pure states are local unitary equivalent to a real state via the Schmidt decomposition [Pre98]. A similar argument for measurements however is not possible. As a result, definition 2 suffers from a serious drawback; it can only be used to self-test sets of measurements that are invariant under the complex conjugation of all measurement operators. To see this note that since $p(ab|xy) = (p(ab|xy))^*$ then (assuming a real state $|\psi'\rangle$)

$$\begin{aligned} p(ab|xy) =& \mathrm{tr}\left[|\psi'\rangle\langle\psi'|\ \mathsf{M}'_{a|x} \otimes \mathsf{N}'_{b|y}\right] \\ =& \mathrm{tr}\left[|\psi'\rangle\langle\psi'|\ (\mathsf{M}'_{a|x})^* \otimes (\mathsf{N}'_{b|y})^*\right]. \end{aligned} \quad (14)$$

Thus any correlations obtained using $\{|\psi'\rangle, \mathsf{M}'_{a|x}, \mathsf{N}'_{b|y}\}$ can also be obtained using $\{|\psi'\rangle, (\mathsf{M}'_{a|x})^*, (\mathsf{N}'_{b|y})^*\}$. These two realisations are generally not equivalent under local unitary operations. In this case, one cannot self-test the set $\{|\psi'\rangle, \mathsf{M}'_{a|x}, \mathsf{N}'_{b|y}\}$ using definition 2 since there is always another realisation $\{|\psi'\rangle, (\mathsf{M}'_{a|x})^*, (\mathsf{N}'_{b|y})^*\}$ that is not related to the first via a local isometry but results in the same correlations.

A straightforward solution to this problem first proposed in [MM11] is to generalise the definition of measurement self-testing so that one self-tests the measurements $\{\mathsf{M}'_{a|x}, \mathsf{N}'_{b|y}\}$ if one can show that on the support of $|\psi'\rangle$, the physical measurements act as some unknown convex combination of $\{\mathsf{M}'_{a|x}, \mathsf{N}'_{b|y}\}$ and $\{(\mathsf{M}'_{a|x})^*, (\mathsf{N}'_{b|y})^*\}$. This is in line with the general spirit of self-testing in which one aims to certify the measurements up to all the intrinsic limitations of the device-independent scenario. See appendix A.1 for a possible definition along these lines and section 8.2.1 for an example of such a self-test.

In principle, there may be more state and measurement transformations other than com-

plex conjugation that do not affect the observed probabilities. Determining this set is still an open problem. While in the case of qubit bipartite systems one can aim at self-testing states and measurements up to local isometries and complex conjugations, it is unclear if more transformations may be present when considering higher dimensional systems or multipartite scenarios.

3.7.2 Self-testing via simulation

Another recent approach presented in [Kan16] is to adopt the philosophy that self-testing a reference state or measurements should imply that the physical state or measurements be capable to *simulate* the reference state or measurements. For states, this translates to finding a local quantum channel $\Lambda_A \otimes \Lambda_B$ that maps the physical state to the reference state, thus allowing the simulation of any measurement on the reference state by first applying the channel followed by the desired measurement. Note that this definition is equivalent to definition 1 since via Stinespring's dilation theorem [Cho75, Sti55] any local channel can be realised by first applying a local isometry then tracing out any irrelevant degrees of freedom.

For measurements, one considers unital channels, i.e. quantum channels that preserve the identity (and thus map sets of measurements to sets of measurements). The idea is then (say, for Alice) that if one can find a unital channel such that $\Lambda[\mathsf{M}_{a|x}] = \mathsf{M}'_{a|x}$, then one can simulate the reference measurement $\mathsf{M}'_{a|x}$ on any state by first applying the dual quantum channel $\Lambda^\dagger$ on the state followed by the physical measurement $\mathsf{M}_{a|x}$. Since

$$\mathrm{tr}\left[\Lambda^\dagger[\varrho]\mathsf{M}_{a|x}\right] = \mathrm{tr}\left[\varrho\Lambda[\mathsf{M}_{a|x}]\right] = \mathrm{tr}\left[\varrho\mathsf{M}'_{a|x}\right] \tag{15}$$

one recovers the same statistics as making the reference measurement on any state ϱ. This approach was used in [RKB18] to self-test the Bell state measurement (see section 8.2.4) .

3.7.3 Measurement self-testing based on commutation

Yet another approach to measurement self-testing focuses on certifying that the physical measurements satisfy some desired commutation relation on the support of the physical state. This can be advantageous, as commutation relations are often the only relevant features that one is interested in, and since they are invariant under isometry maps the approach can lead to simpler proofs of self-testing. Furthermore, in the case of perfect statistics, certifying a particular commutation relation may be enough to prove full self-testing statements of the form of definition 2. This approach has been used to prove measurement self-testing statements for anti-commuting qubit observables [Kan17] and sets of mutually unbiased bases in dimension 3 [KŠT+19]. It is very close in spirit to one of the earliest self-testing statements given in [PR92]. For further discussion on this technique, see section 8.2.2.

4 A first example

The maximally entangled state of two-qubits

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{18}$$

is the quantum state which is most emblematic of the significance entanglement has in quantum theory and is used in a wide class of information processing protocols [BBC+93, BW92, Eke91]. In this section we show how to prove formal self-testing statements for this state and locally anti-commuting observables. Many of the techniques used to self-test more complex states and measurements can be understood as a generalisation of those presented here. We work in a simple scenario in which Alice and Bob each have two inputs ($x, y = 0, 1$) and two outputs ($a, b = \pm 1$). We chose the convention of having ± 1 valued outcomes since it will be convenient to work with the observables

$$\mathsf{A}_x = \mathsf{M}_{+|x} - \mathsf{M}_{-|x}\,; \quad \mathsf{B}_y = \mathsf{N}_{+|y} - \mathsf{N}_{-|y}, \tag{19}$$

where $\mathsf{M}_{a|x}$, $\mathsf{N}_{b|y}$ are the physical measurements operators in (5). Note that since the physical measurement operators are projective (see section 3.2), the operators A_x, B_y are by construction Hermitian and unitary. We thus have

$$\mathsf{A}_x^\dagger = \mathsf{A}_x\,; \quad \mathsf{A}_x^2 = \mathbb{1}\,; \quad \mathsf{B}_y^\dagger = \mathsf{B}_y\,; \quad \mathsf{B}_y^2 = \mathbb{1}. \tag{20}$$

Following definition 1 we work with a purification $|\psi\rangle_{\mathrm{ABP}}$ of the physical state where the measurements act trivially on $\mathcal{H}_\mathrm{P}$. In the following we

Box 3.1: Bell Nonlocality and the CHSH inequality

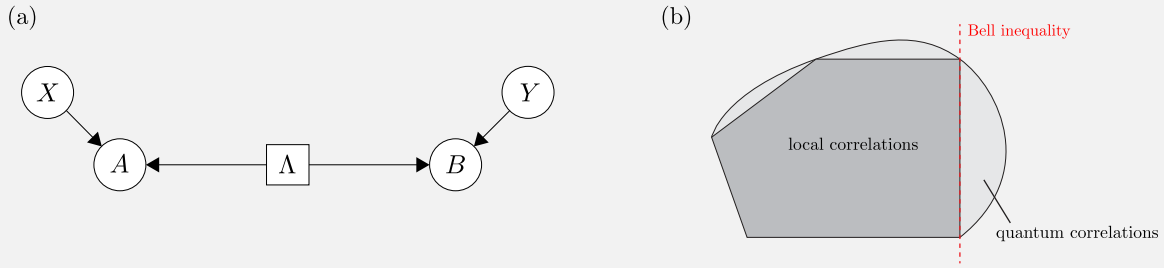
Bell nonlocality is a counter-intuitive property of quantum correlations discovered by John Bell in 1964 [Bel64]. The correlations $p(a,b|x,y)$ are called *local* if they can be reproduced by shared classical information. To formalise this, we represent the shared information by a classical random variable $\Lambda \sim \pi(\lambda)$. Averaging over this information, the possible correlations that Alice and Bob can achieve is given by (see (a) below for the corresponding classical causal network)

$$p(a,b|x,y) = \int_\Lambda \pi(\lambda) p_A(a|x,\lambda) p_B(b|y,\lambda) \mathrm{d}\lambda. \tag{16}$$

Notice that local measurements on any separable state $\rho = \int_\Lambda \mathrm{d}\lambda \pi(\lambda) \sigma_\lambda^{\mathrm{A}} \otimes \sigma_\lambda^{\mathrm{B}}$ lead to correlations of the above form, and so (16) is precisely those correlations that can be achieved using separable states. If we collect all of the probabilities into a single vector $\mathbf{p} = (p(00|00), p(01|00), \cdots)$ then the set of local correlations forms a convex polytope, the facets of which are called *Bell inequalities* (see (b), below). Remarkably, if Alice and Bob share an entangled quantum system, they may produce correlations that are *nonlocal*, i.e. which violate a Bell inequality and therefore cannot be written in form (16). An important Bell inequality, called the CHSH Bell inequality [CHSH69], already exists in the simplest scenario in which Alice and Bob have two inputs $(x,y = 0,1)$ and two outcomes $(a,b = \pm 1)$. It is given by

$$\beta_{\mathrm{CHSH}} = \langle \mathsf{A}_0\mathsf{B}_0\rangle + \langle \mathsf{A}_1\mathsf{B}_0\rangle + \langle \mathsf{A}_0\mathsf{B}_1\rangle - \langle \mathsf{A}_1\mathsf{B}_1\rangle \leq 2, \tag{17}$$

where $\langle \mathsf{A}_x\mathsf{B}_y\rangle = \sum_{a,b} a \cdot b\, p(ab|xy)$ denotes the *correlator* for the inputs x, y. Measurements on the maximally entangled state $|\phi^+\rangle = [|00\rangle + |11\rangle]/\sqrt{2}$ can violate this inequality up to $\beta_{\mathrm{CHSH}} = 2\sqrt{2}$. For a comprehensive review on Bell nonlocality, see [BCP+14].



do not explicitly write the identity on the purification space, e.g. A_x should be understood as $\mathsf{A}_x \otimes \mathbb{1}_{\mathrm{P}}$.

The central object we will use for self-testing is the CHSH Bell inequality [CHSH69] (see box 3.1 for a summary of Bell nonlocality)

$$\beta_{\mathrm{CHSH}} = \langle \mathsf{A}_0\mathsf{B}_0\rangle + \langle \mathsf{A}_1\mathsf{B}_0\rangle + \langle \mathsf{A}_0\mathsf{B}_1\rangle - \langle \mathsf{A}_1\mathsf{B}_1\rangle \leq 2.$$

Performing certain local measurements on the state $|\phi^+\rangle$ leads to a violation of $\beta_{CHSH} = 2\sqrt{2}$. More specifically, both Alice and Bob use anticommuting measurement observables to achieve this violation. Alice measures $\mathsf{A}_0 = \sigma_{\mathrm{x}}$ and $\mathsf{A}_1 = \sigma_{\mathrm{z}}$, while Bob measures $\mathsf{B}_0 = (\sigma_{\mathrm{z}} + \sigma_{\mathrm{x}})/\sqrt{2}$ and $\mathsf{B}_1 = (\sigma_{\mathrm{x}} - \sigma_{\mathrm{z}})/\sqrt{2}$. The reverse statement, that the violation $2\sqrt{2}$ can only be achieved by measurements applied on $|\phi^+\rangle$, represented the first self-testing statement. Early proofs of this statement can be found in [SW87], [PR92], [BMR92] and [Tsi93], a decade and a half before the term self-testing was coined.

In the following we show how to self-test $|\phi^+\rangle$ from correlations achieving the maximal violation of the CHSH inequality. The central step in the proof will be to show that Alice and Bob's local observables anticommute on the support of their shared state, i.e. $\{\mathsf{A}_0, \mathsf{A}_1\}|\psi\rangle = \{\mathsf{B}_0, \mathsf{B}_1\}|\psi\rangle = 0$. We present two methods to achieve this; (i) a geometrical argument for anticommutativity of Bob's observables (section 4.1), and (ii) an algebraic argument (section 4.2). Once this is achieved, the anticommuting observables can be

used to build the required local isometry that is needed to prove a formal self-testing statement (section 4.3).

4.1 Geometrical proof of anticommutativity

In this section we give a simple geometric proof that the correlations maximally violating the CHSH inequality can be achieved only by measuring locally anticommuting observables. This will require knowing all correlations, not only the observation that $\beta_{CHSH} = 2\sqrt{2}$. The ideal correlations achieving this violation are

$$\begin{aligned} \langle\psi|\mathsf{A}_0\mathsf{B}_0\,|\psi\rangle &= \frac{1}{\sqrt{2}}, \quad \langle\psi|\mathsf{A}_0\mathsf{B}_1\,|\psi\rangle = \frac{1}{\sqrt{2}}, \\ \langle\psi|\mathsf{A}_1\mathsf{B}_0\,|\psi\rangle &= \frac{1}{\sqrt{2}}, \quad \langle\psi|\mathsf{A}_1\mathsf{B}_1\,|\psi\rangle = -\frac{1}{\sqrt{2}}. \end{aligned} \tag{21}$$

Let us define vectors

$$\begin{aligned} \mathbf{a}_0 &\equiv \frac{1}{\sqrt{2}}(\mathsf{A}_0 + \mathsf{A}_1)\,|\psi\rangle\,, & \mathbf{a}_1 &\equiv \frac{1}{\sqrt{2}}(\mathsf{A}_0 - \mathsf{A}_1)\,|\psi\rangle\,, \\ \mathbf{b}_0 &\equiv \mathsf{B}_0\,|\psi\rangle\,, & \mathbf{b}_1 &\equiv \mathsf{B}_1\,|\psi\rangle\,. \end{aligned}$$

Equations (21) imply the following inner product values:

$$\mathbf{a}_0 \cdot \mathbf{b}_0{}^\dagger = 1, \qquad \mathbf{a}_1 \cdot \mathbf{b}_1{}^\dagger = 1. \tag{22}$$

The Cauchy-Bunyakovski-Schwarz inequality $\mathbf{a} \cdot \mathbf{b}^\dagger \leq |\mathbf{a}||\mathbf{b}|$ implies

$$|\mathbf{a}_i||\mathbf{b}_i| \geq 1 \qquad \text{for} \quad i = 0, 1,$$

where $|\mathbf{a}_i| = \sqrt{\mathbf{a}_i \cdot \mathbf{a}_i{}^\dagger}$. Since operators A_i and B_j are unitary, vectors $\mathbf{b}_0$ and $\mathbf{b}_1$ have unit norm, which implies

$$|\mathbf{a}_i| \geq 1, \qquad \text{for} \quad i = 0, 1. \tag{23}$$

The norms of the vectors $\mathbf{a}_0$ and $\mathbf{a}_1$ satisfy

$$|\mathbf{a}_0|^2 + |\mathbf{a}_1|^2 = 2 \tag{24}$$

by construction, which together with (23) implies $|\mathbf{a}_0| = |\mathbf{a}_1| = 1$. Since eqs. (22) represent the saturation of the Cauchy-Bunyakovski-Schwarz inequality, vectors $\mathbf{a}_i$ and $\mathbf{b}_i$ for $i = 0, 1$ must be parallel, i.e. $\mathbf{b}_i = \mathbf{a}_i$. This implies

$$\begin{aligned} &\{\mathsf{B}_0, \mathsf{B}_1\}\,|\psi\rangle = (\mathsf{B}_0\mathsf{B}_1 + \mathsf{B}_1\mathsf{B}_0)\,|\psi\rangle \\ =&\frac{(\mathsf{A}_0 - \mathsf{A}_1)\mathsf{B}_0 + (\mathsf{A}_0 + \mathsf{A}_1)\mathsf{B}_1}{\sqrt{2}}\,|\psi\rangle \\ =&\frac{(\mathsf{A}_0 - \mathsf{A}_1)(\mathsf{A}_0 + \mathsf{A}_1) + (\mathsf{A}_0 + \mathsf{A}_1)(\mathsf{A}_0 - \mathsf{A}_1)}{2}\,|\psi\rangle \\ =&0, \end{aligned} \tag{25}$$

and thus B_0 and B_1 anti-commute on the support of $|\psi\rangle$. Note that since the correlations are symmetric, the same result holds for Alice's observables.

4.2 Algebraic proof of anticommutativity

In principle, it is not easy to find correlations which self-test some state and measurements. Natural candidates, however, are correlations that maximally violate a particular Bell inequality. Moreover, the structure of the Bell inequality can be useful for proving self-testing statements, especially in cases when simple geometric considerations are not possible. Here we show how one can deduce an anticommutation relation for Bob's observables from the observation $\beta_{\text{CHSH}} = 2\sqrt{2}$. As a starting point we take the SOS decomposition of the shifted CHSH Bell operator (see box 4.1 for a summary of SOS decompositions):

$$\begin{aligned} &2\sqrt{2}\mathbb{1} - \mathcal{B}_{\text{CHSH}} = \\ &\frac{1}{\sqrt{2}}\left[\left(\frac{\mathsf{A}_0 + \mathsf{A}_1}{\sqrt{2}} - \mathsf{B}_0\right)^2 + \left(\frac{\mathsf{A}_0 - \mathsf{A}_1}{\sqrt{2}} - \mathsf{B}_1\right)^2\right], \end{aligned} \tag{30}$$

which follows from the properties (20). For any state $|\psi\rangle$ leading to $\beta_{\text{CHSH}} = 2\sqrt{2}$, i.e. $\langle\psi|\mathcal{B}_{\text{CHSH}}\,|\psi\rangle = 2\sqrt{2}$ we thus have

$$\frac{\mathsf{A}_0 \pm \mathsf{A}_1}{\sqrt{2}}\,|\psi\rangle = \mathsf{B}_{0/1}\,|\psi\rangle\,, \tag{31}$$

as explained in equation (28) in box 4.1. With these relations we can prove that B_0 and B_1 anticommute in the same way we did in (25).

4.3 Swap gate

We now prove a formal self-testing statement for the state $|\phi^+\rangle$ in the form of definition 1. This will require proving the existence of an isometry Φ mapping the physical state $|\psi\rangle$ to our reference state $|\psi'\rangle = |\phi^+\rangle$. In the majority of self-testing proofs the isometry is explicitly constructed and in most cases it takes the form of the partial Swap gate given in figure 4.

The main idea behind this particular isometry is as follows. In the case that the physical state is a two-qubit state and the operators are $\mathsf{Z}_\text{A} = \sigma_\text{z}^\text{A}$, $\mathsf{X}_\text{A} = \sigma_\text{x}^\text{A}$, $\mathsf{Z}_\text{B} = \sigma_\text{z}^\text{B}$ and $\mathsf{X}_\text{B} = \sigma_\text{x}^\text{B}$, the action of the circuit is to swap the physical state with the state $|00\rangle$ of the registers A and B. Of course, given the device-independent scenario we cannot

Box 4.1: SOS decompositions

To every Bell inequality $\mathcal{I} = \sum_{a,b,x,y} w_{ab}^{xy} p(a,b|x,y)$ corresponds a Bell operator

$$\mathcal{B} = \sum_{a,b,x,y} w_{ab}^{xy} \mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y} \tag{26}$$

such that the violation is obtained as $\beta = \mathrm{tr}\left[\mathcal{B}\rho\right]$. If the maximal violation achievable by using quantum resources (*i.e.* the quantum bound) is β_Q the *shifted Bell operator* is defined as $\beta_Q \mathbb{1} - \mathcal{B}$. Every shifted Bell operator is by construction positive semidefinite since $\langle\psi|\mathcal{B}\,|\psi\rangle \leq \beta_Q$ for all $|\psi\rangle$. Imagine the shifted Bell operator admits a decomposition

$$\beta_Q \mathbb{1} - \mathcal{B} = \sum_{\lambda} P_\lambda^\dagger P_\lambda, \tag{27}$$

where each P_λ is a polynomial in the operators $\mathsf{M}_{a|x}$ and $\mathsf{N}_{b|y}$. The decomposition (27) is called a *sum of squares (SOS) decomposition* of the shifted Bell operator. If the polynomials are of degree at most n in either $\mathsf{M}_{a|x}$ or $\mathsf{N}_{a|x}$ we say the SOS decomposition is of n-th degree.
SOS decompositions for Bell inequalities are typically hard to find. One can use numerical methods to find SOS decompositions of various degrees via the NPA hierarchy [NPA07, NPA08] (in particular, see [PNA10] for a link to SOS decompositions).
SOS decompositions allow one to extract potentially useful information about the physical state $|\psi\rangle$ and measurements used to achieve the maximal violation of the corresponding Bell inequality. From (27) we have

$$\begin{aligned} \langle\psi|\beta_Q\mathbb{1} - \mathcal{B}\,|\psi\rangle = 0 \quad &\Rightarrow \quad \sum_\lambda \langle\psi|P_\lambda^\dagger P_\lambda\,|\psi\rangle = 0 \quad \Rightarrow \quad \sum_\lambda \|P_\lambda\,|\psi\rangle\,\|^2 = 0 \\ &\Rightarrow \quad P_\lambda\,|\psi\rangle = 0 \qquad \forall\lambda \end{aligned} \tag{28}$$

Since P_λ is a function of the operators used to obtain the maximal violation, the relations of the form $\{P_\lambda\,|\psi\rangle = 0\}_\lambda$ often represent nontrivial statements about the strategy used to maximally violate the Bell inequality under consideration. Additionally, if a non-maximal violation $\beta_Q - \epsilon$ is observed the approximate relations analogous to (28) can be obtained:

$$\langle\psi|\beta_Q\mathbb{1} - \mathcal{B}\,|\psi\rangle = \epsilon \qquad \Rightarrow \qquad \|P_\lambda\,|\psi\rangle\,\| \leq \sqrt{\epsilon} \qquad \forall\lambda \tag{29}$$

These relations are often significant for proving robust self-testing statements.

assume that the physical state is a two-qubit state or any particular form of the operators. However, from sections 4.1 and 4.2, we know that like σ_z, σ_x, the operators A_0, A_1 and B_0, B_1 anti-commute on the support of the state. The idea is then to use these operators to create new operators Z_A, X_A, Z_B, X_B which act in an analogous way to σ_z, σ_x on $|\psi\rangle$. Since we expect our physical state to be $|\phi^+\rangle$ (up to a local isometry), the hope is that by using these operators in the place of σ_z and σ_x one will still be able to extract $|\phi^+\rangle$ into the ancilla space. Indeed, this is the case. More precisely, we choose

$$\begin{aligned} \mathsf{Z}_\mathrm{A} &= \frac{1}{\sqrt{2}}(\mathsf{A}_0 + \mathsf{A}_1), \qquad & \mathsf{X}_\mathrm{A} &= \frac{1}{\sqrt{2}}(\mathsf{A}_0 - \mathsf{A}_1), \\ \mathsf{Z}_\mathrm{B} &= \mathsf{B}_0, & \mathsf{X}_\mathrm{B} &= \mathsf{B}_1. \end{aligned} \tag{32}$$

Note that we have

$$\{\mathsf{Z}_\mathrm{A}, \mathsf{X}_\mathrm{A}\} = 0 \tag{33}$$

by construction and

$$\{\mathsf{Z}_\mathrm{B}, \mathsf{X}_\mathrm{B}\}\,|\psi\rangle = 0 \tag{34}$$

from (25). Furthermore from (31) we have

$$\mathsf{Z}_\mathrm{A}\,|\psi\rangle = \mathsf{Z}_\mathrm{B}\,|\psi\rangle\,, \quad \mathsf{X}_\mathrm{A}\,|\psi\rangle = \mathsf{X}_\mathrm{B}\,|\psi\rangle\,. \tag{35}$$

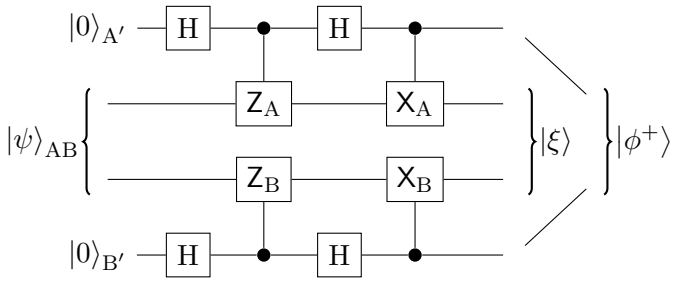


Figure 4: The partial swap gate isometry used to self-test the maximally entangled state of two qubits. H is the Hadamard gate. After the application of the circuit, the maximally entangled state is extracted from $|\psi\rangle$ to the ancilla qubits.

In order for Φ to be a valid isometry, Z_A, X_A, Z_B and X_B must be unitary. This is automatically the case for Z_B and X_B (see (20)), however it is not necessarily the case for Z_A and X_A. To deal with this problem, we need to *regularise* these operators so that they are unitary. Formally, to regularise a Hermitian operator Z, one changes all zero eigenvalues of Z to 1, resulting in a new Hermitian operator Z^*. The regularised operator is then obtained by normalising the eigenvalues of Z^*, i.e. $\hat{Z} = |Z^*|^{-1}Z^*$. Note that $\hat{Z}$ is unitary by construction. One can often show that the regularised operators act in same way as the original operators on the physical state, i.e. $\hat{Z}\,|\psi\rangle = Z\,|\psi\rangle$. This is indeed the case for our example (see appendix A.2). From hereon we therefore take Z_A and X_A to be the regularised unitary operators and continue to use the substitutions (32) without problem.

After a straightforward calculation one finds that the output of the isometry is

$$\begin{aligned}\Phi[|\psi\rangle] = \frac{1}{4}\Big[&|00\rangle \otimes (\mathbb{1}+\mathsf{Z}_\mathrm{A})(\mathbb{1}+\mathsf{Z}_\mathrm{B})\,|\psi\rangle \\ &+ |01\rangle \otimes (\mathbb{1}+\mathsf{Z}_\mathrm{A})\mathsf{X}_\mathrm{B}(\mathbb{1}-\mathsf{Z}_\mathrm{B})\,|\psi\rangle \\ &+ |10\rangle \otimes \mathsf{X}_\mathrm{A}(\mathbb{1}-\mathsf{Z}_\mathrm{A})(\mathbb{1}+\mathsf{Z}_\mathrm{B})\,|\psi\rangle \\ &+ |11\rangle \otimes \mathsf{X}_\mathrm{A}(\mathbb{1}-\mathsf{Z}_\mathrm{A})\mathsf{X}_\mathrm{B}(\mathbb{1}-\mathsf{Z}_\mathrm{B})\,|\psi\rangle\Big],\end{aligned}$$

or in more compact form

$$\Phi[|\psi\rangle] = \sum_{i,j\in\{0,1\}} |ij\rangle_{\mathrm{A'B'}} \otimes \hat{f}_{ij}\,|\psi\rangle_{\mathrm{ABP}}\,, \qquad (36)$$

where

$$\hat{f}_{ij} = \frac{1}{4}\mathsf{X}_\mathrm{A}^i(\mathbb{1}+(-1)^i\mathsf{Z}_\mathrm{A})\mathsf{X}_\mathrm{B}^j(\mathbb{1}+(-1)^j\mathsf{Z}_\mathrm{B}).$$

Using (35) expressions of the form $(\mathbb{1}\pm\mathsf{Z}_\mathrm{A})(\mathbb{1}\mp\mathsf{Z}_\mathrm{B})\,|\psi\rangle$ are automatically equal to zero, setting $\hat{f}_{01}\,|\psi\rangle = \hat{f}_{10}\,|\psi\rangle = 0$. The expression $\hat{f}_{11}\,|\psi\rangle$ can be simplified in the following manner:

$$\begin{aligned}\hat{f}_{11}\,|\psi\rangle &= \frac{1}{4}\mathsf{X}_\mathrm{A}(\mathbb{1}-\mathsf{Z}_\mathrm{A})\mathsf{X}_\mathrm{B}(\mathbb{1}-\mathsf{Z}_\mathrm{B})\,|\psi\rangle \\ &= \frac{1}{4}(\mathbb{1}+\mathsf{Z}_\mathrm{A})\mathsf{X}_\mathrm{A}(\mathbb{1}+\mathsf{Z}_\mathrm{B})\mathsf{X}_\mathrm{B}\,|\psi\rangle \\ &= \frac{1}{4}(\mathbb{1}+\mathsf{Z}_\mathrm{A})(\mathbb{1}+\mathsf{Z}_\mathrm{B})\,|\psi\rangle \\ &= \hat{f}_{00}\,|\psi\rangle\end{aligned}$$

The second line is obtained by using anticommutativity relations (33) and (34), while (35) and the unitarity of X_B was used to obtain the third line. Finally we see that the output of the Swap isometry is

$$\Phi[|\psi\rangle_{\mathrm{ABP}}] = |\phi^+\rangle_{\mathrm{A'B'}} \otimes |\xi\rangle_{\mathrm{ABP}}\,, \qquad (37)$$

where $|\xi\rangle = \sqrt{2}\hat{f}_{00}\,|\psi\rangle$. Note that $|\xi\rangle$ is necessarily normalised since the circuit of figure 4 is unitary. We have thus self-tested the state $|\phi^+\rangle$ in the sense of definition 1. Although we have worked with a purification of the physical state, the isometry does not act on the purification space, as needed from definition 1. This is because Φ is constructed from the measurement operators themselves, which by assumption act only on the local Hilbert spaces of Alice and Bob and therefore not on the purification space of $|\psi\rangle$.

4.3.1 Partial vs full Swap gates

The partial Swap gate was used in self-testing protocols for the first time in [MYS12] and in a large number of self-testing proofs since then. The full Swap gate differs from the partial one in that it contains another controlled gate before the first Hadamard is applied to the ancillary qubit. This controlled gate can be omitted if the ancilla

is initiated in the state $|0\rangle$. In order to get better robust self-testing protocols it might be useful that Alice and Bob each have a local pair of maximally entangled ancillas. In this case the full Swap gate has to be used (see [McK16a]). The generalisation of the Swap gate useful for self-testing states of local dimension larger than two is introduced in [YN13]. For more details on different types of Swap gates used for self-testing see Appendix A.3.

4.4 Self-testing of measurements

The measurements Alice and Bob use to maximally violate the CHSH inequality can also be self-tested via the Swap isometry. Here we explicitly show how to self-test Bob's measurement observable B_0. For that purpose we check how the partial Swap gate transforms the state $\mathsf{B}_0|\psi\rangle$, which can also be written as $\mathsf{Z}_\mathrm{B}|\psi\rangle$:

$$\begin{aligned}\Phi[\mathsf{B}_0|\psi\rangle] &= \sum_{i,j\in\{0,1\}} |ij\rangle_{\mathrm{A'B'}}\,\hat{f}_{ij}\mathsf{B}_0|\psi\rangle \\ &= \sum_{i,j\in\{0,1\}} |ij\rangle_{\mathrm{A'B'}}\,\hat{g}_{ij}|\psi\rangle\,,\end{aligned}$$

where

$$\begin{aligned}\hat{g}_{ij} &= \frac{1}{4}\mathsf{X}_\mathrm{A}^i(\mathbb{1}+(-1)^i\mathsf{Z}_\mathrm{A})\otimes\mathsf{X}_\mathrm{B}^j(\mathbb{1}+(-1)^j\mathsf{Z}_\mathrm{B})\mathsf{Z}_\mathrm{B} \\ &= \frac{1}{4}\mathsf{X}_\mathrm{A}^i(\mathbb{1}+(-1)^i\mathsf{Z}_\mathrm{A})\otimes\mathsf{X}_\mathrm{B}^j((-1)^j\mathbb{1}+\mathsf{Z}_\mathrm{B}) \\ &= (-1)^j\hat{f}_{ij}.\end{aligned}$$

This relation implies $\hat{g}_{01}=\hat{g}_{10}=0$ and $\hat{g}_{11}=-\hat{g}_{00}$. Thus the output of the Swap isometry will be

$$\Phi(\mathsf{B}_0|\psi\rangle) = (\mathbb{1}\otimes\sigma_\mathrm{z}|\phi^+\rangle_{\mathrm{A'B'}})\otimes|\xi\rangle_{\mathrm{ABP}}\,, \quad (38)$$

i.e. the measurement observable acts on the support of $|\psi\rangle$ as σ_z. A similar method can be used to self-test all other measurement observables used for the maximal CHSH violation. Note that (38) implies a self-test of the measurement operators. Since from (19) one has $\mathsf{N}_{b|0}=(\mathbb{1}+b\mathsf{B}_0)/2$ it follows by linearity of Φ that

$$\Phi(\mathsf{N}_{b|0}|\psi\rangle) = \left(\mathbb{1}\otimes\frac{\mathbb{1}+b\sigma_\mathrm{z}}{2}|\phi^+\rangle_{\mathrm{A'B'}}\right)\otimes|\xi\rangle\,. \quad (39)$$

Combining this and the previous section, we can prove a full state and measurement self-testing statement as follows. This concludes the introductory sections of the review.

Self-testing statement for the CHSH inequality

Let $\{|\psi\rangle_{\mathrm{ABP}}\,,\mathsf{A}_0,\mathsf{A}_1,\mathsf{B}_0,\mathsf{B}_1\}$ be the state and the ±1 valued observables maximally violating the CHSH inequality. Then there exists a local isometry Φ such that

$$\begin{aligned}\Phi(|\psi\rangle) &= |\phi^+\rangle\otimes|\xi\rangle\,,\\ \Phi(\mathsf{A}_0|\psi\rangle) &= (\frac{\sigma_\mathrm{x}+\sigma_\mathrm{z}}{\sqrt{2}}\otimes\mathbb{1}\,|\phi^+\rangle)\otimes|\xi\rangle\\ \Phi(\mathsf{A}_1|\psi\rangle) &= (\frac{-\sigma_\mathrm{x}+\sigma_\mathrm{z}}{\sqrt{2}}\otimes\mathbb{1}\,|\phi^+\rangle)\otimes|\xi\rangle\,,\\ \Phi(\mathsf{B}_0|\psi\rangle) &= (\mathbb{1}\otimes\sigma_\mathrm{z}\,|\phi^+\rangle)\otimes|\xi\rangle\,,\\ \Phi(\mathsf{B}_1|\psi\rangle) &= (\mathbb{1}\otimes\sigma_\mathrm{x}\,|\phi^+\rangle)\otimes|\xi\rangle\,.\end{aligned}$$

for some state $|\xi\rangle$.

---

5 Self-testing of bipartite states

In this section we give an overview of the existing results in the self-testing of bipartite quantum states. All of the results are for the self-testing of pure states, since mixed states cannot be self-tested (see section 3.5). In 5.1 we present the known results from self-testing qubit states, focusing first on the large literature dedicated to the maximally entangled pair of qubits. In 5.2 we move to self-testing of bipartite states of a higher local dimension. Finally, in 5.3 we review the results and methods to self-test many copies of the maximally entangled pair of qubits.

5.1 Self-testing of two-qubit states

5.1.1 The maximally entangled pair of qubits

The fact that the maximal violation of the CHSH inequality can be obtained only by using the maximally entangled pair of qubits or a mixture of maximally entangled qubit states corresponding to different degrees of freedom was reported already in [SW87, PR92, BMR92, Tsi93]. An alternative method to self-test the maximally entangled pair of qubits is presented in [MY04], today mostly known as the Mayers-Yao self-test. While [SW87, PR92, BMR92, Tsi93] can be considered as the avant-garde self-testing papers, [MY04] stands out as the founding work which defined self-testing as a protocol 'on its own' and pointed out its importance. It is worth mentioning that Mayers and Yao made a similar statement already

in [MY98], where they called the reference correlations 'self-checking'. In the Mayers-Yao protocol, Alice and Bob both measure three observables, σ_z, σ_x and $(\sigma_z + \sigma_x)/\sqrt{2}$. The proof is geometric in spirit and the isometry the authors use does the same job as the Swap gate, but the authors do not make the connection to the idea of applying a swap unitary. The self-test was made robust in [MMMO06]. A simplified proof of the Mayers-Yao self-test, in which Alice makes the same measurements, while Bob measures only σ_z and σ_x appeared in the supplementary material of [McK14].

The concept of robustness and relevant figures of merit when self-testing the maximally entangled pair of qubits were introduced in [BLM+09], alongside with some explicitly calculated robustness bounds. The first completely device-independent robust self-test of the maximally entangled pair of qubits, both CHSH and Mayers-Yao based, appeared in [MYS12]. Further inequivalent proofs for self-testing the maximally entangled pair of qubits were reported in [MS13], where the authors gave a condition for a given binary XOR game to be a robust self-test, and in [ŠASA16], where the chained Bell inequalities were used to self-test the maximally entangled state and an arbitrary number of real measurements. An improvement of the robustness bounds were provided numerically in [YVB+14] and [BNS+15], and analytically in [Kan17], which is currently the best self-test of the maximally entangled pair of qubits in terms of robustness. An important contribution to the self-testing of the maximally entangled pair of qubits is [WWS16], which characterises all the correlations that self-test the state using two dichotomic measurements per party. The robustness of these self-tests was estimated in [LWH+19].

All the results presented so far used only real measurements. The self-testing of maximally entangled pairs of qubits using σ_y observables was introduced in [MM11] based on the chained Mayers-Yao conditions, also in [APVW16] and [ABB+17] based on the elegant Bell inequality [Gis09], and in [Kan17] based on the extended version of CHSH introduced in [Slo11] (more on the issue of self-testing complex measurements will follow in section 8.2.1).

5.1.2 Self-testing of partially entangled states

All pure entangled states of two qubits admit a Schmidt decomposition

$$|\psi_\theta\rangle = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle \qquad \theta \in (0, \pi/4]. \tag{40}$$

Such states are known as partially entangled pairs of qubits, and they maximally violate the tilted CHSH inequalities [AMP12]:

$$\alpha\langle A_0\rangle + \langle A_0 B_0\rangle + \langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle \leq 2 + \alpha.$$

The maximal quantum violation $\sqrt{8 + 2\alpha^2}$ is achieved by the corresponding partially entangled state (40) for $\tan 2\theta = \sqrt{2\alpha^{-2} - 1/2}$. To achieve the maximal violation Alice measures $A_0 = \sigma_z$ and $A_1 = \sigma_x$ while Bob measures $B_0 = \cos\mu\,\sigma_z + \sin\mu\,\sigma_x$ and $B_1 = \cos\mu\,\sigma_z - \sin\mu\,\sigma_x$, with $\tan\mu = \sin 2\theta$. The proof that the maximal violation of the tilted CHSH inequality self-tests the corresponding partially entangled pair of qubits appeared in [YN13]. It relied on an SOS decomposition of the shifted Bell operator, but the proof appeared to have an error which made the self-testing proof invalid. The work [BP15] introduced a systematic way to find SOS decompositions for arbitrary shifted Bell operators. A whole family of SOS decompositions corresponding to the tilted CHSH Bell operator is introduced which was used to show that every tilted CHSH inequality self-tests the corresponding partially entangled pair of qubits. Improved robustness bounds for self-testing partially entangled pairs of qubits through violation of the tilted CHSH inequalities were presented in [CKS19]. Two different Bell inequalities, inequivalent to the tilted CHSH inequality and useful for self-testing the partially entangled pairs of qubits appeared in [BAŠ+20] and [WBSS18].

The nonlocal character of partially entangled pairs of qubits can be assessed through the Hardy test [Har92, Har93]. In [RZS12] it is proven that Hardy test can be used as a robust self-test for the following states

$$|\psi_\varphi\rangle = \alpha(|01\rangle + |10\rangle) + e^{i\varphi}\sqrt{1 - 2\alpha^2}\,|11\rangle\,,$$

where $a = \sqrt{(3 - \sqrt{5})/2}$ and φ is a free parameter.

A recent contribution [WKB+19] presents a self-test for any partially entangled pair of qubits and all three Pauli measurements (up to complex conjugation) on Alice's side. Bob needs to

apply six measurements. The self-test is proven from the value of three Bell inequalities; two maximally violated tilted CHSH inequalities and one non-maximally violated CHSH inequality.

5.2 Self-testing of qudit states

The self-testing of bipartite entangled states of higher local dimension (qudits) is more complicated task than the self-testing of qubit states. The good understanding of the qubit case has inspired the use of methods that we call 'subspace methods' in which different two-qubit subspaces of the state are self-tested until enough information is gained to self-test the full state. In subsection 5.2.1 we review this approach, before focusing on more genuinely d-dimensional methods in subsections 5.2.2 and 5.2.3. Some states of local dimension 2^n can be seen as a tensor product of n qubit states. In such cases the so-called parallel self-testing is often used, described in section 5.3.

5.2.1 Subspace methods

Self-testing of maximally entangled states of any dimension is discussed for the first time in [YN13]. The isometry for self-testing introduced there is a high-dimensional generalisation of the Swap gate. The authors provided a set of correlations which self-test the maximally entangled state of two qudits

$$\left|\Phi_d^+\right\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle \,. \tag{41}$$

One party performs three measurements and the other four. The idea is to self-test separately maximally entangled subnormalised substates $|\psi_{0,1}\rangle = |00\rangle + |11\rangle$, $|\psi_{2,3}\rangle = |22\rangle + |33\rangle$, $\cdots$, $|\psi_{d-2,d-1}\rangle = |d-2,d-2\rangle + |d-1,d-1\rangle$. This can be done if all of the substates maximally violate the CHSH inequality (although in [YN13] the authors used a different correlation to test the substates). For this, both parties apply the measurements which are direct sums of the ideal CHSH measurements. This step is not enough, since the mixed state $1/d \sum_{i=0}^{d-2} |\psi_{i,i+1}\rangle \langle\psi_{i,i+1}|$ could also pass the test. Another necessary step is self-testing of the substates $|\psi_{d-1,0}\rangle$, $|\psi_{1,2}\rangle$ and so on. It is clear that the mixed state given above cannot provide correlations necessary for this step, where the two parties use again measurements which are the direct sum of the ideal CHSH measurements in a shifted basis, i.e. they now self-test the states $|\psi_{1,2}\rangle, |\psi_{3,4}\rangle, \cdots, |\psi_{d-1,0}\rangle$. The direct sum of σ_z measurements are the same in both bases, thus one party applies three measurements in total while the other applies four.

An arbitrary pure bipartite state admits the Schmidt decomposition

$$|\psi\rangle = \sum_{i=0}^{d-1} \lambda_i |ii\rangle \,. \tag{42}$$

The generalisation of the above explained method to self-testing states of the form (42) is given in [CGS17]. In the first step the sub-states $|\psi_{i,i+1}\rangle = \lambda_i |ii\rangle + \lambda_{i+1} |i+1,i+1\rangle$ for $i = 0,\cdots,d-2$ are self-tested via the maximal violation of the tilted CHSH inequalities. The second step self-tests the shifted states $|\psi_{i,i+1}\rangle = \lambda_i |ii\rangle + \lambda_{i+1} |i+1,i+1\rangle$ for $i = 1,\cdots,d-1$. This result completed the problem of self-testing all bipartite pure states. The Bell inequalities corresponding to this type of the self-test for maximally entangled states are described in [Col18].

5.2.2 Self-testing from qudit correlations

The method for self-testing all pure bipartite entangled states presented in the previous section relied on self-testing two-qubit sub-states. The measurements used in the self-test were also block-diagonal, where all blocks were either 2×2 or 1×1. It is surprisingly difficult to prove self-testing statements about high-dimensional states without resorting to such methods. In this section we outline a few protocols for self-testing qudit states that use genuinely qudit measurements.

The first such results were proven in [BNS+15], [YVB+14] and [SAT+17] where two-qutrit states were self-tested by using the numerical Swap method (for details see section 7.1.4). In [BNS+15] and [YVB+14] the maximal violation of the CGLMP inequality [CGL+02] was used to self-test the partially entangled state of two qutrits:

$$|\psi\rangle = \frac{1}{\sqrt{2+\gamma^2}} \left(|00\rangle + \gamma |11\rangle + |22\rangle\right) \tag{43}$$

where $\gamma = (\sqrt{11} - \sqrt{3})/2$, and in [SAT+17] the SATWAP Bell inequality is introduced and used to self-test the maximally entangled pair of qutrits.

An important contribution in this direction is the analytic self-test presented in [KŠT+19]. The maximally entangled pair of qutrits is self-tested through the maximal violation of a generalised CHSH inequality. These inequalities, introduced in [KŠT+19] can be seen as a special class of Buhrman-Massar inequalities [BM05], represent good candidates for self-testing maximally entangled states in any prime dimension d. Alice and Bob, both have d inputs, and the measurements necessary for the maximal violation are mutually unbiased bases. For higher dimensions, the SOS-decomposition of the shifted Bell operator is provided, but the self-testing statement is still lacking. In fact, for $d = 5$ and $d = 7$, it is proven that the maximal violation can be achieved by using inequivalent quantum realisations, however all of them involve the maximally entangled state in dimensions 5 and 7, respectively.

Another contribution to self-testing maximally entangled states of qudits in the context of nonlocal games is given in [Man14]. There, the author considers a specific type of nonlocal games, the so-called pseudo-telepathy weak projection games. A nonlocal game is called pseudo-telepathy game if it can be won with probability equal to one by using quantum finite dimensional strategy, but cannot be won by using classical strategies [BBT05]. Weak projection games belong to a sub-class of pseudo-telepathy games and [Man14] shows that every such game can be used to self-test maximally entangled states in finite dimensions.

5.2.3 Group theoretic tools

Self-testing properties of non-local games were elaborately explored in [Slo11] and [CS17b]. The common method for both works is the 'algebraisation' of the winning strategies in nonlocal games. The idea of relating representations of a Clifford algebra to the optimal strategies to win the CHSH game was used already in [SW87] and [Tsi87]. In [Slo11], to each XOR game $\mathcal{G}$ is associated a C^* algebra $\mathcal{A}$, such that optimal strategies to win $\mathcal{G}$ correspond to representations of $\mathcal{A}$. Furthermore, there is a relation between near-optimal strategies and approximate representations. Using these techniques a self-testing statement for high-dimensional maximally entangled states via a generalisation of the CHSH game is implicitly given in [Slo11].

In [CS17b], the authors study self-testing properties of a class of pseudo-telepathy games, known as linear-constraint system games, of which the magic square and magic pentagram games are two popular examples [Per90, Mer90b]. In these games, the players are asked for assignments to a subset of variables in a system of linear equations, and they win the game if they return consistent and valid assignments. The authors extend the representation theoretic framework of [CM14], [CLS17] and [Slo20] and obtain a generic self-testing result for linear-constraint system games of a certain kind. They apply this result to obtain a self-testing protocol for a tensor product of n maximally entangled pairs of qubits. The self-testing condition is the perfect score in either the magic square game or the magic pentagram game. It is proven in [CM14] that perfect strategy for every linear-constraint system game which is also a pseudo-telepathy game must involve a maximally entangled state. On the other side in [CLS17] it is shown that a solution group can be associated to every linear-constraint system game. Moreover, the operators used in the winning strategy must satisfy certain algebraic relations determined by the solution group. In [CS17b] the authors use these results and by exploiting algebraic properties of the solution group corresponding to the magic square and magic pentagram games prove the self-testing statement for a tensor product of maximally entangled pairs of qubits. The self-test is also proven to be robust.

5.3 Self-testing n maximally entangled pairs of qubits

In this section we outline methods and results for self-testing n copies of the maximally entangled state of two qubits (which itself is a maximally entangled state of dimension 2^n). Here, there are two main approaches; *sequential self-testing* and *parallel self-testing*.

5.3.1 Sequential self-testing

The first result relating to the self-testing of n maximally entangled pairs of qubits (here also called EPR pairs) appeared in [RUV13]. In this scheme, in each round of the experiment the devices receive inputs (x_i, y_i) for $i = 1, \cdots, n$, labelling the measurement bases for i-th maximally entangled pair. The inputs are given to the devices sequentially: first the inputs (x_1, y_1)

are given and the outputs (a_1, b_1) are returned; then the inputs (x_2, y_2) are given and the outputs (a_2, b_2) are returned. This process is continued until the n-th pair of outcomes is collected and it is characterised by the following transcript

$$\begin{aligned} &a_1, b_1 \quad \text{given} \quad x_1, y_1, \\ &a_2, b_2 \quad \text{given} \quad a_1, x_1, x_2, b_1, y_1, y_2, \\ &\qquad \cdots, \\ &a_n, b_n \quad \text{given} \quad a_1, x_1, \cdots, a_{n-1}, x_{n-1}, x_n, b_1, y_1, \\ &\qquad\qquad\qquad\quad \cdots, b_{n-1}, y_{n-1}, y_n \end{aligned}$$

There is no assumption that in each round the source emits the same state and the measurement strategies in the rounds may depend on the inputs and outputs in all previous rounds. In [RUV13] the authors prove that if the parties win CHSH game in $\omega^* n$ rounds, where ω^* is the optimal probability to win the CHSH game, there is isometry mapping the state the parties shared at the beginning of the procedure to the tensor product of n EPR pairs. The result is stated in its robust form: if the parties win CHSH game in $(1-\epsilon)\omega^* n$ rounds, then at the beginning of any randomly chosen block of $m = n^{\Omega(1)}$ rounds the state of the parties can be mapped to a state $f(\epsilon)$-close to the tensor product of m EPR pairs. The drawback of the work is a very low robustness, *i.e.* as ϵ increases the number of rounds necessary to extract a state $f(\epsilon)$-close to m EPR pairs grows very fast.

5.3.2 Parallel self-testing

A more popular approach for self-testing n EPR pairs is parallel self-testing (see figure 5). Here, the inputs are not given sequentially but all at the same time, *i.e.* the devices receive input vectors $\mathbf{x} = (x_1, \cdots, x_n)$, $\mathbf{y} = (y_1, \cdots, y_n)$ and return outputs vectors $\mathbf{a} = (a_1, \cdots, a_n)$, $\mathbf{b} = (b_1, \cdots, b_n)$. In principle this makes it more difficult to prove self-testing statements than in the sequential scenario, since one assumes less structure on how the outcomes are generated. To self-test a single maximally entangled pair we saw in section 4 that it is enough to identify a pair of anticommuting observables. In the case of n pairs, one has not only to find n pairs of anticommuting obervables, but also to show that observables from different pairs mutually commute. An important feature of parallel self-tests is their robustness. A parallel self-test is robust if any

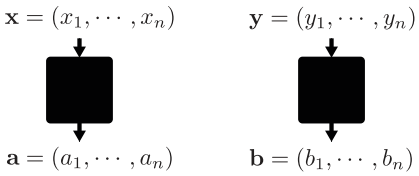


Figure 5: Scenario for parallel self-testing. Alice and Bob both receive a list of n inputs and provide n outputs, which correspond to measurements made on n independent copies of a physical state. The aim is to prove that the statistics self-test n independent copies of the reference state

strategy producing correlations that are ϵ-close to the ideal ones must use a state which is $f(\epsilon, n)$-close to $|\psi'\rangle^{\otimes n}$, where $f(\epsilon, n)$ is a monotonically increasing function in ϵ. How quickly the function $f(\epsilon, n)$ increases with ϵ and n determines how good robustness is.

The first parallel self-test was proven for 2 EPR pairs in [WBMS16]. The work gives two different self-tests: one based on the optimal success in a double use of the CHSH game and the other on the optimal success in the Magic Square game [Mer90b, Per90]. The result was subsequently generalised for arbitrary n: via parallel repetition of the CHSH game in [Col17] and [McK17] and via parallel repetition of the Magic Square Game in [Col17] and [CN16]. The usefulness of the Magic Pentagram game [Mer90b] for self-testing a tensor product of three EPR pairs was proven in [KM18]. Self-testing of n EPR pairs via parallel repetition of the Mayers-Yao self-test is given in [McK16b]. We also note that the self-test [CS17b] discussed in the previous section belongs to this class of parallel self-tests.

In recent years, several works appeared which also managed to self-test n EPR pairs shared by two parties but not by parallel repetition of any single self-test of a single pair. The first of such results was presented in [OV16], based on the XOR games introduced in [Slo11]. Later, self-testing of n EPR pairs with measurements performed on few of them in each round was the subject of [CRSV18]. This self-test is nondestructive: not all entanglement is consumed in the self-test, but can be used for eventual later protocols.

A combination of self-testing based on nonlocal games with the quantum version of the linearity test from [BLR93], named Pauli braiding test [NV17] led to the first self-test of n EPR pairs in which robustness does not get worse if the num-

ber of EPR pairs tested increases. Another parallel self-test keeping this desirable property is presented in [NV18]. The test can be seen as a quantum version of the classical plane-vs-point test for multivariate low-degree polynomials [RS97].

Finally, while all self-tests presented in this section certify n EPR pairs and tensor products of the observables σ_{x} and σ_{z}, it is possible to extend them to involve certification of σ_{y} also. This was first done in [CGJV17] and later in [BŠCA18b], up to the uncertainty of the complex conjugation of the full n-qubit measurement operators as explained in section 3.7.

5.3.3 Overlapping qubits

A standard parallel self-test of n EPR pairs proves the existence of n pairs of anticommuting observables, where any two observables belonging to different anticommuting pairs necessarily commute. As explained in [CRSV17] each anticommuting pair of observables defines a qubit. Hence the dimension of the underlying Hilbert space in this case must be at least 2^n. The main contribution of [CRSV17] is the estimation of the dimension of the underlying Hilbert space if observables from different anticommuting pairs do not commute exactly, which might happen when the self-testing conditions are approximately satisfied. This leads to the concept of 'overlapping qubits', which, depending on the amount of the overlap can be 'packed' in the Hilbert space whose dimension grows polynomially with n.

6 Self-testing of multipartite states

All bipartite pure states admit a Schmidt decomposition, which simplifies the characterisation of bipartite entanglement and the self-testing of bipartite pure states. Multipartite states do not admit such a simple characterisation, although some generalisations of the Schmidt decomposition exist in the entanglement literature [AAC+00, Kra10]. While all bipartite pure entangled states can be self-tested, when it comes to self-testing of multipartite states, only some partial results exist. Furthermore, from a 'loophole free' perspective, multipartite self-testing is considerably more demanding than bipartite self-testing, since it requires space-like separation between multiple measurement devices.

In this chapter we identify four main methods for self-testing multipartite entangled states: self-testing of graph states based on the structure of their stabilizer operators (section 6.1); tailoring Bell inequalities to self-test specific states (section 6.2); reductions to bipartite methods (section 6.3); parallel self-testing of multipartite states (section 6.4); and self-testing from marginal information only (section 6.5).

6.1 Self-testing of graph states from stabilizer operators

The first multipartite states to be self-tested were graph states [McK14]. Formally, given a graph G defined by a set of vertices $V = \{1, \cdots, N\}$ and a set of edges E (pairs of connected vertices of V), the graph state corresponding to G is given by

$$|G\rangle = \prod_{(i,j)\in E} \mathsf{CZ}_{i,j} \, |+\rangle^{\otimes N}, \tag{44}$$

where $\mathsf{CZ}_{i,j}$ is the controlled-σ_{z} two-qubit unitary $\mathsf{CZ} = \mathrm{diag}(1, 1, 1, -1)$ acting on qubits i and j. Equivalently, $|G\rangle$ can be defined as the unique state that is stabilized by (i.e. is a $+1$ eigenstate of) a set of N local stabiliser operators $\sigma_x^i \otimes_{j\in n(i)} \sigma_z^j$, where $n(i)$ is the neighbourhood of vertex i; the set of vertices connected to i on G.

A self-testing protocol for any graph state corresponding to a connected graph is provided in [McK14]. Note that graph states corresponding to graphs that are not connected must be separable with respect to at least one bipartition. The reference measurements needed for the self-testing are given by the stabilizer operators themselves aided by a few measurements generalising those from Mayers-Yao self-test. More specifically, for an arbitrary graph state, one party has to measure three observables: σ_{z}, σ_{x} and $(\sigma_{\mathrm{x}} + \sigma_{\mathrm{z}})/\sqrt{2}$, while all the other parties measure only σ_{x} and σ_{z}. The self-test is robust to small imperfections and the isometry is the multipartite generalisation of the Swap gate.

The approach from [BAŠ+20] can be also placed in the following subsection, but since it is intrinsically related to stabilizers we discuss it in this group. Starting from any graph state, the authors introduce a method to construct a Bell inequality that is maximally violated by the corresponding state. Moreover, the derived Bell inequality can be used to self-test the state. Each

	Robustness	Inputs size (in bits)	Outputs size (in bits)
[BŠCA18b]	$\mathrm{poly}(n, \epsilon)$	$O(n)$	n
[CRSV18]	$\mathrm{poly}(n, \epsilon)$	$O(\log\ n)$	1
[Col17]	$\mathrm{poly}(n, \epsilon)$	$O(n)$	n
[CS17b]	$\mathrm{poly}(n, \epsilon)$	$O(n)$	n
[CGJV17]	$\mathrm{poly}(\epsilon)$	$O(n\ \log\ n)$	2
[CN16]	$\mathrm{poly}(n, \epsilon)$	$O(n)$	n
[McK16b]	$\mathrm{poly}(n, \epsilon)$	$O(n)$	n
[McK17]	$\mathrm{poly}(n, \epsilon)$	$O(n)$	n
[NV17]	$\mathrm{poly}(\epsilon)$	$O(n)$	2
[NV18]	$\mathrm{poly}(\epsilon)$	$O(\mathrm{poly}(\log\ n))$	$\mathrm{poly}(\log\ \log\ n)$
[OV16]	$\mathrm{poly}(n, \epsilon)$	$O(\log\ n)$	1

Table 1: Comparative properties of different self-tests of n EPR pairs. The most important aspect of a self-test of n EPR pairs when it comes to practical usefulness is its robustness to noise (or rigidity). The other relevant property is its complexity, in terms of the size of the inputs. The size of the outputs is also a relevant factor, especially in possible applications for randomness expansion. For now, the self-testing protocol presented in [NV18] has the best properties in terms of the total number of inputs (polynomial) and robustness bounds (independent on n). The papers use different distance measures, but all the bounds given here are in terms of the Euclidean distance using definition 4. The work [CGJV17] self-tests σ_{y} measurements on each EPR pairs, and the number of inputs increases in order to deal with the issue of complex conjugation (see 3.7.1.) If one omits self-testing of σ_{y} from the protocol the number of inputs is $O(n)$.

party measures an anti-commuting pair of observables from the real plane of the Bloch sphere. Beyond graph states, the method can be used to self-test the so-called partially entangled GHZ states $\cos\theta\,|0\rangle^{\otimes n} + \sin\theta\,|1\rangle^{\otimes n}$ for any $n \geq 2$.

6.2 Tailoring Bell inequalities

In [PVN14] the authors introduce a method to build permutationally invariant Bell inequalities with two measurement settings per party useful for self-testing multipartite states. The method is tailored for a specific state $|\psi'\rangle$ and the measurements leading to the maximal violation are chosen from the real plane of the Bloch sphere. A linear program can be used to find a Bell operator, whose eigenstate is $|\psi'\rangle$ and maximises the ratio of the quantum and classical bound. The derived Bell inequality is just a suitable candidate for self-testing, which further must be checked by utilising the numerical Swap method technique (see section 7.1.4). Since the self-testing proof relies on the Swap method, it becomes too costly when the number of parties becomes larger than four. Examples of the successful implementation of this method involve the tripartite W state, the tripartite and four-partite GHZ state and the four-qubit linear cluster state.

Another method for developing Bell inequalities, tailored for self-testing of multipartite qubit states is described in [SBWS18]. As in [PVN14], all parties can perform two different measurements and the constructed Bell inequalities are suitable candidates for self-testing applications. The starting point for choosing a Bell operator is not the permutational invariance, but the structure of the stabilizers of the state. The method can be applied to multipartite states that are not graph states, in which case these stabilizer operators will not all be tensor products of Pauli operators. Of all the Bell operators mimicking the structure of the stabilizers, constructed from the arbitrary two real measurements per party, the optimal candidate is the one whose maximum eigenvalue is the local maximum with respect to the small perturbation of the local measurement directions. The robust self-test is then checked by using semidefinite programming to find the lower bound to the fidelity of the state providing the maximal violation and $|\psi'\rangle$ (see section 7.1.3). As example the authors apply the method to self-test a family of four qubit states $CU_\phi\,|\phi^+\rangle \otimes |\phi^+\rangle$, where $CU_\phi = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \exp[-i\phi\sigma_{\mathrm{x}}]$. Since the self-testing is proven by employing numerical methods, it becomes infeasible when the number of parties increase.

6.3 Reductions to bipartite methods

Self-testing protocols for multipartite states can be constructed by reusing self-testing protocols for bipartite states. The idea is as follows: when $n-2$ parties perform appropriate projective measurements, they might collapse the state of the remaining two parties into some pure bipartite entangled state, which in principle can be self-tested by using methods from section 5. By repeating the process of projecting and self-testing for different pairs of parties one might expect to gather enough information to self-test the whole multipartite state. An important restriction is that the measurement used by any party in the projecting part must be some of the measurement the same party uses in the self-testing part of the protocol.

The idea was first used in [WCY+14] to self-test W-state $|W\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$. Whenever one of the parties performs the measurement in the computational basis and obtains outcome $+1$ the state of the remaining two parties becomes maximally entangled $\sim (|01\rangle + |10\rangle)$. This state can be self-tested by maximally violating the CHSH inequality, for example. The authors of [WCY+14] show that by repeating the above process twice for different parties measuring in the computational basis, the whole state can be self-tested using the Swap isometry. They also show that a similar method, based on self-testing of partially entangled two-qubit states, can be used to self-test states of the form $|W_\gamma\rangle = (|001\rangle + |010\rangle + \gamma\,|100\rangle)/\sqrt{2+\gamma^2}$. The method was generalised in [ŠCAA18] to prove self-testing of all permutationally invariant qubit Dicke states, all qubit graph states, and all multipartite states of any local dimension admitting the Schmidt decomposition $|\psi_\lambda\rangle = \sum_{i=0}^{d-1} \lambda_i\,|i, i, \cdots, i\rangle$, representing the first self-test of a high-dimensional multipartite state. Self-testing of W-states for any number of parties was also proven in [Wu17], and self-testing of all Dicke state was proven in [Fad17].

The self-testing of graph states whose underlying graph is a triangular lattice is shown in [HH18]. The whole graph is shared by three parties and if one party measures its qubits in the σ_z basis it prepares maximally entangled pairs of qubits for the remaining two parties, which are in [HH18] self-tested through the Mayers-Yao criterion.

6.4 Parallel self-testing of multipartite states

In section 5.3 we saw many ways to self-test n EPR pairs by using parallel repetition of CHSH or Magic Square game. Up to date, the only parallel self-test of some multipartite state is shown in [BKM19]. The authors use diagramatic proofs based on categorical quantum mechanics [CK17], to prove that parallel repetition of the GHZ game robustly self-tests n copies of the GHZ state.

6.5 Self-testing using only marginal information

Almost all the protocols for self-testing multipartite states presented so far require measuring full-body correlators, that is, they depend on correlations between all parties. This quickly becomes a practical problem since measuring such correlations is typically experimentally very challenging. The possibility of self-testing by measuring only few-body correlators is the subject of [LCH+18]. The authors use the numerical Swap method (see section 7.1.4) to self-test the tripartite W-state, a class of W-like states $(|001\rangle + |010\rangle + \gamma\,|100\rangle)/\sqrt{2+\gamma^2}$ and the states maximally violating Bell inequalities defined in [TSV+14] by using only two-body correlators. The four-partite W-state is also self-tested using three-body correlators.

7 Robust self-testing of states

It is impossible to meet exactly the conditions for ideal self-testing. On one hand, experimental noise and imperfections undermine hope to reproduce exactly the reference correlations (*i.e.* those obtained by performing reference measurements on the reference quantum state). On the other hand, even if all noise contributions are eliminated, one must work with a finite sample size and so the precise probabilities cannot be known, but only estimated up to some statistical confidence level. In order to make self-testing protocols practically meaningful, it is therefore crucial to make them robust to deviations from the ideal case. For possible definitions of robust self-testing see Defs. 4 and 5.

The first self-testing protocol to be made robust was the Mayers-Yao self-test of maximally

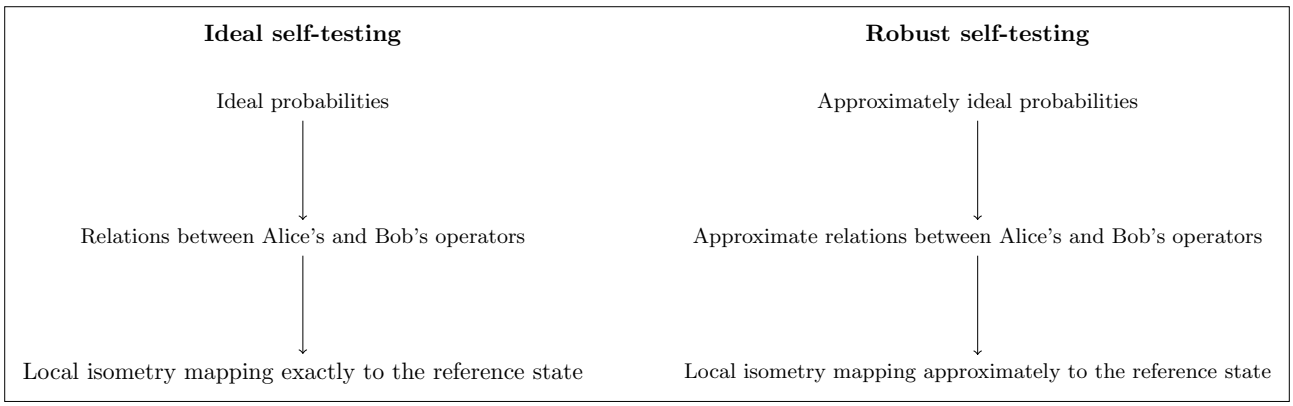


Figure 6: The program for robust self-testing. The aim is to show that approximately satisfied self-testing conditions imply the existance of the local isometry which approximately maps the physical state to the reference one.

entangled pair of qubits [MMMO06]. Robust self-testing through the CHSH inequality was explored in [BLM+09] and simple robust self-testing protocols based on both the Mayers-Yao and the CHSH criterion were presented in [MYS12]. The techniques presented therein remained the main tool for making self-testing protocols robust in the majority of later contributions. As more is known about ideal self-testing the focus of the research is shifting towards finding better techniques for assessing robustness. Arguably, it remains a principal challenge in the field.

In this section we review the main contributions to robust self-testing and the techniques predominantly used in the literature. In section 7.1 we identify and explain five approaches:

- An approach based on the vector norm inequalities (Section 7.1.1);
- Methods relying on the use of Jordan's lemma (Section 7.1.2);
- An approach based on the operator inequalities (Section 7.1.3);
- The numerical Swap method (Section 7.1.4);
- An algebraic method (Section 7.1.5).

Finally, in Section 7.2 we discuss recent progress on noise-tolerant self-testing of a tensor product of many EPR pairs.

7.1 Robust self-testing methods

7.1.1 Norm inequalities method

The bulk of self-testing protocols start from the observed probabilities $p(a,b|x,y) = \langle\psi|\mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y}|\psi\rangle$ or the maximal violation of some Bell inequality and deduce equations of the type (see e.g. (34) and (35) from section 4)

$$f(\{\mathsf{M}_{a|x}\},\{\mathsf{N}_{b|y}\})\,|\psi\rangle = 0, \tag{45}$$

where f is some polynomial function in the measurement operators. Such relations can be drawn from either geometrical arguments (like in [MY04]), algebraic identities (like in [McK14]) or SOS decompositions (like in [BP15]). The relations (45) are a necessary step in proving that the appropriate isometry (the Swap gate in most cases) maps the physical state to the reference one,

$$\Phi(|\psi\rangle) = |\psi'\rangle \otimes |\xi\rangle\,. \tag{46}$$

Although the self-testing proof requires that the correlations be ideal, one could hope to follow the same proof in which the exact relations are exchanged with approximate ones, leading to a noise-dependent bound on the self-tested fidelity. More precisely, when the observed probabilities are within ε distance from the ideal ones (or the violation of the Bell inequality is ε-far from the maximal value), analogously to (45), the aim is to find approximate relations:

$$\|f(\{\mathsf{M}_{a|x}\},\{\mathsf{N}_{b|y}\})\,|\psi\rangle\,\| \leq g_f(\varepsilon), \tag{47}$$

where $\|\cdot\|$ is a vector vector norm (usually taken to be Euclidean) and $g_f(\epsilon)$ are some increasing functions for which $g_f(0) = 0$. One can then often guarantee that the appropriate isometry Φ satisfies

$$\|\Phi(|\psi\rangle) - |\psi'\rangle \otimes |\xi\rangle\,\| \leq g_\Phi(\varepsilon), \tag{48}$$

where g_Φ is obtained by propagating the uncertainties (47) through the isometry circuit.

	Asymptotic behaviour of g_Φ
[MYS12]	$O(\epsilon^{\frac{1}{4}})$
[McK14]	$O(\epsilon^{\frac{1}{4}})$
[BP15]	$O(\epsilon^{\frac{1}{2}})$
[ŠASA16]	$O(\epsilon^{\frac{1}{2}})$
[WCY+14]	$O(\epsilon^{\frac{1}{4}})$

Table 2: Comparative properties of different robust self-tests based on vector norm inequalities.

Relations of the type (47) are usually obtained via various vector norm inequalities, such as Cauchy-Bunyakovski-Schwarz, triangle or Hölder inequalities. These techniques were first used in [MYS12] and later in [McK14, WCY+14]. If a self-testing proof relies on the maximal violation of a Bell inequality, the relations (45) can be conveniently obtained from the SOS decomposition of the shifted Bell operator (see box 4.1 and equation (29) therein). The usefulness of SOS decompositions for robust self-testing was first noted in [YN13] and later used in e.g. [BP15, ŠASA16].

Techniques based on vector norm inequalities are useful in making self-testing protocols robust, but the robustness bounds are typically not very good due to large constants appearing in them. The asymptotic behaviour of the function g_Φ for different self-testing protocols based on this method is given in Table 2.

7.1.2 Utilising Jordan's lemma

One of the main difficulties in the device-independent description of quantum experiments is related to the inability to fix the dimension of the underlying Hilbert space, which prevents the parameterisation of the measurements and states used in the experiment. This difficulty stays the prime hurdle towards calculating robust self-testing bounds. A very useful theoretical asset enabling a solution in scenarios where each party has two dichotomic measurements is the Jordan lemma [PAB+09] (see lemma 2 therein). It allows to effectively reduce an arbitrary-dimensional experiment to the one in which the local subsystems are qubit systems.

For the purposes of robust self-testing the Jordan lemma was first time used in [BLM+09] to obtain robust self-testing of the maximally entangled pair of qubits through violation of the CHSH inequality. Later, it was used in [SBWS18] for the robust self-testing of a arbitrary multipartite states using the Bell inequalities introduced therein and described in section 6.2 of this review. For simplicity, here we give a short description of the method to the bipartite scenario, while keeping in mind that, as described in [SBWS18], it can straightforwardly be applied to the multipartite case.

The Jordan lemma states that given two Hermitian matrices of finite or countably infinite dimension and with eigenvalues ± 1, there exists a unitary transformation that simultaneously block diagonalises them, where each block is of size at most 2×2. Consider a self-testing protocol in which Alice and Bob each have a pair of ± 1 valued observales A_x, $x = 0, 1$ for Alice and B_y, $y = 0, 1$ for Bob. It follows there is a choice of local basis in which these observables take the block structure described above. One can further assume that each of the blocks is of size 2×2, since a one-dimensional block is equivalent to a two-dimensional block where the state has support only on one of these dimensions. One can then apply additional unitary rotations to each of the blocks so that they take real values only. Given this structure, one can paramaterise the observables as follows

$$\begin{aligned} \mathsf{A}_x &= \bigoplus_i \mathsf{A}_i = \bigoplus_i \cos\alpha_i \sigma_{\mathrm{x}} + (-1)^x \sin\alpha_i \sigma_{\mathrm{z}}, \\ \mathsf{B}_y &= \bigoplus_j \mathsf{B}_j = \bigoplus_j \cos\beta_j \sigma_{\mathrm{x}} + (-1)^y \sin\beta_j \sigma_{\mathrm{z}} \end{aligned} \tag{49}$$

This parameterisation covers all possibilities: $\alpha_i = 0$ implies that the observables commute in that block, whereas $\alpha_i = \pi/4$ implies anticommutation in that block. Consequently, the Bell operator can be written as $\mathcal{B} = \oplus_{ij} \mathcal{B}(\mathrm{A}_i, \mathrm{B}_j)$. Following such parametrisation the Bell violation can be written as

$$\beta = \sum_{ij} p_{ij} \mathrm{tr}[\mathcal{B}(\mathrm{A}_i, \mathrm{B}_j)\rho_{ij}] \tag{50}$$

where $p_{ij}\rho_{ij}$ are projections of the physical state ρ onto the blocks of Alice's and Bob's observables. Each block can then be treated separately to achieve an expression of the form

$$F(\Lambda_{\mathrm{A}}^i \otimes \Lambda_{\mathrm{B}}^j(\rho_{ij}), |\psi'\rangle\langle\psi'|) \geq f(\beta). \tag{51}$$

In [SBWS18] it is proven that if f is a convex function of β there exist maps Λ_{A} and Λ_{B} such

that the fidelity between $\Lambda_A \otimes \Lambda_B(\rho)$ and $|\psi'\rangle\langle\psi'|$ given the violation β is lower bounded by $f(\beta)$. In [BLM+09] a similar convexity argument is used to obtain the final bound.

The remaining challenge is to obtain relations of the form (51). In [BLM+09] the problem is solved analytically and the isometry used is just the one that rotates the blocks of the observables to obtain the form given in (49). The work [SBWS18] provides a general recipe: (51) can be solved by using a nonlinear optimisation with one variable per party.

7.1.3 Operator inequalities method

An analytic approach to robust self-testing, introduced in [Kan16] currently gives the best robustness bounds for the self-testing of two-qubit states. It is suited for self-testing protocols based on a Bell inequality violation. The method uses the notion of extraction (see section 3.6.1) and works by proving an operator inequality of the form

$$K \geq s\mathcal{B}_{\mathcal{I}} + \mu\mathbb{1}, \tag{52}$$

for all Bell operators $\mathcal{B}_{\mathcal{I}}$ for the Bell inequality $\mathcal{I}$ in question, where $K = \Lambda_A^\dagger \otimes \Lambda_B^\dagger(|\psi'\rangle\langle\psi'|)$ and $\Lambda^\dagger$ is the dual channel of Λ with respect to the Hilbert-Schmidt inner product. This allows one to make linear robust self-testing statements, that is, to prove the existence of real parameters s and μ such that the extractability-violation trade-off defined in (13) satisfies

$$\mathcal{Q}_{\psi,\mathcal{B}_{\mathcal{I}}}(\beta) \geq s\beta + \mu. \tag{53}$$

One thus has

$$F(\Lambda_A \otimes \Lambda_B(\rho), |\psi'\rangle) \geq s\beta + \mu \tag{54}$$

for all states ρ achieving violation greater that β.

In principle it is a difficult task to prove the operator inequality (52) for all Bell operators regardless of the dimension. In [Kan16] Jordan's lemma is exploited to derive the current best robustness bounds for self-testing the maximially entangled state of two qubits. The method uses the CHSH inequality. The local channel $\Lambda_A \otimes \Lambda_B$ appearing in (54) is as follows. First, local unitary transformations are applied to Alice and Bob's subsystems so that via the Jordan lemma, their local observables take a block diagonal form as in (49). Then, for each block, one applies the α-dependent dephasing channel

$$\Lambda_\alpha[\rho] = \frac{1+g(\alpha)}{2}\rho + \frac{1-g(x)}{2}\Gamma(\alpha)\rho\Gamma(\alpha).$$

Here $g(\alpha) = (1+\sqrt{2})(\sin\alpha + \cos\alpha - 1)$ and

$$\Gamma(\alpha) = \begin{cases} \sigma_x & \alpha \in [0, \pi/4] \\ \sigma_z & \alpha \in (\pi/4, \pi/2]. \end{cases} \tag{55}$$

Bob's channel Λ_B is defined analogously. This choice is shown to imply the lower bound (54) to the fidelity with $s = (2+\sqrt{2})/8$ and $\mu = -(1+2\sqrt{2})/4$ (see figure 7 for a plot).

In [Kan16] inequality (52) is also proven for Mermin inequalities in order to self-test the tripartite GHZ state. Moreover, the fidelity lower bound for the Mermin inequality is proven to be optimal in the sense that for any violation there always exists a state achieving that violation with the self-tested fidelity to the reference state. The method has also been used for robust self-testing of partially entangled pairs of qubits [CKS19] and to assess the performance of different self-tests of a maximally entangled pair of qubits [LWH+19].

7.1.4 Numerical Swap method

The analytic techniques presented in the previous two subsections are only useful for either small amounts of noise (norm inequalities method), or (for now) solvable in simple cases, mostly when each party applies two binary measurements (operator inequalities method). For self-testing protocols which cannot be made robust with analytic methods, one can resort to a numerical method called the Swap method, introduced in [BNS+15, YVB+14]. While its applicability is still limited to simpler protocols due to computational resource requirements, it is responsible for the majority of practically relevant robust self-testing bounds.

The Swap method uses the Swap gate isometry (see section 4.3) and makes use of the fidelity of the extracted state as a figure of merit, as in definition 5. To get a lower bound on the fidelity, one needs to minimise the fidelity between the state of the output registers of the Swap gate and the reference state, given that the input state to the Swap gate provides the violation β. For example, for two-qubit states we have seen in section

Box 7.1: The NPA Hierarchy

In its most general form, the NPA hierarchy [NPA07, NPA08, PNA10] is a method to tackle optimisation problems involving polynomials of non-commuting variables, and as a result is suited to certain optimisation problems in quantum theory. Define optimisation problems of the form

$$\min_{|\psi\rangle,\mathsf{M}_{a|x},\mathsf{N}_{b|y}} \langle\psi|\mathcal{P}(\{\mathsf{M}_{a|x},\mathsf{N}_{b|y}\})\,|\psi\rangle \quad \text{subject to} \quad \langle\psi|\mathcal{F}_i(\{\mathsf{M}_{a|x},\mathsf{N}_{b|y}\})\,|\psi\rangle \geq 0 \;\; \forall i\,, \tag{56}$$

where $\mathcal{P}$ and $\mathcal{F}_i$ are polynomials in the measurement operators $\{\mathsf{M}_{a|x},\mathsf{N}_{b|y}\}_{a,x,b,y}$ and where the dimension of the state and measurement can be potentially infinite. The NPA hierarchy is a sequence of convex optimisation problems that provide increasingly better lower bounds to the optimal solution of the above by relaxing the problem to a minimisation over a larger set. Each of these relaxations can be solved via a corresponding semi-definite program [BV04]. Many problems in quantum information can be cast in the above form, particularly in the device-independent setting where the state and measurements are unknown.

The NPA hierarchy works as follows. Consider a generic state and measurement operators $\{|\psi\rangle\,,\{\mathsf{M}_{a|x}\},\{\mathsf{N}_{b|y}\}\}$. Then, define sets $\mathcal{S}_k$ (each corresponding to a level of the hierarchy) comprised of the identity operator and all (non-commuting) products of operators $\mathsf{M}_{a|x},\mathsf{N}_{b|y}$ up to degree k; e.g. $S_1 = \{\mathbb{1}\} \cup_{a,x} \{\mathsf{M}_{a|x}\} \cup_{b,y} \{\mathsf{N}_{b|y}\}$, $S_{k+1} = S_k \cup_{i,j} \{S_k^{(i)} S_1^{(j)}\}$, where $S_k^{(i)}$ is the i^{th} element of S_k. Define the moment matrix of order k, Γ^k, by $\Gamma^k_{i,j} = \langle\psi|S_k^{(i)\dagger} S_k^{(j)}\,|\psi\rangle$. For any state and measurements $\{|\psi\rangle\,,\{\mathsf{M}_{a|x}\},\{\mathsf{N}_{b|y}\}\}$, the matrix Γ^k is Hermitian positive semidefinite and satisfies some linear constraints given by the orthogonality conditions of the measurement operators. One can thus tackle optimisation problems of the form (56) by minimising the corresponding elements of the matrix Γ_k, under linear constraints on Γ_k and $\Gamma_k \succeq 0$. Such a problem is an instance of a semidefinite program which, via duality theorems, can be run to obtain certified lower bounds to the optimal solution.

4, equation (36) that this fidelity is given by

$$F(\rho_{swap}, |\psi'\rangle) = \sum_{i,j,k,l\in\{0,1\}} c_{ij}^{kl} \langle\psi|\hat{f}_{kl}^\dagger \hat{f}_{ij}\,|\psi\rangle\,,$$

where $\rho_{swap} = \text{tr}_{\text{AB}}\,[\Phi[\rho]]$, and $c_{ij}^{kl} = \langle kl|\psi'\rangle\langle\psi'|ij\rangle$. Note that from the definition of f_{ij}, the above is equal to $\langle\psi|\mathcal{P}(\{\mathsf{A}_a^x,\mathsf{B}_b^y\})\,|\psi\rangle$, where $\mathcal{P}$ is a polynomial in the measurement operators. As a result, lower bounds to the minimum fidelity (subject to a Bell inequality violation) can be found numerically via a corresponding semi-definite program defined by the NPA hierarchy; see box 7.1 for more details.

The first applications of the method are given in [YVB+14, BNS+15], which involve the following self-testing results: the self-test of the singlet state and Bob's measurements from the CHSH inequality, the self-test of the singlet state from the Mayers-Yao criterion, the self-test of partially entangled pair of qubits from the tilted CHSH inequality, the self-test of a pure two qutrit state maximally violating CGLMP [CGL+02] inequality and the self-test of entangling measurements. Subsequently the method has been used to devise robust self-tests of the maximally entangled pair of qutrits [SAT+17], the whole family of pure entangled qutrit states [WPD+18], the three qubit W-state [WCY+14, PVN14], three- and four-qubit GHZ states and the four-qubit linear cluster state [PVN14], a family of tripartite pure states, including the W-state from only marginal information [LCH+18], and a tensor product of two singlet states [WBMS16]. It has also been used to compare the performance of different types of self-tests of the singlet state, presented in [WWS16].

7.1.5 Algebraic method

In section 5.2.2 we discussed self-testing through the 'algebraisation' of the winning strategies in nonlocal games. Let us briefly recall that the crux of the method is associating an algebraic

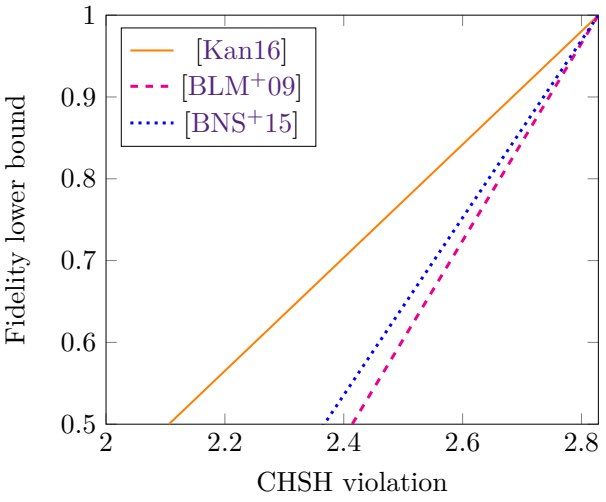


Figure 7: Lower bounds on the self-tested fidelity with the maximally entangled pair of qubits as a function of the observed violation of the CHSH inequality for three methods. A trivial lower bound on the fidelity is 0.5, achievable with the separable state $|00\rangle$. Finding the optimal curve remains as an open question. The impossibility to obtain a fidelity higher than 0.5 for every CHSH violation > 2 is proven in [CKS19]. The proof is constructive: there exists a state ρ providing the CHSH violation of ≈ 2.0014, nevertheless there is no local channel Λ such that fidelity between $\Lambda(\rho)$ and Φ^+ is higher than 0.5.

invariant, called the solution group, to each linear constraint system (LCS) nonlocal game. The rules of the nonlocal game allow one to define an abstract group whose representations correspond to the winning quantum strategy of the game. The correspondence between the group representations and winning strategies then allows for the use of techniques from group theory to prove self-testing statements.

In [CS17b] this reasoning is taken one step further: a quantum strategy winning the generalised magic square game with high probability allows to extract an approximate representation of the solution group, or equivalently, a mapping between the group elements and unitary operators which is approximately a homomorphism. The closeness between the approximate and the exact representation is then used to make a robust self-testing statement.

The most important ingredient for constructing robust self-tests in this way is the stability theorem for approximate representations from [GH17]. It states that for any approximate n-dimensional representation f of a finite group $G = \{g_i\}_i$ there exists an exact unitary m-dimensional representation h such that the Hilbert-Schmidt distance between $f(g_i)$ and $h(g_i)$ is small and m is close to n. The distance between these two representations is related to the score the physical strategy gained in the LCS game under consideration. The full robustness statement is obtained through the use of the van Kampen diagrams [Kam33].

7.2 Robust certification of large entanglement

In this section we discuss few contributions dealing with robustly certifying large amounts of entanglement without explicitly stating any self-testing result. There are two main reasons why such results merit attention in a review like this. The first is that for many purposes they could be used instead of robust self-testing protocols and moreover the self-testing statement is implicitly present for noiseless correlations. The second reason is the possible influence they could have on future approaches to robust self-testing.

A difference between robustness and noise tolerance when it comes to self-testing a tensor product of n entangled pairs $|\psi'\rangle^{\otimes n}$ is emphasised in works [AFB19] and [AFY18]. The known self-testing protocols are robust in the sense that any strategy producing correlations that are ϵ-close to the ideal ones must use a state which is $f(\epsilon, n)$-close to $|\psi'\rangle^{\otimes n}$, where $f(\epsilon, n)$ scales as $an^b\epsilon^c$ for appropriate constants a,b and c. This is, however, not the same as noise-tolerance since noisy source producing the state $\rho^{\otimes n}$, where ρ is ϵ-close to $|\psi'\rangle$ is not $f(\epsilon, n)$-close to $|\psi'\rangle^{\otimes n}$. The fidelity of such state with $|\psi'\rangle^{\otimes n}$ drops exponentially with n, so there is very little hope to make any non-trivial self-testing statement about such highly entangled state. Instead of self-testing $|\phi^+\rangle^{\otimes n}$ [AFY18] designs a one-shot test which is able to certify states whose entanglement of formation [BDSW96] is $\Omega(n)$. This certification method is noise-tolerant in the sense that the states $\rho^{\otimes n}$ are able to pass the test with high probability. A method to bound the one-shot distillable entanglement [BD10] of the states produced by an uncharacterised source is presented in [AFB19]. The protocol is operationally useful since not all entanglement is consumed for certification. Both these results are implicit self-tests since the maximal score in the introduced games implies that the state produced by a source must be $|\phi^+\rangle^{\otimes n}$.

8 Self-testing of measurements

In many cases the correlations which self-test a quantum state also self-test the applied measurements. As a result, many of the state self-testing results presented in the previous sections are accompanied by a corresponding statement for the measurements. In this section we give an overview of such results. In section 8.1 we review the known self-testing results for various sets of measurements, and in section 8.2 we discuss the different methods that have been used to achieve these results. We end the section with an overview of robustness techniques in measurement self-testing in section 8.3.

8.1 Measurement self-testing results

8.1.1 Qubit measurements

The simplest set of incompatible qubit measurements is given by a pair of Pauli observables σ_x and σ_z. Self-testing of these measurements (together with their rotated versions $(\sigma_x \pm \sigma_z)/\sqrt{2}$ for the other party) can be achieved through the maximum violation of the CHSH Bell inequality (see Section 4) or related self-tests. Such self-testing statements can be found in [MYS12, Kan17, BNS+15, WCY+14]. Self-testing of the set of local observables $\{\sigma_x, \sigma_z, (\sigma_x \pm \sigma_z)/\sqrt{2}\}$ can be achieved through the so called 'Mayers-Yao' self test and its generalisations [MY04, McK14, MYS12]. A method to self-test large sets of qubit observables that are equally spaced on the equator of the Bloch sphere was given in [ŠASA16] based on the maximum violation of the chained Bell inequalities [Pea70, BC90]. A protocol for self-testing an arbitrary measurement from the real plane of the Bloch sphere is given in [McK16a]. Self-testing of pairs of observables of the form $\cos\mu\,\sigma_x \pm \sin\mu\,\sigma_z$ is given in [BP15] and [Kan17] through the maximal violation of the tilted or weighted CHSH inequalities [AMP12, LLP10]. The first self-testing of the set of three local Pauli observables $\{\sigma_x, \sigma_y, \sigma_z\}$ first appeared in [MM11], using the 'phase kick-back' (see section 8.2.1) method and a generalised definition of self-testing to deal with the issue of complex conjugation. Other examples of such self-tests can be found in [ABB+17, Kan17, WKB+19].

8.1.2 Qudit measurements

Self-testing results for measurements of dimension larger than two are much less common. The only self-test of mutually unbiased bases in a prime dimension higher that 2 was given in [KŠT+19] for dimension $d = 3$. Self-testing of the Bell state measurement was first achieved analytically in [RKB18, BSS18] (see section 8.2.4 for an outline of the method). Self-tests of sets of measurements in high dimension can be achieved using the same techniques as in parallel self-testing of states (section 5.3). In this way, n-fold tensor products of the measurements $\{\sigma_x, \sigma_z\}$ and $\{\sigma_x, \sigma_y, \sigma_z\}$ in dimension 2^n have been achieved [BŠCA18b, CGJV17, WBMS16, McK17, Col17, NV17, CN16, BKM19, KM18, CS17b, NV18].

8.1.3 Non-projective measurements

Although definition 2 of measurement self-testing assumes that the physical measurements are projective, one can nevertheless aim to prove that on the support of the reduced state of the self-tested state they act as some desired POVM. More specifically, suppose we have self-tested the reference state $|\psi'\rangle$. Since the trace is invariant under isometry maps, the correlations can be written

$$p(a,b|x,y) = \mathrm{tr}\left[|\psi'\rangle\langle\psi'|_{\mathrm{A'B'}} \otimes \sigma_{\bar{\mathrm{A}}\bar{\mathrm{B}}}\, \mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y}\right],$$

where the local measurements are projective and may act on both the primed and bared spaces. Taking the trace over the barred spaces we have

$$p(a,b|x,y) = \mathrm{tr}\left[|\psi'\rangle\langle\psi'|\, \tilde{\mathsf{M}}_{a,b|x,y}\right], \tag{57}$$

where

$$\tilde{\mathsf{M}}_{a,b|x,y} = \mathrm{tr}_{\bar{\mathrm{A}}\bar{\mathrm{B}}}\left[\mathbb{1}_{\mathrm{A'B'}} \otimes \sigma_{\bar{\mathrm{A}}\bar{\mathrm{B}}}\, \mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y}\right]. \tag{58}$$

To 'self-test' non-projective measurements, one aims to show that $\tilde{\mathsf{M}}_{a,b|x,y} = \mathsf{M}'_{a|x} \otimes \mathsf{N}'_{b|y}$, where now the reference measurements can be non-projective. Essentially, one is self-testing a Stinespring dilation [Sti55] of the non-projective measurement.

In this manner, a self-test of the 'tetrahedral' qubit POVM first appeared in [APVW16], with rigorous proofs appearing later in [ABB+17] and [ABDC18], and an experimental demonstration presented in [SMN+20]. These results were proven using the method of 'post-hoc' self-testing, that we describe in 8.2.3. To self-test

measurements which are neither projective nor rank-one POVMs [WBSS18] use the approach developed by the same authors for the self-testing of quantum channels, described here in section 9.1.

8.2 Methods in measurement self-testing

In this section we outline some of the methods that have been used to prove measurements self-testing statements.

8.2.1 Phase kickback method for self-testing complex measurements

As mentioned in section 3.7, definition 2 is not suitable for self-testing complex-valued measurement operators. Take for example the problem of self-testing $|\phi^+\rangle$, the maximally entangled state of dimension 2, and $\{\sigma_z, \sigma_x, \sigma_y\}$, the three Pauli observables for say Alice. In section 4, we have seen how one can self-test the state $|\phi^+\rangle$ and $\{\sigma_x, \sigma_z\}$. Here, the issue of complex conjugation is not a problem since there exists a local basis in which the measurements and state are both real. However, there is no local basis in which the observables $\{\sigma_z, \sigma_x, \sigma_y\}$ are all real. Thus, we have two distinct possibilities for Alice's measurements, $\{\sigma_z, \sigma_x, \sigma_y\}$ and $\{\sigma_z^*, \sigma_x^*, \sigma_y^*\}$=$\{\sigma_z, \sigma_x, -\sigma_y\}$, both of which are compatible with the observed correlations.

A natural question to ask is, given this uncertainty, what is the strongest possible self-testing statement that one could hope to prove? This question was first tackled by [MM11], see also [CGS17, BŠCA18b]. The basic idea is as follows. Consider a self-testing scenario in which Alice has (at least) three measurements given by the observables A_0, A_1, A_2. Take a known self-testing protocol for the state $|\phi^+\rangle$ and observables $\{\sigma_x, \sigma_z\}$ for Alice. Use this self-testing protocol three times for the pairs $\{\mathsf{A}_0, \mathsf{A}_1\}$, $\{\mathsf{A}_0, \mathsf{A}_2\}$, $\{\mathsf{A}_1, \mathsf{A}_2\}$, introducing new measurements for Bob and Alice if necessary. Since this proves that each pair $\mathsf{A}_i, \mathsf{A}_j$ anti-commute, one proves that the observables $\{\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2\}$ pairwise anti-commute and should essentially be $\{\sigma_z, \sigma_x, \sigma_y\}$ or $\{\sigma_z, \sigma_x, -\sigma_y\}$. More precisely, one introduces a pair or local ancillas $|00\rangle_{\mathrm{A''A'}}$ for Alice and another pair $|00\rangle_{\mathrm{B''B'}}$ for Bob and proves the existence of an isometry Φ such that

$$\begin{aligned}
\Phi[|\psi\rangle] &= |\phi^+\rangle_{\mathrm{A'B'}} \otimes |\xi\rangle \\
\Phi[\mathsf{A}_0 |\psi\rangle] &= (\sigma_z \otimes \mathbb{1} |\phi^+\rangle_{\mathrm{A'B'}}) \otimes |\xi\rangle \\
\Phi[\mathsf{A}_1 |\psi\rangle] &= (\sigma_x \otimes \mathbb{1} |\phi^+\rangle_{\mathrm{A'B'}}) \otimes |\xi\rangle \\
\Phi[\mathsf{A}_2 |\psi\rangle] &= (\sigma_y \otimes \mathbb{1} |\phi^+\rangle_{\mathrm{A'B'}}) \otimes \sigma_z^{\mathrm{A'}} |\xi\rangle
\end{aligned} \tag{59}$$

where the state $|\xi\rangle$ has the form

$$|\xi\rangle = |\xi_0\rangle_{\mathrm{AB}} \otimes |00\rangle_{\mathrm{A''B''}} + |\xi_1\rangle_{\mathrm{AB}} \otimes |11\rangle_{\mathrm{A''B''}}\,. \tag{60}$$

In (59) the additional σ_z measurement on the junk state acts as an effective 'controlled conjugation' for the measurement of σ_y on $|\phi^+\rangle$, where the probability to perform the conjugation is given by $\langle\xi_1|\xi_1\rangle$, which remains unknown. Note that if we consider only the space $\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{B}$ then the action of A_2 is to perform some unknown convex combination of σ_y and $-\sigma_y$, as expected. Similar statements can be proven for Bob, where the register $\mathrm{B'}$ acts as a control for a possible conjugation of his measurements. Note that given the form of (60), Alice and Bob will conjugate their measurement operators in a correlated fashion, as required from (14). The isometry, introduced in [MM11] and later used in [JMS20] to prove the above self-testing statement is an extension to the Swap isometry (see figure 4) introduced in section 4. The full isometry consists of the regular Swap isometry, followed by two extra 'phase kickback' controlled unitaries; see figure 8.

8.2.2 Self-testing measurements based on commutation

The majority of self-testing protocols first prove self-testing of the state, and then move to self-test the form of measurements on the support of the self-tested state. An alternative approach for binary observables was used already in [PR92] and revived in [Kan17]. In this approach the violation of a Bell inequality is directly related to the commutation properties of measurement observables without the need to prove a statement of the form of definition 2. In the two input, two output scenario the figure of merit (for Alice's observables) is directly relatable to the maximal violation of the CHSH inequality and is given by

$$t_{01} = \frac{1}{2}\mathrm{tr}(|[\mathsf{A}_0, \mathsf{A}_1]|\rho_\mathrm{A}), \tag{61}$$

where $\rho_\mathrm{A} = \mathrm{tr}_\mathrm{B}\rho_\mathrm{AB}$ is Alice's reduced state of the physical state. The maximal CHSH violation implies $t_{01} = 1$, which further can be used to infer

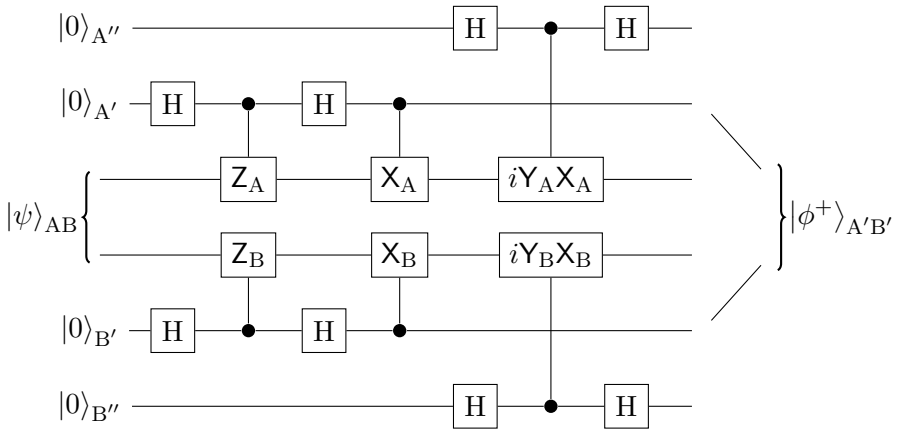


Figure 8: Swap gate with a phase kick back at the end of the circuit . The Y operators are constructed from the additional measurement operators in a similar fashion to (32)

anticommutativity of A_0 and A_1 on ρ_A. Beyond CHSH, it is also proven that the maximal violation of the Mermin-Ardehali-Belinskii-Klyshko inequalities [Mer90a, Ard92, BK93] implies the parties use anticommuting observables to achieve the maximal violation.

The method is also applied to self-test a set of three mutually anti-commuting observables. Note that there exists a basis in which any two anticommuting observables A_0 and A_1 can be written

$$\mathsf{A}_0 = \sigma_z \otimes \mathbb{1}, \qquad \mathsf{A}_1 = \sigma_x \otimes \mathbb{1}. \tag{62}$$

If an inequality involving three observables $\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2$ can be used to certify $t_{01} = t_{02} = t_{12} = 1$ then besides relation (62) the following relation can be extracted

$$\mathsf{A}_2 = \sigma_y \otimes \mathrm{A}_Y, \tag{63}$$

where A_Y is a Hermitian ± 1-eigenvalue operator. Hence, when measuring A_2 the measurement result for A_Y on the 'junk' Hilbert spaces takes care of the complex conjugation issue in the same way as (59).

Once the form (62) is extracted for measurement observables of all parties it is possible to also make statements about the underlying state. Furthermore, in [Kan17] this method is useful to certify observables which are not anticommuting but maximally violate weighted CHSH inequalities introduced in [LLP10]. Going beyond binary measurements, the extension of this method is applied also in [KŠT+19] to self-test mutually unbiased bases in the dimension $d = 3$.

8.2.3 Post-hoc self-testing of measurements

Once a state and sufficiently many measurements have been self-tested, further measurements can often be self-tested 'for free' through a method that we call post-hoc self-testing. As an example, the maximal violation of the CHSH inequality assures that up to an isometry the shared state is $|\phi^+\rangle$, Alice's measurement observables are σ_z and σ_x, and Bob's measurement observables $(\sigma_z \pm \sigma_x)/\sqrt{2}$. The self-testing protocol can be extended to certify any other real qubit observable applied by either Alice or Bob. Assume Bob uses another measurement observable B_2 which we want to self-test as $\cos\theta\sigma_x + \sin\theta\sigma_z$ on his half of the maximally entangled state. If Bob performs this measurement, we will observe the correlations $\langle\psi|\mathsf{A}_0\mathsf{B}_2|\psi\rangle = \cos\theta$ and $\langle\psi|\mathsf{A}_1\mathsf{B}_2|\psi\rangle = \sin\theta$. Now, the maximal violation of the CHSH inequality implies that $\mathsf{A}_0|\psi\rangle$ and $\mathsf{A}_1|\psi\rangle$ are orthogonal. If we take these two states to be the first two states in an orthonormal basis of the full space, it must be that $\mathsf{B}_2|\psi\rangle = \cos\theta\mathsf{A}_0|\psi\rangle + \sin\theta\mathsf{A}_1|\psi\rangle$. Applying the isometry to this, we have

$$\begin{aligned}\Phi[\mathsf{B}_2|\psi\rangle] =& \Phi\left[\cos\theta\mathsf{A}_0|\psi\rangle + \sin\theta\mathsf{A}_1|\psi\rangle\right] \\ =& (\cos\theta\sigma_z \otimes \mathbb{1} + \sin\theta\sigma_x \otimes \mathbb{1}|\phi^+\rangle) \otimes |\xi\rangle \\ =& (\mathbb{1} \otimes \cos\theta\sigma_z + \mathbb{1} \otimes \sin\theta\sigma_x|\phi^+\rangle) \otimes |\xi\rangle\,,\end{aligned}$$

as required, where we have used the property $\mathsf{M} \otimes \mathbb{1}|\phi^+\rangle = \mathbb{1} \otimes \mathsf{M}^T|\phi^+\rangle$.

This technique can be understood from the perspective of measurement tomography. Given a set of linearly independent pure states that are tomographically complete on some subspace, one can infer the form of any measurement in this

subspace from the statistics of measurement outcomes on the set of states. Given the CHSH self-test, we know that conditioned on Alice's input and output, the reduced states of Bob up to a unitary transformation are $\pi^{\mathrm{B}}_{a|x} \otimes \mathbb{1}_{\mathrm{B}}$, where $\pi_{a|x} = |0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|, |-\rangle\langle -|$ depending on the value of x, a. These four states are informationally complete for real qubit measurements, and can thus be used to infer further such measurements for Bob when interpreted as states in a measurement tomography protocol. The technique can be applied in a similar way for higher-dimensional self-testing protocols and to the post-hoc self-testing of complex measurements. The first time such an approach was used was for self-testing real measurements applied on a graph state in [McK16a], expanding the protocol for self-testing graph states from [McK14]. This technique has also been particularly useful to self-test non-projective measurements (see 8.1.3).

8.2.4 Self-testing of entangling measurements

An entangling measurement is one whose measurement operators are non-separable with respect to some bipartition of the Hilbert space. Two recent works [RKB18, BSS18] have presented analytic methods to robustly self-test the Bell state measurement (BSM), the entangling measurement whose eigenvectors are the four maximally entangled Bell states $\{|\phi^+\rangle\langle\phi^+|, |\phi^-\rangle\langle\phi^-|, |\psi^+\rangle\langle\psi^+|, |\psi^-\rangle\langle\psi^-|\}$. Here the reference scenario is an entanglement swapping protocol: Bob possesses two particles, one maximally entangled with Alice's particle and the other with Carmela's. Bob performs the BSM on his two particles, and depending on his outcome projects the particles of Alice and Carmela onto one of the Bell states. These four Bell states can be self-tested by maximally violating the four different CHSH inequalities (mutually related by relabelling) conditioned on the outcome of Bob. The idea for self-testing is simple: if Alice and Carmela maximally violate all CHSH inequalities then it must be that Bob's measurement is the BSM. Importantly, to maximally violate each of the four different Bell inequalities, Alice and Carmela use the same measurements.

In [RKB18, BSS18], the entanglement swapping scenario is used to self-test the BSM using the notion of measurement self-testing via simulation described in section 3.7.2. Here, one necessarily needs to identify some well defined local Hilbert spaces for Bob in order to define entanglement. This is achieved by assuming that there are two independent sources between Alice and Bob, and between Bob and Carmela. Entanglement is then defined with respect to the Hilbert spaces of these two sources. A self-testing protocol for entangling measurements whose eigenvectors are partially entangled pairs of qubits, or GHZ states is also presented in [RKB18]. In [BSS18] the techniques for self-testing quantum channels is used to self-test the BSM. For more details on these techniques see section 9.1.

It is also worth mentioning here that in [RHC+11], a protocol to device-independently certify the existence of an entangling measurement is given, which was later shown to be robust in [BNS+15] via the use of the numerical Swap method (section 7.1.4). Both these works however only prove the existence of some entangling measurement but do not provide a self-testing statement for a particular measurement. In the context of witnessing irreducible dimension a way to certify entangling measurements is also presented in [CCBS17] alongside with a figure of merit quantifying how entangled the measurement operators are.

8.3 Robust measurement self-testing

In this section we give an overview of the approaches to robust self-testing of measurements. As we saw in section 3.6 there are a number of valid figures of merit one could consider when robustly self-testing a state. Given the increased complexity of measurements compared to states, the self-testing of measurements is even more diversified. In what follows we discuss a few approaches to quantify how close a physical measurement $\{\mathsf{M}_x\}$ is to some reference measurement $\{\mathsf{M}'_x\}$.

The straightforward approach, in accordance with definition 4 uses the same methods as in the self-testing of states. In robust self-testing of states one defines a figure of merit that captures the closeness between the states $\Phi[\rho_{\mathrm{AB}}]$ and $|\psi'\rangle\langle\psi'|_{\mathrm{A'B'}} \otimes \sigma_{\bar{\mathrm{A}}\bar{\mathrm{B}}}$. For measurement self-testing, one can simply use the same figure of merit between the subnormalised states $\Phi\left[\mathsf{M}_{a|x} \otimes \mathbb{1}\, \rho_{\mathrm{AB}}\, \mathsf{M}^{\dagger}_{a|x} \otimes \mathbb{1}\right]$ and $\left(\mathsf{M}'_{a|x} \otimes \mathbb{1}\, |\psi'\rangle\langle\psi'|_{\mathrm{A'B'}}\, \mathsf{M}'^{\dagger}_{a|x} \otimes \mathbb{1}\right) \otimes \sigma_{\bar{\mathrm{A}}\bar{\mathrm{B}}}$. This will

mean that there will be a different value associated to each of the measurement operators; a single figure of merit can be obtained by, for example, taking the average or maximum of these values. Such an approach is used, for example, in [MYS12, McK14, BP15, ŠASA16].

The Swap method [YVB+14, BNS+15] can also be used to define a figure of merit for robust measurement self-testing. Taking the CHSH example, to estimate the closeness of Alice's measurements to the reference measurements, the Swap gate is applied only on her system (i.e. only Alice's local branch of the Swap gate is used) and the ancilla is initiated in one of the eigenstates $\left|\varphi_{\pm}^{\mathsf{A}'_i}\right\rangle$ of her reference observable A'_i. In the ideal case, if Alice measures the reference observable A'_i after the Swap gate is applied she will deterministically obtain the outcome ± 1. The probability that this measurement gives the result $+1$ is then used as a figure of merit to asses the closeness of the measurement, however it is not proven to give a distance measure. As with the estimation of the fidelity with the reference state, one can use the NPA hierarchy to lower bound this quantity with respect to the given CHSH violation.

A different figure of merit, analogous to the notion of state extractability (see section 3.6), was suggested in different self-testing contexts [TKV+18, RKB18, BSS18, TSV+20, WBSS18]. If D is a suitably chosen distance measure on the set of measurements, one can define the distance $\mathcal{D}$ between the physical measurement $\mathsf{M}_{a|x}$ and the reference one $\mathsf{M}'_{a|x}$ as

$$\mathcal{D}(\mathsf{M}_{a|x}, \mathsf{M}'_{a|x}) = \frac{1}{c_a} \max_{\Lambda} \sum_a D(\Lambda(\mathsf{M}_{a|x}), \mathsf{M}'_{a|x}), \tag{64}$$

where c_a is a normalisation factor and the maximisation is taken over all completely positive and unital maps $\Lambda : \mathcal{L}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{L}(\mathcal{H}_{\mathrm{A}'})$. Depending on the type of reference measurements D can be chosen to be the overlap (as in [RKB18, TKV+18, TSV+20]), Uhlmann fidelity (as in [BSS18, WBSS18]) or any other distance measure. While the physical state ρ does not explicitly appear in (64), the map Λ has to depend in some way on it. In [WBSS18, BSS18] measurements are self-tested through their action on the maximally entangled pair of qudits and the state appears explicitly in the distance measure.

9 Extensions of self-testing to other scenarios

In this section we cover three extensions to the standard scenario of self-testing. In section 9.1 we cover works that self-test the action of a quantum gate in a device-independent manner. In section 9.2 we focus on the so-called semi-device independent approaches. In section 9.2.3 we focus on self-testing via contextuality.

9.1 Self-testing of quantum gates and circuits

The paradigm of self-testing can be useful in scenarios going beyond the certification of states and measurements. Anticipating usefulness in the certification of devices for quantum computing, one may ask if it is possible to certify quantum gates, *i.e.* unitary transformations. First answers to this question came already in the early days of self-testing with two contributions devoted to the task of self-testing of quantum gates or quantum circuits, [vDMMS07] and [MMMO06]. Although [vDMMS07] has the phrase 'self-testing' in its title, it does not correspond to the fully device-independent scenario; the certification relies on several assumptions such as knowledge of the dimension of the system, which shifts it to the landscape of semi-device-independent scenarios.

The first protocol providing a recipe to self-test quantum gates acting on an arbitrary number of qubits is presented in [MMMO06]. Denote the physical implementation of the gates Alice and Bob use with G_{A} and G_{B}. For the protocol to work, Alice and Bob must have access to the *same* gate, that is, $G_{\mathrm{A}} = G_{\mathrm{B}}$. The core of the protocol is the Mayers-Yao self-test of the maximally entangled pair of qubits. To self-test a one-qubit unitary gate $G'_{\mathrm{A}'}$ acting on her system, Alice has to share a maximally entangled pair of qubits with Bob. As usual, the state shared between Alice and Bob is $|\psi\rangle$ and they perform measurements $\{\mathsf{M}_{a|x}\}$ and $\{\mathsf{N}_{b|y}\}$. The aim is to show that there is a local isometry Φ such that

$$\Phi \otimes \mathbb{1}_{\mathrm{P}} \left[G_{\mathrm{A}} \, \mathsf{M}_{a|x} \otimes \mathbb{1} \, |\psi\rangle_{\mathrm{ABP}} \right] = \\ = G'_{\mathrm{A}'} \mathsf{M}'_{a|x} \otimes \mathbb{1} \, |\phi^+\rangle_{\mathrm{A}'\mathrm{B}'} \otimes |\xi\rangle_{\bar{\mathrm{A}}\bar{\mathrm{B}}\mathrm{P}}$$

where $\{\mathsf{M}'_{a|x}\}$ are the reference measurements for the Mayers-Yao self-test. The protocol consists of three parts:

- The Mayers-Yao self-test on the input state $|\psi\rangle$,
- The Mayers-Yao self-test on the output state $G_A \otimes G_B |\psi\rangle$,
- A check that $G_A \otimes \mathbb{1}_B |\psi\rangle_{AB}$ reproduces the statistics of ${G'}_{A'} \otimes \mathbb{1}_{B'} |\phi^+\rangle_{A'B'}$ with respect to the Mayers-Yao measurements.

The first two steps serve for self-testing the underlying state and ensure that G is a unitary gate (at this step potentially the identity gate). The third step can be seen as a tomography of G, since the measurements and state are already self-tested in the first two steps. Note that this means one can only self-test gates having real coefficients with respect to the self-tested measurements. The method is also extended to many-qubit gates. Each of Alice's qubit on which a gate acts is maximally entangled with another qubit of Bob, and the tensor product structure of Alice's and Bob's Hilbert spaces is assumed. The procedure repeats as in the case of one-qubit gates, with three steps involving the self-test of the input and output states which are now tensor products of many maximally entangled pairs of qubits and tomography of the corresponding multi-qubit gate. By using this method one can self-test the whole quantum circuit by self-testing each gate in sequence according to the recipe given above. This self-test is also proven to be robust.

Another self-test of quantum gates with simpler structure and significantly better robustness bounds is given in [SBWS18]. It is more general than [MMMO06] since it provides a framework to lower bound the fidelity with an arbitrary quantum channel Γ'. For Alice to self-test the channel Γ' she again has to share a maximally entangled pair of qubits with Bob, but now Bob does not perform any channel to his system. Let the physical implementation of the channel be denoted as Γ. The aim is to find the fidelity between the reference channel Γ' and the physical one Γ. The protocol consists of two steps:

- The self-test of the input state $|\psi\rangle$. The result provides a lower bound to the input fidelity F_i between $\Lambda_A^i \otimes \Lambda_B |\psi\rangle$ and $|\phi^+\rangle$, where Λ_A^i and Λ_B are the CPTP maps as explained in 3.7.2.
- The appropriate self-test which finds a lower bound of the output fidelity F^o between the state $\Lambda_A^o \otimes \Lambda_B (\Gamma_A \otimes \mathbb{1}_B |\psi\rangle_{AB})$ and the reference output state ${\Gamma'}_{A'} \otimes \mathbb{1}_{B'} |\phi^+\rangle_{A'B'}$.

The fidelity of the physical channel to the reference channel is proven to be lower bounded by $\cos(\arccos(F_i) + \arccos(F_o))$. The main challenge is to find the appropriate self-test necessary for the second step. The paper gives the solution for unitary channels (*i.e.* quantum gates), generalises the protocol for many-qubit channels and provides the explicit solution for arbitrary two-qubit controlled gate of the form $CU_\varphi = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes e^{-i\varphi\sigma_x}$. Since such gates are necessary and sufficient for universal quantum computing (together with a set of single qubit gates) the toolkit represents an important contribution to the self-testing of all the building-blocks of a quantum computer.

Aside from this, the paper [SBWS18] is also valuable for two contributions independent of quantum channel self-testing. One is a method to self-test multipartite states, described in 6.2 and the other a technique useful for robust self-testing, described in 7.1.3. Furthermore, by defining the gates in terms of their Krauss representation, the techniques from [SBWS18] have been generalised in [WBSS18] to allow for self-testing of measurements other than rank-one POVMs.

9.2 Semi-device-independent scenarios

A number of works have investigated extensions of self-testing to so-called semi-device-independent (SDI) scenarios. In the device-independent scenario, all devices are treated as black boxes and one hence imposes minimal assumptions on the states and measurements. In the SDI scenario, some additional assumptions are added, without assuming a full characterisation of the entire set-up. As such, the SDI scenario can be seen as a weaker version of the DI scenario, intermediate between the scenarios of full device independence and full characterisation. Moving to the SDI scenario can be advantageous for at least three reasons. First, the additional assumptions can overcome some of the mathematical difficulties of the DI scenario and make statements easier to prove and results more tolerant to noise; second, for some scenarios it may actually be necessary to move to SDI scenario in order to make any non-trivial statements (see 9.2.2), and third, the additional assumptions

may be very natural given a particular experimental set-up or level of trust in some devices. In this section we give an overview of three extensions of self-testing to the SDI scenario, namely one-sided device-independent self-testing, commonly known as the EPR steering scenario (section 9.2.1), self-testing in prepare-and-measure scenarios (section 9.2.2), and self-testing based on noncontextuality inequalities (section 9.2.3).

9.2.1 One sided device-independent self-testing (EPR steering)

The one-sided device-independent scenario (also commonly referred to as the EPR steering scenario), is equivalent to the standard self-testing scenario, with the additional assumption that there is one trusted party (here Bob) whose device is fully characterised, that is, his measurement operators are known. Thus, Bob is able to apply any quantum measurement and can in principle perform quantum state tomography of his half of the state. Alice, as in the self-testing scenario, receives classical input x to her device and outputs classical output a. The subnormalised state of Bob conditioned on Alice's input x and output a is given by

$$\sigma_{a|x} = \mathrm{tr}_{\mathrm{A}}\left[\mathsf{M}_{a|x} \otimes \mathbb{1}\rho_{\mathrm{AB}}\right] \tag{65}$$

The set $\{\sigma_{a|x}\}_{a,x}$ is called an assemblage. It is said that the assemblage $\{\sigma_{a|x}\}_{a,x}$ admits a local hidden state model (LHS) if it admits a decomposition

$$\sigma_{a|x} = \int_{\lambda} d\lambda\, q(\lambda) p_{a|x,\lambda}\rho_{\lambda}, \qquad \forall a, x, \tag{66}$$

where $q(\lambda)$ is a normalised probability density and ρ_{λ} is a normalised density operator acting on the local Hilbert space of Bob. If the assemblage $\{\sigma_{a|x}\}_{a,x}$ is incompatible with a LHS model one says that it demonstrates steering. The existence of a LHS model can be refuted by violation of steering inequalities, which take into account the correlations between Alice's outputs and the outputs of known measurements performed by Bob. Another way to prove that the assemblage $\{\sigma_{a|x}\}_{a,x}$ demonstrates steering is by using simple SDP optimisations [WJD07],[CS17a],[UCNG19].

The decomposition (66) captures the types of assemblages that Bob can see if the two parties do not share any entanglement. Thus, a violation of

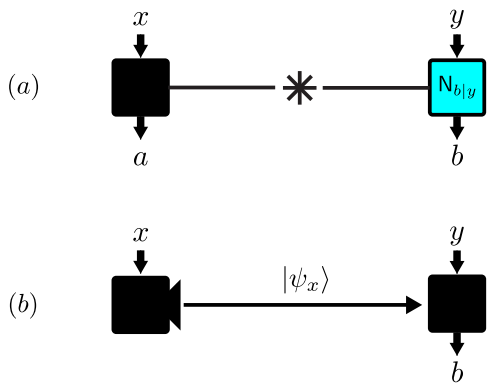


Figure 9: Semi-device-independent scenarios. (a) The one-sided device-independent scenario. One of the parties (here Bob) is assumed to have a trusted measurement device (i.e. his measurement operators are known). (b) The prepare-and-measure scenario. Alice sends a quantum state to Bob, conditioned on her input.

(66) demonstrates that the shared state must be entangled. A natural question is in which cases can we go beyond witnessing entanglement and recover the shared state ρ_{AB}. This task was introduced in [ŠH16] and [GWK17] under the name one-sided device-independent (1SDI) self-testing. In [ŠH16] the authors are mostly interested in the robustness of 1SDI self-testing and how it compares to the robustness of standard self-testing, while the authors of [GKW15] are also interested in the application to delegated quantum computing protocols (see Section 10.4). Two types of 1SDI self-testing are introduced: correlation based, which draws conclusions only from the violations of steering inequalities, and assemblage-based, which works with the full assemblage. An interesting conclusion is that in the case of the simplest self-test of the maximally entangled pair of qubits, the asymptotic behaviour of the self-tested fidelity as a function of noise is the same in both the 1SDI and DI scenarios. How general this statement is remains as an open question. The 1SDI scenario is also very useful for self-testing a tensor product of many EPR pairs. In the standard self-testing of such states the main difficulty is establishing a tensor product structure, while in 1SDI scenario this comes for free due to the fact that Bob's device is characterised. Numerical techniques, similar to the Swap method, for robust self-testing in the 1SDI scenario were also presented in work [ŠH16]. 1SDI self-testing of all pure two-qubit states is presented in [GBD+18].

9.2.2 Self-testing in the prepare-and-measure scenario

A recent series of works have adapted the self-testing scenario to the prepare-and-measure scenario. Here, Alice sends one of a number of states $|\psi_x\rangle$, labelled by x, to Bob, who measures $\{\mathsf{M}_{b|y}\}$ conditioned on input y and obtains outcome b. The statistics of the experiment are therefore given by

$$p(b|x,y) = \mathrm{tr}[|\psi_x\rangle\langle\psi_x|\mathsf{M}_{b|y}]. \tag{67}$$

In analogy to the case of self-testing entangled states and measurements, one aims to infer from the statistics that the preparations and measurements $\{|\psi_x\rangle, \mathsf{M}_{b|y}\}$ are equal to some reference set $\{|\psi'_x\rangle, \mathsf{M}'_{b|y}\}$ up to some unknown isometry.

In contrast to the Bell scenario, non-trivial statements can only be made if one places additional assumptions on the experiment. To see this, note that any statistics $p(b|x,y)$ can be reproduced by sending the label x to Bob, i.e. with the preparations $|\psi_x\rangle = |x\rangle$, and Bob simply outputting b with probability $p(b|x,y)$. Thus, self-testing any set of preparations that are not diagonal in the same basis is impossible without some additional assumptions. As is common in the prepare-and-measure scenario, a number of recent works [TKV+18, TSV+20, MP19, FK19] overcome this by assuming an upper bound on the Hilbert space dimension of the preparations and measurements. A similar assumption has also been studied in the Bell scenario [BLM+09, GBS16] where the state and measurements are assumed to be qubit systems, making self-testing statements significantly easier to prove.

A convenient figure of merit in prepare-and-measure scenario is the success in a game called a random access code (RAC) [ANTSV99, Nay99, THMB15]. In a $n^d \to 1$ RAC, Alice receives n dits $x = (x_1, x_2, \cdots, x_n)$ and Bob receives $y = 1, 2, \cdots, n$. The aim is to maximise the average probability that Bob correctly guesses the input bit x_y, i.e. to maximise the expression

$$\mathcal{A}_{n^d\to 1} = \frac{1}{2d^n}\sum_{x,y} p(b = x_y|x,y). \tag{68}$$

In [TKV+18], the authors study as a figure of merit the $2^2 \to 1$ RAC. It is proven that the value $\mathcal{A}_{2^2\to 1}$ can be used to perform robust self-testing of the preparations $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and measurements given by the qubit observables $(\sigma_x \pm \sigma_z)/\sqrt{2}$ under the assumption of qubit preparations and measurements, using a technique based on that in [Kan16] (similar statements also appeared in [WLP13, BQB14] in the context of SDI quantum key distribution protocols and dimension witnesses). This is then generalised to a self-test of any pair of non-commuting qubit observables by adding an input-dependent bias to (68). The authors also use $\mathcal{A}_{2^2\to 1}$ to self-test a non-trivial set of qutrit preparations and measurements, and implement an adaptation of the numerical Swap method (see Section 7.1.4) to deal with the prepare-and-measure scenario. In [FK19], the authors study the $2^d \to 1$ RAC. It is proven that this game provides a robust self-test of a pair of measurements that correspond to two mutually unbiased bases in dimension d. Further to this, the authors show how the score of the RAC can also be used to bound both the incompatibility robustness [HKR15] of the pair and the randomness of the measurement outputs. It is worth emphasising that self-testing claims in this scenario can be made for arbitrary dimension-bounded communication games, *i.e.* it is not restricted to RACs.

Several works have investigated self-testing of non-projective measurements in the dimension-bounded prepare-and-measure scenario. In [MP19] the authors start from the $3^2 \to 1$ RAC to develop a self-test of the extremal 'tetrahedral' qubit POVM. In [TSV+20], a general method is given to self-test any extremal qubit POVM, given a self-test of a set of preparations with opposite Bloch vectors to the POVM on the Bloch sphere. In a similar fashion in [TRR19] the authors provide a self-test of d-dimensional SIC POVM (whenever it exists). To prove the ideal self-testing all works use the same idea; if there is one outcome of a measurement that never occurs for a given preparation, it follows that the corresponding POVM element must be opposite to the preparation on the Bloch sphere. From this one can use a self-test of preparations to effectively tomograph the POVM measurement in a similar manner to that in Section 8.2.3. In [TSV+20] the protocol is made robust by introducing a convenient distance measure which is used in the experimental demonstration reported therein. All three works also discuss certification of the non-projective nature of a measurement, which is a weaker form of certification than ro-

bust self-testing since it does not discuss closeness to any particular POVM.

The recent work [MBP19] investigates the self-testing of non-projective measurements in a prepare-and-measure scenario involving a sequence of measurements, using figures of merit that are closely linked to the $2^2 \to 1$ RAC. To achieve the optimal success probability in the game, one party needs to perform a so-called Lüders instrument, which corresponds to a non-projective measurement. The authors then derive bounds on the maximal eigenvalue of the corresponding measurement operators given an observed score in the game, using a numerical approach based on an adaptation of the NPA hierarchy to the prepare-and-measure scenario.

9.2.3 Self-testing through noncontextuality inequalities

One of the important features of quantum theory is contextuality, first noticed via the Kochen-Specker theorem [KS67]. In general, in any deterministic hidden variable model reproducing quantum correlations, the outcome of a measurement M must depend on its context, *i.e.* the set of compatible measurements one may perform alongside M. Contextuality can be detected through the violation of noncontextuality inequalities, of which the simplest is the Klyshko-Can-Binicioğlu-Shumovsky (KCBS) inequality [KCBS08]. It corresponds to the scenario in which five projective binary measurements $\{\mathsf{M}_i = (\mathsf{M}_{0|i}, \mathsf{M}_{1|i})\}_{i=1}^5$ can be performed and each pair $\mathsf{M}_i, \mathsf{M}_{i+1}$ is compatible, i.e.

$$[\mathsf{M}_i, \mathsf{M}_{i+1}] = 0 \tag{69}$$

and exclusive *i.e.* $\mathrm{tr}(\mathsf{M}_{0|i}\mathsf{M}_{0|i+1}) = 0$ (the labels of measurements are taken modulo 5). If we denote $p_i = \mathrm{tr}[\mathsf{M}_{0|i}\rho]$, where ρ is the measured state the KCBS inequality reads:

$$\sum_{i=1}^{5} p_i \leq 2.$$

The inequality is satisfied in all outcome deterministic noncontextual theories, while quantum measurements achieve the value $c_q = 5\cos(\pi/5)/(1+\cos(\pi/5))$. The maximal quantum value is achieved by measuring a pure state $\rho = |v_0\rangle\langle v_0|$ and measurements $\mathsf{M}_{0|i} = |v_i\rangle\langle v_i|$ where

$$|v_0\rangle = (1,0,0)^T,$$
$$|v_i\rangle = (\cos\theta, \sin\theta\sin\phi_i, \sin\theta\cos\phi_i)^T,$$

where $\cos\theta = \cos(\pi/5)/(1+\cos(\pi/5))$ and $\phi_i = i\pi(4/5)$.

Note that since this scenario consists of making measurements on a single quantum system, the statistics can always be simulated classically and it is thus impossible to achieve self-testing in a fully device-independent manner. In [BRV+19] the authors overcome this by assuming compatibility relations such as (69), thus rendering the scheme semi-device independent. Using this, they give a general scheme to self-test quantum states using noncontextuality inequalities and prove that the maximal quantum violation of the KCBS inequality robustly self-tests the above strategy. In other words, for any state ρ and measurements $\{|v_i\rangle\langle v_i|'\}$ which can be used to achieve the violation $c_q - \epsilon$ of KCBS inequality there exist a unitary U such that

$$\|U\,|v_i'\rangle - |v_i\rangle\,\| \leq O(\sqrt{\epsilon}), \qquad \forall i.$$

The proof holds also for the generalisations of KCBS inequality given in [BBC+11, AQB+13, LSW11]. The crux of the proof is an equivalence between the optimal strategy for violating the KCBS inequality and the solution to a certain type of SDP optimisation known as the Lovász theta number of an odd cycle graph [Lov79].

10 Applications of self-testing

The birth of self-testing is usually associated to the Mayers-Yao paper [MY04] from 2004. It set the terminology and formalism, including the first usage of the term self-testing in this context and identifying local isometries as relevant transformations. A similar main result as in [MY04] was presented in [MY98], although in the context of whether untrusted sources can be pertinent for cryptographic tasks. This earlier paper used the term 'self-checking' instead of 'self-testing'. Moreover, [MY98] is at the same time one of the pioneering works in device-independent cryptography, indicating importance of self-testing for the development of device-independent protocols. Since then self-testing has been scrutinised as a task of twofold significance:

- *purely theoretical*, related to exploring the conditions for a probability distribution to determine a specific quantum state and/or measurements, and proving that such statements also hold approximately. This theoretical aspect was reviewed in Sections 4,5, 6, 7, 8 and 9.2. As a result, ideas and results from self-testing can lead to progress in related theoretical areas.

- *practical*, relevant for creating new device-independent or semi-device-independent protocols for different tasks. In the Mayers-Yao paper [MY04] the authors say '*We hope that it will have application in different areas of quantum information processing*'. Fifteen years later we can observe that this hope is fulfilled.

In this section we give an overview of the applications of self-testing during the first fourteen years after the technique has been formally introduced. On the practical side, we cover the relation of self-testing with device-independent randomness generation in section 10.1, device-independent quantum cryptography in section 10.2, and device-independent entanglement certification in section 10.3. In section 10.4 we describe the applications to delegated quantum computing 10.4. Finally, from the theoretical side, in section 10.5 we describe the influence self-testing has had in understanding the structure of the set of quantum correlations. In particular in section 10.5.1 we highlight a link to the study of quantum correlations produced by finite vs infinite quantum systems, and in section 10.5.2 how self-testing has been used to prove an inequivalence between uncertainty relations and Bell nonlocality.

10.1 Device-independent randomness generation

The probabilistic nature of quantum mechanics can be exploited for generation of random numbers. In the simplest example, measuring in the computational basis a qubit in the state $|+\rangle$ results in a perfectly random output bit. However, the certification of the random nature of bits obtained this way relies on the exact characterisation of both the quantum state and the measurement performed. The device-independent scenario offers much less stringent requirements for randomness certification, by qualitatively relating randomness with nonlocality. By treating her devices as non-communicating black boxes Alice can certify some amount of randomness by observing the violation of a Bell inequality. The first results in this direction show that the maximal violation of the Mermin [Col06, CK11b] and the CHSH inequality [PAM+10] can be used in this way. For more information on certification of quantum randomness see [AM16] and references therein.

Here, we comment on the relation between self-testing and randomness. A self-testing protocol proves the existence of a pure entangled state and a certain set of measurements acting on it. Once this conclusion is made, certified random bits come for free since local measurements on a pure entangled state necessarily produce random outcomes. As a result, ideas from self-testing are often either implicitly present in device-independent randomness works or are explicitly used as tools to prove randomness lower bounds.

In the pioneering works of [Col06, CK11b] a self-testing statement is implicitly present, where the authors prove that only an orthogonal sum of GHZ states can maximally violate the Mermin inequality. In [CY14], the sequential self-testing of n EPR-pairs proven in [RUV13] is used as a subprotocol for infinite randomness expansion with a constant number of devices.

Simple symmetry-based arguments are used in [DPA13] to prove that the violation of some Bell inequalities can be used to certify the presence of genuine randomness. A necessary condition is that there exists a unique probability distribution maximally violating the Bell inequality. One way to prove such uniqueness is through self-testing: if the maximal violation of the Bell inequality is a self-test the maximally violating probability distribution has to be unique. Furthermore, incomplete results from [DPA13], were proven to be true by using self-testing techniques in [ŠASA16].

The results on self-testing properties of binary XOR games from [MS13] were expanded in [MS16] and used to devise protocols for exponential randomness expansion. More recently, the authors of [BMP18] directly use robust self-testing bounds for the tilted-CHSH inequality [BP15] to lower bound the randomness generated in their protocol. Self-testing techniques are also

used in [APVW16, ABDC18, WKB+19] to prove that two bits of local randomness can be certified from a two-qubit entangled state.

10.2 Device-independent quantum cryptography

10.2.1 Quantum key distribution

Quantum key distribution (QKD) is the most widely studied quantum cryptographic protocol in which two parties, Alice and Bob, use quantum resources to generate a shared private key which can later be used for encryption and decryption of messages. The security of a standard QKD protocol relies on the correct characterisation of all devices, which can be difficult to achieve in practice and far from ideal from a security perspective. An alternative approach comes from device-independent quantum key distribution (DIQKD), where security is based only on the observation of the correlations, and can be proven even if the constituent devices are treated as black boxes. DIQKD is intimately related to DI randomness generation; whereas in randomness generation one aims to have random outcomes, in a DIQKD protocol one aims to have random outcomes that are also correlated between Alice and Bob (thus ensuring a shared private key). As with randomness generation, the security of DIQKD is often measured against the violation of some Bell inequality. For a concise review on the topic see [ER14].

An indication of a close relation between DIQKD and self-testing is their common root in the Mayers-Yao work [MY98]. It discusses self-testing as a protocol for the first time (under the name self-checking) and recognises that it can help to use untrusted devices in cryptographic setting. [MY98] consider the BB84 protocol [BB84] in which Alice certifies an untrusted source she wants to use. The source is supposed to emit EPR pairs with Alice keeping one particle and measuring it and sending the other one to Bob. The untrusted source can be self-tested using the Mayers-Yao self-testing criterion, as explained in section 5. The protocol is later discussed in [MT02] in the context of the Ekert QKD protocol [Eke91]. The second Mayers-Yao paper [MY04], improving the first one by characterising the measurements (and introducing the phrase 'self-testing') also discussed the relation of self-testing with the BB84 protocol.

Ever since then self-testing and DIQKD have been intertwined. A certification of some quantum resource is implicitly present in every DIQKD security proof, however in some works the relation between self-testing, as the strongest form of certification, and DIQKD was explicitly examined. The effect of the inability to self-test complex measurements on the security of cryptographic tasks has been the subject of [MM11]. The authors prove that the 6-state QKD protocol [BBBW84, Bru98] can be secure even if the devices are untrusted, despite the issue with complex conjugation. Similarly like in the protocols for randomness expansion, the self-testing properties of XOR binary nonlocal games explored in [MS13] were used in [MS16] to prove the security of certain class of QKD protocols. Finally, the concept of parallel DIQKD developed analogously to parallel self-testing was first introduced in [JMS17] and the security proof relied on the rigidity of the magic square game [WBMS16] allowing for parallel self-testing of two singlets. A simplified proof appeared in [Vid17].

10.2.2 Cryptography beyond quantum key distribution

Bit commitment— Bit commitment is a cryptographic primitive in which Alice chooses a bit b that she wants to first commit, then later reveal, to Bob. The protocol should be both binding (Alice should not be able to change her choice of b after the commit step) and hiding (Bob should not be able to know b until Alice chooses to reveal). In a classical protocol, either Alice or Bob can cheat with probability 1 without being caught, *i.e.* either Alice can alter the bit after committing or Bob can learn it before it is revealed. Although unconditionally secure bit commitment is known to be impossible even using quantum resources [May97, LC97], there exist quantum protocols in which either party's probability to successfully cheat is strictly smaller than 1 [CK11a]. [SCA+11] introduces the idea of a DI quantum bit commitment protocol in which besides not trusting each other, Alice and Bob do not trust their equipment either. The security of the protocol is based on the self-testing fact that the maximal violation of the Mermin inequality can only be achieved by measuring the GHZ state. A version of DI quantum bit commitment based on the

violation of the CHSH inequality is presented in [AMPS16], in which the security can be seen as consequence of the self-testing properties of the CHSH inequality. Similarly, the violation of the CHSH inequality has been used to prove the security of DI relativistic bit commitment in [AK15], ruling out the possibility of location attacks in which devices are able to track their own space and time coordinates. None of the works explicitly relate their results to the corresponding self-testing protocol however.

Weak string erasure— Weak string erasure (WSE) [KWW12] is a primitive which can be used in two-party cryptographic protocols in which no large scale reliable quantum storage is available to the cheating party. WSE provides a random bit string $(b_1, \cdots, b_n)$ to Alice, while sending a randomly chosen substring $(b_{i_1}, \cdots, b_{i_k})$ to Bob, together with the set $(i_1, \cdots, i_k)$ specifying the location of substring bits. WSE is secure against Bob if he cannot learn much about the full string given to Alice, while it is secure against Alice if she cannot learn the location of Bob's bits. A DI version of this protocol useful for bit commitment or oblivious transfer is introduced in [KW16] and the security is related to the self-testing properties of the CHSH inequality.

Position verification— Finally, we briefly mention the position verification primitive, useful in position-based cryptography in which the parties have to convince the (honest) verifiers that they are located at a particular location. Protocols for position verification that improve the security by using quantum communication have been proposed in [KMS11, Mal10]. The DI security of position verification against adversaries with no quantum memory is proven in [RTK+18], and can also be traced to the self-testing properties of the CHSH inequality.

10.3 Entanglement detection

One of the most basic tasks in quantum information is that of detecting entanglement of a bipartite quantum system via local measurements on its subsystems. Device-independent entanglement detection considers this problem in the device-independent scenario, i.e. where all local measurement devices are treated as black boxes. Since the observation of Bell nonlocal correlations necessarily implies that the underlying state is entangled, the standard approach to DI entanglement detection involves violating a Bell inequality. However, since there exist entangled mixed states that do not violate any Bell inequality[2] [Wer89, Bar02, ADA14, BHQB16, JHA+15, BFF+16, HQB+16], this method cannot be used for all entangled states. A partial solution to this problem, allowing for the entanglement detection of all entangled states, was given in [Bus12] (see also [BRLG13]) using the concept of a 'semi-quantum game'. Here, the classical inputs in a Bell test are replaced by 'quantum inputs' $|\psi_x\rangle, |\psi_y\rangle$, that is, a set of known quantum states that are sent to the measurement device instead of the classical labels x and y. This scenario is semi-device-independent since although the measurement devices are treated as black boxes, the quantum input states must be trusted.

In [BŠCA18a, BŠCA18b], tools from self-testing and semi-quantum games were used to construct fully DI protocols for the entanglement detection of all entangled mixed states. The idea is as follows. If one achieves a self-test of a particular state and local measurements for Alice, then this certifies (up to a local isometry) the reduced states of Bob conditioned on a particular choice of input/output for Alice. In this way one can certify an ensemble of state preparations (conditioned on Alice's input/output) on Bob's local Hilbert space. These preparations can then be used as quantum inputs in a semi-quantum game. Since (i) the quantum inputs are now certified device-independently, (ii) the semi-quantum games scenario can be applied to all entangled states, the two can be combined to construct a fully device-independent protocol that works for all entangled states. Specifically, one needs to consider a network scenario in which the state of interest is augmented with two auxiliary bipartite states that are used to prepare the quantum inputs. Here, tools from parallel self-testing as well as the issue of complex conjugation become important for the general proof.

[2] At least in the original Bell scenario in which Alice and Bob can perform any number of non-sequential local measurements on a single copy of the state. In more complex measurement scenarios (see [CASA11, SDSB+05, Pal12, TRC19, BRGP12, HQBB13, Pop95]) it is generally unknown if such states exists.

10.4 Delegated quantum computing

Delegated computation is a protocol in which a party, usually called a verifier, delegates a computational task to another party, usually called a prover. The verifier aims to solve difficult computational tasks, but does not have enough computational resources. The prover, on the other side, has a very powerful computer and is able to solve any task the verifier is interested in. When one talks about delegated quantum computation (DQC) the prover possesses a quantum computer, while the verifier has either only classical computing resources or limited quantum resources but wants to solve a problem intractable for classical computing devices. For a concise review on the existing approaches in DQC see [GKK18].

There are two desirable properties of a DQC protocol: verifiability and blindness. The protocol is said to be verifiable if the verifier can be convinced that the solution provided by the prover(s) is correct. This is non-trivial, since the verifier is unable to solve the problem. Blindness of the protocol is related to the secrecy of the computation. It is ensured when the prover(s) cannot learn anything about the computational task the verifier wants to perform. It is very difficult to construct a DQC protocol with a fully classical verifier and a single prover which is verifiable and blind. The first protocol that achieves this, under computational assumptions, is [Mah18]. In principle, it is easier to achieve both verifiable and blind protocol with a classical verifier when there is more than one prover. In this case the provers are entangled and forbidden to communicate. Verifiability is proven if the verifier can be convinced that the two or more non-communicating provers are performing the prescribed sequence of measurements. This, of course, requires that the verifier be able to test that the provers perform measurements from a set that is universal for quantum computing. The latter is exactly a self-testing task. Thus it is no surprise, that self-testing is useful for such a delegation protocol, yet orchestrating such a computation in a verifiable fashion is a delicate task. Delegation protocols with two or more provers based on self-testing typically achieve information theoretic security.

The first such protocol was presented by Reichardt, Unger and Vazirani (RUV) in [RUV13]. The protocol involves two provers sharing a tensor product of many EPR pairs and the computation model is quantum computation by teleportation [GC99]. The provers are able to convince the verifer that they posses N EPR pairs by obtaining the optimal score in sequential playing of the CHSH game. The complexity of RUV protocol in terms of time and the number of EPR pairs needed is extremely large. The protocol was subsequently improved in [JMS20] where each Bell pair is shared by two provers, making the number of provers increase significantly at the expense of reducing the overall complexity. The advantage of parallel self-testing of N EPR pairs instead of sequential was exploited in [NV17] and [CGJV17]. The latter obtains a protocol with an almost optimal overhead (in the size of the computation) in terms or resources used, by exploiting parallel self-tests with robustness independent of the number of EPR pairs tested, discussed previously in subsection 5.3. The work [GKW15] shows that RUV protocol can be significantly improved if the verifier is actually quantum and wants to be convinced that they share with the prover n EPR pairs. In this case the self-testing of n EPR pairs through steering becomes a relevant sub-protocol.

Another example of self-testing incorporated into a delegated quantum computing protocol is [McK16a]. The DQC protocol involves many provers which share a graph state. The model of computation is measurement-based quantum computing (MBQC) [RB01, RBB03]. The protocol is made verifiable by using the self-testing of graph-states mostly based on [McK14]. Based on a similar idea a significantly simplified protocol appeared in [HH18]: since the triangular lattice graph state is universal for MBQC [MP13] the number of provers can be reduced to three and the number of necessary copies of the graph states is also considerably smaller than in [McK16a].

10.5 Structure of the set of quantum correlations

Here we highlight two ways in which self-testing as furthered our understanding of the set of quantum correlations.

10.5.1 Correlations from finite vs infinite dimensional quantum strategies

It is said that the correlations $\{p(a,b|x,y)\}_{a,b,x,y}$ admit a quantum strategy if there exists a state

$|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ and projective measurements $\{\mathsf{M}_{a|x}\}_{a,x}, \{\mathsf{N}_{b|y}\}_{b,y}$ such that

$$p(a,b|x,y) = \langle\psi|\mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y}\,|\psi\rangle\,.$$

This strategy is also called a *tensor-product strategy* due to the tensor product between Alice's and Bob's spaces. Different sets of quantum correlations arise when certain conditions are imposed on the state $|\psi\rangle$ and/or measurements $\{\mathsf{M}_{a|x}\}_{a,x}, \{\mathsf{N}_{b|y}\}_{b,y}$. The correlations obtained through a tensor-product strategy on finite-dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ constitute the set denoted as $\mathcal{C}_q$. If the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ can also be infinite dimensional the set is denoted as $\mathcal{C}_{qs}$. The closure of the set $\mathcal{C}_q$ is called $\mathcal{C}_{qa}$. Additionally, a *commuting-operator strategy* is one in which no tensor product structure is imposed but instead all measurement operators of Alice commute with all those of Bob, i.e.

$$p(a,b|x,y) = \langle\psi|\mathsf{M}_{a|x}\mathsf{N}_{b|y}\,|\psi\rangle\,.$$

with $[\mathsf{M}_{a|x}, \mathsf{N}_{b|y}] = 0$. The commuting-operator model is used in algebraic quantum field theory and all such correlations are denoted by the set $\mathcal{C}_{qc}$. The set inclusion relation defines a hierarchy among these sets [PT15]:

$$\mathcal{C}_q \subseteq \mathcal{C}_{qs} \subseteq \mathcal{C}_{qa} \subseteq \mathcal{C}_{qc}. \tag{70}$$

Whether $\mathcal{C}_{qc}$ is equivalent to either $\mathcal{C}_{qs}$ or $\mathcal{C}_{qa}$ are problems known as Tsirelson's problems [Tsi93]. Recently, it has been proven that $\mathcal{C}_{qs} \neq \mathcal{C}_{qc}$ [Slo20], and also that $\mathcal{C}_{qs} \neq \mathcal{C}_{qa}$ in [Slo19]. Whether $\mathcal{C}_{qa} \subset \mathcal{C}_{qc}$ remains an open problem.

Self-testing techniques have also inspired proving a strict inclusion of $\mathcal{C}_q$ in $\mathcal{C}_{qs}$. The inequivalence between these two sets was proven in [CS17c] in cases when either the number of inputs or the number of outputs is infinite. The separation between $\mathcal{C}_q$ and $\mathcal{C}_{qs}$ for finite input or output alphabets was proven by the same authors in [CS18]. The separation is demonstrated by explicitly giving the correlations which can be obtained with infinite-dimensional quantum strategies, but not with any finite-dimensional ones. The proof is inspired by the protocol for self-testing infinite-dimensional bipartite pure states, described in section 5.2.1. In the finite case, the self-test of a bipartite state can be interpreted as involving one of two different protocols depending on the parity of the dimension. An infinite dimensional state does not have a defined parity and can thus be self-tested by either protocol. The authors use this fact as the theoretical basis to prove the separation.

Following Slofstra's proof of non-closure of the quantum set of correlations [Slo19] alternative proofs appeared in [DPP19] and [MR19]. All these proofs rely on the representation theory of C^*-algebras. A relatively simpler proof, using embezzling entanglement [vDH03] and self-testing, is presented in [Col20].

10.5.2 Uncertainty relations and Bell nonlocality

Self-testing has also been used as a tool to understand the relationship between uncertainty relations, steering and Bell nonlocality. In [OW10] it was shown that in the optimal quantum strategy for a large class of Bell inequalities called XOR games, the steered states of Bob after a measurement by Alice are always such that they saturate a fine-grained uncertainty relation defined by the Bell inequality itself. This was then extended to more Bell inequalties in [ZGZ+16]. Whether such a link was true for generic Bell inequalities remained an open question.

In [RM+18] (building on [ZGZ+16]) the authors answer this in the negative by providing specific examples of Bell inequalities for which the relationship does not hold. To achieve this, self-testing statements for the Bell inequalities are proven, from which the form of the steered states can be determined and checked against the corresponding uncertainty relations. The self-testing statements are proven using Jordan's lemma (see section 7.1.2) to reduce the problem to essentially a two-qubit strategy, which simplifies the analysis significantly.

11 Experiments

The bulk of self-testing procedures are still only theoretical recipes. This is understandable since the majority of robust self-testing protocols have fidelity bounds that decrease rapidly with noise and serve only as a proof of principle. However, in the last years there has been an increasing number of self-testing protocols robust to realistic amounts of noise (see section 7). Here we mention the few experimental realisations of such protocols.

The biggest experimental hurdle towards fully device-independent protocols is simultaneously closing detection and locality loopholes. [BRS+18] reports the self-testing of a Bell state distributed over 398 meters through the violation of the CHSH inequality free of both detection and locality loopholes and furthermore free of the i.i.d. assumption. In this light it is the first fully device-independent self-testing protocol to be implemented in practice. Entanglement between the distant atoms is generated by entangling the spin of each atom with polarisation of a single photon. The obtained fidelity is 55.54% at a confidence level of 99%. By applying the same theoretical tools to analyse the data obtained in the loophole-free Bell test presented in [HKB+16] no fidelity higher than the trivial 50% could be found.

The remainder of the experimental self-testing contributions are not based on a completely loophole-free Bell tests. [TWE+17] reports a high violation of the CHSH inequality by a pair of $^9Be^+$ ions. The violation is used to make a self-testing statement, based on [Kan16]. At the 95% confidence level the pair of $^9Be^+$ ions has 0.958 fidelity with the maximally entangled pair of qubits. An overview of the inferred self-testing bounds from some previous works reporting CHSH violations is also presented. In [ZCP+18] the operator inequalities for robust self-testing from [Kan16] are tested for a large number of bipartite and tripartite qubit states encoded in photon polarisation degrees of freedom.

Experimental robust self-testing of partially entangled pairs of qubits using the Swap method is presented in [ZCY+19]. The systems under consideration are polarisation entangled photons. Self-testing of partially entangled qubit pairs is also used to heuristically estimate the fidelity of a produced ququart state with a given reference state. Robust self-testing of partially entangled pairs of qubits encoded in photon polarisation degrees of freedom was reported in [GMM+19]. The self-testing was done through the violation of the tilted CHSH inequality and the robustness bounds were estimated by using the numerical results from [CKS19]. In [GPL+19] the authors explore the certification of partially entangled pairs of photons encoded in the polarisation degree of freedom. The fidelity of the entangled pair with the corresponding partially entangled pair of qubits is estimated in two ways: by using standard tomographic methods and self-testing. The obtained fidelities have ratio ≈ 0.998, implying that for the case of qubit states self-testing can be used to achieve almost the same conclusions as tomography. It is argued that self-testing may have an advantage over tomography even when the detection and locality loopholes are not closed since it avoids characterisation of measurements and assumptions about dimension and, in principle, requires estimating fewer average values.

In [WPD+18] various two-qutrit entangled states are self-tested using photons entangled in the mode degree of freedom of the waveguides in a silicon based integrated optical chip. Fidelity bounds were obtained numerically via the Swap method. The self-tested states are the maximally entangled pair of qutrits (estimated fidelity 0.799), the state maximally violating the CGLMP inequality [CGL+02] (estimated fidelity 0.68) and a state maximally violating an extension of one of the SATWAP inequalities [SAT+17] (estimated fidelity 0.832).

Experimental self-testing in the steering scenario is the subject of [LLW+19]. The fidelity of the underlying physical state with the GHZ state is estimated based on the violation of the Mermin's steering inequality [CHRW11]. The fidelity lower bound is estimated to be $0,7866$, while the tomographically retrieved fidelity is 0.8725 ± 0.0034.

Finally, in [ZCP+19] the authors report an experimental realisation of a robust self-test of a Bell state measurement based on the entanglement swapping protocols of [SBWS18, RKB18] (see section 9.1). Photon pairs that are hyperentangled in the spatial and polarisation degrees of freedom are used to encode the two maximally entangled pairs of qubits that are needed for the entanglement swapping protocol.

12 Concluding remarks and open questions

Recent years have seen an increased interest in device-independent self-testing, accompanied by the plethora of self-testing protocols and methods presented in this review. However, there are still many important unresolved questions.

Without aiming to exhaust the list, we name some open questions and research directions which we believe worthy of attention.

Analytic methods for dimension larger than 2—The majority of known self-testing protocols are either built to self-test multi-qubit states and measurements, or apply existing qubit protocols to the self-testing of higher dimensional systems. The self-testing of states and measurements using methods that exploit the genuine d dimensional nature of quantum systems, is however still a very unexplored area. For instance, it has been known for a long time that via the numerical Swap method, the CGLMP inequality self-tests the two-qutrit state of equation (43). However, a corresponding analytic proof of this statement is still lacking, despite the relative simplicity of the inequality. Similarly desirable are analytic proofs for the self-testing of the maximally entangled states in dimension d using the SATWAP inequalities [SAT+17]. With respect to high dimensional measurement self-testing, one important open question is to extend the analytic self-test of a set of qutrit mutually unbiased basis measurements and the maximally entangled state of [KŠT+19] to higher dimensions. Moving beyond high dimensional systems to continuous variable systems, essentially nothing is known and there exist no protocols to self-test such states.

Multipartite methods—In a similar vein, techniques for self-testing general multipartite states are also needed, since current methods are only known for restricted classes such as graph states. One potential line of research in this direction would be to develop methods to self-test multi-qubit hypergraph states [RHBM13], which exhibit a richer structure than graph states but still admit a useful description in terms of Clifford group stabiliser operators. One would thus need a general method to construct Bell inequalities for such states, as was done for graph states [GTHB05, BAŠ+20]. This appears more complicated for hypergraph states however since the nonlocal nature of the hypergraph stabilizer operators means they do not have an obvious interpretation as local measurement observables (although some progress has been made [GBG16]).

Identifying the set of undetectable transformations—Part of the challenge in going beyond two qubit methods is to identify the set of local transformations defining the equivalence classes of self-testable states and measurements in higher dimensions. As we have seen, the standard definitions presented in section 3 need to be adapted in order to self-test complex valued measurements, stemming from the invariance of quantum correlations under complex conjugation of the state and measurement operators. In higher dimensions, it is still unknown whether there exist more state and measurement transformations that leave correlations invariant. If such transformations exist, an all-encompassing definition of what it means to self-test a state and measurements in general dimension is therefore still missing.

Self-testing of a state or measurements only—In many self-testing works, a self-testing statement for the state is accompanied by an additional self-testing statement for the measurements. One interesting problem would be to find situations where the correlations allow one to identify the state, but not the measurements, even allowing for the freedom of complex conjugation of the measurements in the definition of measurement self-testing. Similarly, it would be interesting to find correlations that allow one to self-test the measurements, but not the state.

Self-testing in non-i.i.d. scenarios—Throughout this review we have made the assumption that each round of the experiment is independent and identical to all others. It would be interesting and practically relevant to attempt to remove this assumption from self-testing protocols. One way to achieve this would be to build sequential self-testing protocols akin one in [RUV13] or by leveraging some recently introduced techniques [BRS+18, DFR16, AFRV19, AF18] for such scenarios. Methods could be borrowed also from the protocols for delegated quantum computation, *i.e.* [CGJV17]. Since the state and measurements can now depend on settings and outcomes in previous rounds, one would also need to adapt the definition of self-testing to apply to such scenarios, as well as derive corresponding confidence bounds from finite statistics. For example, the aim would be to show that, to high statistical confidence, the source is producing something close (by some measure) to n independent copies of $|\psi'\rangle$, where n is the number of experimental rounds.

Improved robustness methods—Finally, methods to improve the robustness bounds of general self-testing protocols are much in need. In practice, the applicability of the majority of self-testing protocols is hindered by very poor tolerance to noise. Significant improvements have been achieved for simple scenarios [Kan16], however it is not clear if these methods can be extended to scenarios with more inputs and outputs due to their dependence on Jordan's lemma. Finding a good robustness bound involves a difficult maximisation over all local isometries, and as a result nearly all methods use one of the few Swap isometries that are known to give good results in the well-explored simple cases. Thus, knowing more useful isometries and understanding which work well for particular classes of states would likely lead to improved robustness bounds.

Acknowledgements

We are grateful to Alexia Salavrakos, Jean-Daniel Bancal, Andrea Coladangelo, Jed Kaniewski, Armin Tavakoli, Erik Woodhead, Alejandro Pozas-Kerstjens, Aleksandra Dimić, Marc-Olivier Renou, Felix Hüber, Sébastien Designolle, Nicolas Brunner, Yeong Cherng Liang, Nikolai Miklin and Rotem Arnon-Friedman for suggestions while preparing the manuscript. We acknowledge funding from the ERC CoG QITBOX, the Spanish MINECO (QIBEQI FIS2016-80773-P, Severo Ochoa SEV-2015-0522), Fundacio Cellex, Generalitat de Catalunya (SGR 1381 and CERCA Programme). IŠ acknowledges funding from SNSF (Starting grant DIAQ). JB acknowleges funding from the Juan de la Cierva-formación grant the AXA chair in quantum information science.

A Appendix

A.1 Self-testing complex measurements

Here we give a possible definition of self-testing of states and complex valued measurements.

Definition 6. (*self-testing of states and complex measurements)*
We say that the correlations $p(a,b|x,y)$ *self-test the state and measurements* $|\psi'\rangle_{\mathrm{A'B'}}, \{\mathsf{M}'_{a|x}\}, \{\mathsf{N}'_{b|y}\}$ if for all states and measurements $\rho_{\mathrm{AB}}, \{\mathsf{M}_{a|x}\}, \{\mathsf{N}_{b|y}\}$ compatible with $p(a,b|x,y)$ there exists a local isometry $\Phi = \Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}$ such that for any purification $|\psi\rangle_{\mathrm{ABP}}$ of ρ_{AB} there exists some state $|\xi\rangle_{\bar{\mathrm{A}}\bar{\mathrm{B}}\mathrm{P}}$ such that

$$\begin{aligned}\Phi \otimes \mathbb{1}_{\mathrm{P}} \left[\mathsf{M}_{a|x} \otimes \mathsf{N}_{b|y} \otimes \mathbb{1}_{\mathrm{P}} |\psi\rangle_{\mathrm{ABP}}\right] \\ = \tilde{\mathsf{M}}_{a|x} \otimes \tilde{\mathsf{N}}_{b|y} \otimes \mathbb{1}_{\mathrm{P}} \left(|\psi'\rangle_{\mathrm{A'B'}} \otimes |\xi\rangle_{\bar{\mathrm{A}}\bar{\mathrm{B}}\mathrm{P}}\right),\end{aligned}$$

for all a, x, b, y, and where

$$\begin{aligned}\tilde{\mathsf{M}}_{a|x} &= \mathsf{M}'_{a|x} \otimes \mathsf{S}_0^{\bar{\mathrm{A}}} + (\mathsf{M}'_{a|x})^* \otimes \mathsf{S}_1^{\bar{\mathrm{A}}} \\ \tilde{\mathsf{N}}_{b|y} &= \mathsf{N}'_{b|y} \otimes \mathsf{T}_0^{\bar{\mathrm{B}}} + (\mathsf{N}'_{b|y})^* \otimes \mathsf{T}_1^{\bar{\mathrm{B}}} \\ &\mathsf{S}_0 + \mathsf{S}_1 \mathbb{1}_{\bar{\mathrm{A}}}, \quad \mathsf{T}_0 + \mathsf{T}_1 = \mathbb{1}_{\bar{\mathrm{B}}}, \\ &\langle\xi|(\mathsf{S}_0 \otimes \mathsf{T}_0 + \mathsf{S}_1 \otimes \mathsf{T}_1) \otimes \mathbb{1}_{\mathrm{P}} |\xi\rangle = 1.\end{aligned}$$

Here, the S_i and T_i part of the measurements are acting as effective controlled complex conjugations of the reference measurements. The final condition ensures that this conjugation is performed in a correlated fashion as implied from (14). The probability that the conjugation is performed depends on the (unknown) junk state and is thus unknown. Note that if one traces out all but the $\bar{\mathrm{A}}\bar{\mathrm{B}}$ space, one obtains some convex combination of the reference and conjugated measurements acting on the reference state.

A.2 Regularisation trick

In this appendix we give more details about the so-called regularisation trick. It refers to the case when one of the operators used to build the Swap gate (see figure 4) is not unitary. This happens already in the case described in Chapter 4 where the operators Z_{A} and X_{A} from equation (32) might have some zero eigenvalues. Let us focus on $\mathsf{Z}_{\mathrm{A}} = (\mathrm{A}_0 + \mathrm{A}_1)/\sqrt{2}$. The first step in the regularisation procedure is to change all the zero eigenvalues of Z_{A} to 1, resulting in a new operator $\mathsf{Z}^*_{\mathrm{A}}$. In the second step, all eigenvalues are normalized, *i.e.* the new operator defined as $\hat{\mathsf{Z}}_{\mathrm{A}} = \mathsf{Z}^*_{\mathrm{A}}/|\mathsf{Z}^*_{\mathrm{A}}|$ is unitary by construction. However, one has to prove that $\hat{\mathsf{Z}}_{\mathrm{A}}$ acts on the physical state in the same way as Z_{A}. For that the following series of inequalities can be used (Note that $\mathsf{Z}^*_{\mathrm{A}}$ acts on $|\psi\rangle$ in the same way as Z_{A} since it can be seen as $\mathsf{Z}_{\mathrm{A}} + P$ where P is the projector

on the kernel of Z_A):

$$\begin{aligned}\|(\hat{\mathsf{Z}}_\mathrm{A} - \mathsf{Z}_\mathrm{A})\,|\psi\rangle\,\| &= \|(\mathbb{1} - \hat{\mathsf{Z}}_\mathrm{A}^\dagger \mathsf{Z}_\mathrm{A})\,|\psi\rangle\,\| \\ &= \|(\mathbb{1} - |\mathsf{Z}_\mathrm{A}|)\,|\psi\rangle\,\| \\ &= \|(\mathbb{1} - |\mathsf{Z}_\mathrm{A}\mathsf{Z}_\mathrm{B}|)\,|\psi\rangle\,\| \\ &\leq \|(\mathbb{1} - \mathsf{Z}_\mathrm{A}\mathsf{Z}_\mathrm{B})\,|\psi\rangle\,\| \\ &= 0\end{aligned}$$

The first line is the consequence of the unitarity of $\hat{\mathsf{Z}}_\mathrm{A}$ and the second uses the definition of $\hat{\mathsf{Z}}_\mathrm{A}$. To get the third line we used the fact that Z_B is unitary. The inequality follows from the operator inequality $A \leq |A|$. The last line stems from equation (31). The key ingredient necessary for regularisation is exactly equation (31). In general, the regularisation of any operator A can be done if there is a unitary U such that $A \otimes \mathbb{1}\,|\psi\rangle = \mathbb{1} \otimes U\,|\psi\rangle$.

A.3 Swap isometries

In this appendix we provide further comments on the different Swap isometries used in the self-testing protocols. In section 4.3 we mentioned that the partial Swap gate given on figure 4 is appropriate only if the ancillas are initiated in the state $|0\rangle$. In the case that the ancillas are in a different state the correct isometry to use is the full Swap gate, given in figure 10.

A generalisation of the Swap gate, given on figure 11, can be used for self-testing of bipartite qudit states $|\psi\rangle = \sum_{j=0}^{d-1} \lambda_j\,|jj\rangle$, where λ_j are positive real numbers. The gate F is the Fourier transform defined as:

$$F\,|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{jk}\,|k\rangle\,,$$

where d is the local dimension of the reference state, and ω is the d-th root of the unity. The controlled gates $C\bar{\mathsf{Z}}$ and $C\bar{\mathsf{X}}$ are defined as follows[3]:

$$\begin{aligned}C\bar{\mathsf{X}}\,|j\rangle\,|\psi\rangle &= |j\rangle\,\bar{\mathsf{X}}^{(j)}\,|\psi\rangle \\ C\bar{\mathsf{Z}}\,|j\rangle\,|\psi\rangle &= |j\rangle\,\bar{\mathsf{Z}}^{j}\,|\psi\rangle\,.\end{aligned}$$

For the gate on figure 11 to work as an effective Swap gate the operators $\bar{\mathsf{X}}$ and $\bar{\mathsf{Z}}$ have to satisfy certain conditions, mimicking anticommutativity

[3]Note that $\{\mathsf{X}^{(j)}\}$ are j different operators, while $\{\mathsf{Z}^j\}$ are j-th powers of the operator Z.

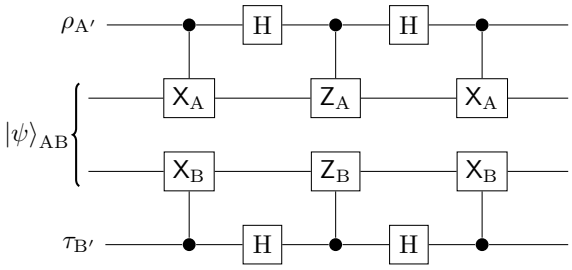


Figure 10: The full Swap gate used in some robust self-testing protocols. If the ancillas are initiated in the state $|0\rangle$ the gate reduces to the partial Swap gate, given on figure 4.

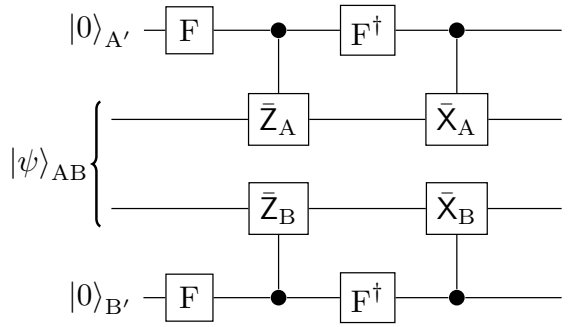


Figure 11: The partial Swap gate used in some protocols for robust self-testing of qudit entangled states.

from the qubit case. In [YN13] the authors give the recipe: operators $\bar{\mathsf{Z}}_\mathrm{A}$ and $\bar{\mathsf{Z}}_\mathrm{B}$ have to satisfy

$$\sum_{j=0}^{d-1} \omega^{ja} \bar{\mathsf{Z}}_\mathrm{A}^j \otimes \mathbb{1}\,|\psi\rangle = \mathbb{1} \otimes \sum_{j=0}^{d-1} \omega^{ja} \mathsf{Z}_\mathrm{B}^j\,|\psi\rangle\,, \quad (71)$$

for all $a \in \{1, \cdots, d\}$. In addition, operators $\bar{\mathsf{X}}_\mathrm{A}^{(k)}$ and $\bar{\mathsf{X}}_\mathrm{B}^{(k)}$ must satisfy

$$\begin{aligned}&\lambda_0 \bar{\mathsf{X}}_\mathrm{A}^{(k)} \otimes \sum_{j=0}^{d-1} \omega^{jk} \bar{\mathsf{Z}}_\mathrm{B}^j\,|\psi\rangle \\ &\quad = \lambda_k \sum_{j=0}^{d-1} \omega^{jd} \bar{\mathsf{Z}}_\mathrm{A}^j \otimes \left(\bar{\mathsf{X}}_\mathrm{B}^{(k)}\right)^\dagger |\psi\rangle\,, \qquad \forall k. \quad (72)\end{aligned}$$

It can be proven that the output state of the isometry Φ_d given on figure 11 and built from the operators satisfying the conditions (71) and (72) has the form $\sum_k \lambda_k\,|kk\rangle_\mathrm{AB} \otimes |\xi\rangle_\mathrm{AB}$ where $|\xi\rangle$ is some normalised state. For more details about the qudit Swap isometry see [YN13, CGS17, ŠCAA18].

A.4 Localising matrices in the Swap method

In section 7.1.4 we presented the numerical Swap method used in robust self-testing protocols. The

isometry used in the Swap method is the Swap gate and as we discussed in Appendix A.2 when one of the operators X_A, X_B, Z_A or Z_B is defined as a sum or difference of physical measurement observables, the Swap isometry might not be unitary. Let us, for simplicity, focus the CHSH case and the operator $\mathsf{Z}_\mathsf{A} = (\mathsf{A}_0 + \mathsf{A}_1)/\sqrt{2}$ and $\mathsf{X}_\mathsf{A} = (\mathsf{A}_0 - \mathsf{A}_1)/\sqrt{2}$ used to build the Swap isometry. In Appendix A.2 we showed how to regularize such operators for the purposes of the ideal self-testing.

The procedure to solve this problem when using the Swap isometry in robust self-testing protocols is introduced in [BNS+15, YVB+14]. In the context of the Swap method one solves the problem by introducing two new operators A_2 and A_3 which are unitary and not too different from $(\mathsf{A}_0 + \mathsf{A}_1)/\sqrt{2}$ and $(\mathsf{A}_0 - \mathsf{A}_1)/\sqrt{2}$, respectively. That way the isometry built by defining $\mathsf{Z}_\mathsf{A} = \mathsf{A}_2$ and $\mathsf{X}_\mathsf{A} = \mathsf{A}_3$ is necessarily unitary. One way to impose the proximity of A_2 and A_3 to $(\mathsf{A}_0 + \mathsf{A}_1)/\sqrt{2}$ and $(\mathsf{A}_0 - \mathsf{A}_1)/\sqrt{2}$, respectively, is by imposing the relaxation

$$\mathsf{A}_2(\mathsf{A}_0 + \mathsf{A}_1)/\sqrt{2} \geq 0 \tag{73a}$$

$$\mathsf{A}_3(\mathsf{A}_0 - \mathsf{A}_1)/\sqrt{2} \geq 0. \tag{73b}$$

This can be enforced by introducing two new moment matrices called the *localizing matrices*. The condition (73a) can be imposed as a requirement that the moment matrix defined as

$$\Gamma^k_{i,j}(\mathsf{A}_2) = \langle\psi|S^{(i)\dagger}\mathsf{A}_2\frac{\mathsf{A}_0 + \mathsf{A}_1}{\sqrt{2}}S^{(j)}\,|\psi\rangle\,, \tag{74}$$

where $S = \{\mathbb{1}, \mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2\}$, is positive semi-definite. An analogous constraint can be made to enforce the condition (73b).

B State and measurement assumptions

Here we overview the assumptions made about the state and measurements in the definitions of self-testing.

B.1 State

In the definitions of section 3 we use a purification $|\psi\rangle_{\mathrm{ABP}}$ of the potentially mixed physical state ρ_{AB}. One does not assume that the state shared between Alice and Bob is pure however, since it is given by

$$\rho_{\mathrm{AB}} = \mathrm{tr}_{\mathrm{P}}[|\psi_{\mathrm{ABP}}\rangle\langle\psi_{\mathrm{ABP}}|]. \tag{75}$$

Suppose we have a self-testing statement in the form of definition 1:

$$\Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}} \otimes \mathbb{1}_{\mathrm{P}}[|\psi\rangle_{\mathrm{ABP}}] = |\psi'\rangle_{\mathrm{A'B'}} \otimes |\xi\rangle_{\bar{\mathrm{A}}\bar{\mathrm{B}}\mathrm{P}}\,.$$

If we trace over the purification space on both sides of the above we obtain

$$\Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}[\rho_{\mathrm{AB}}] = |\psi'\rangle\langle\psi'|_{\mathrm{A'B'}} \otimes \sigma_{\bar{\mathrm{A}}\bar{\mathrm{B}}}.$$

where $\sigma = \mathrm{tr}_{\mathrm{P}}[|\xi\rangle\langle\xi|]$. Thus a self-testing statement of the form of definition 1, implies that the same isometry maps ρ_{AB} to the reference state. This is possible because the isometry map acts trivially on the purification space. This follows from the fact that the isometry is constructed from the measurement operators, which by assumption themselves act non-trivially only on ρ.

B.2 Measurements

We do, however, assume that the physical measurements are projective. This can lead to some confusion, since naturally one may want to repeat an analogous argument to the above that would allow one to treat the measurements as general POVM measurements, and simply make use of a Naimark dilation for mathematical convenience. We elaborate on this difficulty in doing this below.

Let us drop the projective assumption, so that the physical measurements are in general POVM measurements. Imagine we aim to self-test a set of measurements $\mathsf{M}'_{a|x}$ for Alice and the reference state $|\psi'\rangle$ in the sense of definition 2. This immediately poses a problem for the majority of self-testing proofs. For example in (30), one needs the physical measurements to be projective to guarantee $\mathsf{A}_x^2 = \mathbb{1}$ in order to prove anti-commutativity of the observables. In order to proceed to use the standard proofs of measurement self-testing, of which almost all assume the projective nature of the measurements, one has three options:

1. Prove that even if treating the physical measurements as POVM measurements, the only physical measurements that are compatible with the observed correlations are projective measurements.

2. Prove a general theorem that states that if one has an isometry mapping any Naimark dilation of the physical measurements to the reference measurements, this implies a (possibly different) isometry mapping the POVM physical measurements to the reference measurements in the sense of definition 2.

3. Argue that projective measurements are the only fundamental measurements in quantum theory. That is, POVM measurements can only be physically realised via a projective measurement on a dilated space.

Option 1 has been done very rarely; perhaps the only example can be found in [Kan16] when self-testing qubit Pauli measurements. Option 2 would be an analogue for the ability to use a purification of the state as explained above. However, such a theorem has not been proven to the best of our knowledge, and my may not be possible. We comment on option 3 at the end of this section.

Let us focus further on option 2. Define the physical measurements for Alice as usual by $\mathsf{M}_{a|x}$, which may now be POVM. Furthermore, define a Naimark dilation of these measurements by $\tilde{\mathsf{M}}_{a|x}$. The vast majority of self-testing works prove an isometry mapping the dilated measurements $\tilde{\mathsf{M}}_{a|x}$ to the reference measurements:

$$\Phi\left[\tilde{\mathsf{M}}_{a|x}\otimes\mathbb{1}_{\mathrm{B}}\left|\psi\right\rangle\otimes\left|\tilde{0}\right\rangle\right]=\mathsf{M}'_{a|x}\otimes\mathbb{1}_{\mathrm{B}'}\left|\psi'\right\rangle\otimes\left|\xi\right\rangle, \tag{76}$$

where we have explicitly written the ancilla state $\left|\tilde{0}\right\rangle\in\mathcal{H}_{\tilde{\mathrm{A}}}$ used for the dilation, and the purification space of the state is left implicit as in section 4. Now consider the physical (potentially POVM) measurements acting on the physical state.

$$\mathsf{M}_{a|x}\otimes\mathbb{1}_{\mathrm{B}}\left|\psi\right\rangle. \tag{77}$$

At this point, it is tempting to define an isometry Ω that maps this measurement to it's Naimark dilation:

$$\Omega[\mathsf{M}_{a|x}\otimes\mathbb{1}_{\mathrm{B}}\left|\psi\right\rangle]=\tilde{\mathsf{M}}_{a|x}\otimes\mathbb{1}_{\mathrm{B}'}\left|\psi\right\rangle\otimes\left|\tilde{0}\right\rangle, \tag{78}$$

One could then use the standard proof of self-testing by concatenating isometries. Note, however, that fixing an input x, the vectors on the right hand side of (78) are orthogonal for different a since for $a\neq a'$

$$\begin{aligned}&\left(\left\langle\psi\right|\otimes\left\langle\tilde{0}\right|\tilde{\mathsf{M}}_{a'|x}\otimes\mathbb{1}\right)\left(\tilde{\mathsf{M}}_{a|x}\otimes\mathbb{1}\left|\psi\right\rangle\otimes\left|\tilde{0}\right\rangle\right)\\ =&\left\langle\psi\right|\otimes\left\langle\tilde{0}\right|\tilde{\mathsf{M}}_{a'|x}\tilde{\mathsf{M}}_{a|x}\otimes\mathbb{1}\left|\psi\right\rangle\otimes\left|\tilde{0}\right\rangle=0.\end{aligned} \tag{79}$$

The corresponding inner product between the vectors inside the isometry in (78) is

$$\left\langle\psi\right|\mathsf{M}_{a'|x}\mathsf{M}_{a|x}\otimes\mathbb{1}\left|\psi\right\rangle, \tag{80}$$

which is generally not equal to zero if the measurements are POVM. Thus, (78) is generally not valid, since isometry maps conserve the inner product between vectors. This means that one cannot simply consider a Naimark dilation 'for free' since the map which takes the POVM measurements to the dilation is not an isometry.

Nevertheless, one may hope to prove that given a self-test of the dilated measurements (76), one could recover the corresponding map for the physical measurements by somehow discarding the ancilla degrees of freedom used in the dilation, as was done for the purification space of the state. The difficulty here however is that—unlike the purification space— the dilated space is explicitly used by the isometry, since it is constructed from the dilated measurements.

Consider a general state ρ on $\mathcal{H}_{\mathrm{A}}$. For any Naimark dilation $\tilde{\mathsf{M}}_{a|x}$ of $\mathsf{M}_{a|x}$ one has

$$\mathrm{tr}[\tilde{\mathsf{M}}_{a|x}\rho\otimes\left|\tilde{0}\right\rangle\left\langle\tilde{0}\right|]=\mathrm{tr}[\mathsf{M}_{a|x}\rho]. \tag{81}$$

Tracing over the ancilla space only we have

$$\mathrm{tr}[\mathbb{1}\otimes\left\langle\tilde{0}\right|(\tilde{\mathsf{M}}_{a|x})\mathbb{1}\otimes\left|\tilde{0}\right\rangle\rho]=\mathrm{tr}[\mathsf{M}_{a|x}\rho] \tag{82}$$

and since this holds for all ρ we must have

$$\mathsf{M}_{a|x}=\mathbb{1}\otimes\left\langle\tilde{0}\right|(\tilde{\mathsf{M}}_{a|x})\mathbb{1}\otimes\left|\tilde{0}\right\rangle. \tag{83}$$

Returning to (76), we insert the identity $\mathbb{1}_{\mathrm{A}}\otimes\sum_k\left|\tilde{k}\right\rangle\left\langle\tilde{k}\right|_{\tilde{\mathrm{A}}}$ inside the isometry, giving

$$\begin{aligned}&\Phi\left[\left[(\mathbb{1}_{\mathrm{A}}\otimes\sum_k\left|\tilde{k}\right\rangle\left\langle\tilde{k}\right|)\right]\tilde{\mathsf{M}}_{a|x})\otimes\mathbb{1}_{\mathrm{B}}\left|\psi\right\rangle\otimes\left|\tilde{0}\right\rangle\right]\\ &=\mathsf{M}'_{a|x}\otimes\mathbb{1}_{\mathrm{B}'}\left|\psi'\right\rangle\otimes\left|\xi\right\rangle.\end{aligned} \tag{84}$$

Taking the sum outside we find

$$\begin{aligned}&\sum_k\Phi\left[\tilde{\mathsf{M}}^k_{a|x}\otimes\mathbb{1}_{\tilde{\mathrm{A}}}\otimes\mathbb{1}_{\mathrm{B}}\left|\psi\right\rangle\otimes\left|\tilde{k}\right\rangle\right]\\ &=\mathsf{M}'_{a|x}\otimes\mathbb{1}_{\mathrm{B}'}\left|\psi'\right\rangle\otimes\left|\xi\right\rangle.\end{aligned} \tag{85}$$

Where

$$\tilde{\mathsf{M}}^k_{a|x}=\mathbb{1}_{\mathrm{A}}\otimes\left\langle\tilde{k}\right|(\tilde{\mathsf{M}}_{a|x})\mathbb{1}_{\mathrm{A}}\otimes\left|\tilde{0}\right\rangle. \tag{86}$$

From (83) we have $\tilde{\mathsf{M}}^0_{a|x}=\mathsf{M}_{a|x}$ and so

$$\begin{aligned}&\Phi\left[\mathsf{M}_{a|x}\otimes\mathbb{1}_{\tilde{\mathrm{A}}}\otimes\mathbb{1}_{\mathrm{B}}\left|\psi\right\rangle\otimes\left|\tilde{0}\right\rangle\right]\\ &=\mathsf{M}'_{a|x}\otimes\mathbb{1}\left|\psi'\right\rangle\otimes\left|\xi\right\rangle-\sum_{k>0}\Phi\left[\tilde{\mathsf{M}}^k_{a|x}\otimes\mathbb{1}_{\mathrm{B}}\left|\psi\right\rangle\otimes\left|\tilde{k}\right\rangle\right].\end{aligned} \tag{87}$$

If the sum in the right hand side of the above is zero then we have proven that the isometry Φ indeed maps the physical measurements to the reference measurements. However, it is not clear that there exists a Naimark extension such that this is always the case. Showing whether this is or is not possible would be a valuable contribution to the field.

Finally we comment on option 3. This position can be justified on the basis that all other operations in quantum theory (CPTP maps, non-projective measurements) can be seen as the result of combining unitary evolution and projective measurement, and so there is no logical problem that arises with this stance. For some, this argument is not convincing however, since they consider POVMs to be as 'real' as projective measurements, and thus deserve a place in the ontology of the theory.

An alternative way to argue the projective-only assumption is from a information theoretic perspective. More precisely, the measurement update rule in quantum theory can be understood as a process by which an observer updates their description of a quantum state given new information. This new information is given by the outcome of a measurement, and is *classical information* from the perspective of the observer (i.e. it is the classical information that the observer reads from the macroscopic degrees of freedom of the measurement device). Thus it is onto these degrees of freedom (which may have become entangled with the quantum system during the measurement procedure) that the measurement operators act. Since these degrees of freedom are perfectly distinguishable, the measurement operators are described by orthogonal projectors. If one performs another measurement, this amounts to applying a different unitary Schrodinger evolution to the state before observing the measurement procedure, thus mapping the measurement to a different projective measurement. The POVM update rule can then be understood as the effective measurement operator applied to the state that is induced by the observation of this classical information. In this sense, any measurement operator—which by definition describes the effect of obtaining classical information—is described by a projector.

References

[AAC+00] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach. Generalized Schmidt decomposition and classification of three-quantum-bit states. *Phys. Rev. Lett.*, 85:1560–1563, Aug 2000. doi:10.1103/PhysRevLett.85.1560.

[ABB+17] Ole Andersson, Piotr Badziąg, Ingemar Bengtsson, Irina Dumitru, and Adán Cabello. Self-testing properties of Gisin's elegant Bell inequality. *Phys. Rev. A*, 96:032119, Sep 2017. doi:10.1103/PhysRevA.96.032119.

[ABDC18] Ole Andersson, Piotr Badziąg, Irina Dumitru, and Adán Cabello. Device-independent certification of two bits of randomness from one entangled bit and Gisin's elegant Bell inequality. *Phys. Rev. A*, 97:012314, Jan 2018. doi:10.1103/PhysRevA.97.012314.

[ADA14] R Augusiak, M Demianowicz, and A Acín. Local hidden variable models for entangled quantum states. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424002, 2014. doi:10.1088/1751-8113/47/42/424002.

[AF18] Rotem Arnon-Friedman. *Reductions to IID in Device-independent Quantum Information Processing*. PhD thesis, 2018. arXiv:1812.10922.

[AFB19] Rotem Arnon-Friedman and Jean-Daniel Bancal. Device-independent certification of one-shot distillable entanglement. *New Journal of Physics*, 21(3):033010, mar 2019. doi:10.1088/1367-2630/aafef6.

[AFRV19] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. *SIAM Journal on Computing*, 48(1):181–225, 2019. URL: https://epubs.siam.org/doi/abs/10.1137/18M1174726, doi:10.1137/18M1174726.

[AFY18] Rotem Arnon-Friedman and Henry Yuen. Noise-Tolerant Testing of High Entanglement of Formation. In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *45th International Colloquium on Automata, Languages, and Pro-*

gramming (ICALP 2018), volume 107 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:12, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ICALP.2018.11.

[AK15] Emily Adlam and Adrian Kent. Device-independent relativistic quantum bit commitment. *Phys. Rev. A*, 92:022315, Aug 2015. doi:10.1103/PhysRevA.92.022315.

[AM16] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540:213–219, 2016. doi:10.1038/nature20119.

[AMP12] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108(10), Sep 2012. doi:10.1103/physrevlett.108.100402.

[AMPS16] N Aharon, S Massar, S Pironio, and J Silman. Device-independent bit commitment based on the CHSH inequality. *New Journal of Physics*, 18(2):025014, feb 2016. doi:10.1088/1367-2630/18/2/025014.

[ANTSV99] A. Ambainis, A. Nayak, A. Ta-Shama, and U. Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. *Proceedings of 31st ACM Symposium on Theory of Computing*, page 376, 1999. doi:10.1145/301250.301347.

[APVW16] Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. Optimal randomness certification from one entangled bit. *Phys. Rev. A*, 93:040102, Apr 2016. doi:10.1103/PhysRevA.93.040102.

[AQB+13] Mateus Araújo, Marco Túlio Quintino, Costantino Budroni, Marcelo Terra Cunha, and Adán Cabello. All noncontextuality inequalities for the n-cycle scenario. *Phys. Rev. A*, 88:022118, Aug 2013. doi:10.1103/PhysRevA.88.022118.

[Ard92] M. Ardehali. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. *Phys. Rev. A*, 46:5375–5378, Nov 1992. doi:10.1103/PhysRevA.46.5375.

[Bar02] Jonathan Barrett. Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality. *Phys. Rev. A*, 65:042302, Mar 2002. doi:10.1103/PhysRevA.65.042302.

[BAŠ+20] F Baccari, R Augusiak, I Šupić, J Tura, and A Acín. Scalable bell inequalities for qubit graph states and robust self-testing. *Physical Review Letters*, 124(2):020402, 2020. doi:10.1103/PhysRevLett.124.020402.

[BB84] Charles Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984*, pages 175–179, 01 1984. doi:10.1016/j.tcs.2014.05.025.

[BBBW84] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. Eavesdrop-detecting quantum communications channel. *IBM technical disclosure bulletin*, 26(8):4363–4366, 01 1984.

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, Mar 1993. doi:10.1103/PhysRevLett.70.1895.

[BBC+11] Piotr Badziąg, Ingemar Bengtsson, Adán Cabello, Helena Granström, and Jan-Åke Larsson. Pentagrams and paradoxes. *Foundations of Physics*, 41:414–423, 02 2011. doi:10.1007/s10701-010-9433-3.

[BBT05] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, Nov 2005. doi:10.1007/s10701-005-7353-4.

[BC90] Samuel L Braunstein and Carlton M Caves. Wringing out better Bell inequalities. *Annals of Physics*, 202(1):22 – 56, 1990. doi:10.1016/0003-4916(90)90339-P.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014. doi:10.1103/RevModPhys.86.419.

[BD10] Francesco Buscemi and Nilanjana Datta. Distilling entanglement from arbitrary resources. *Journal of Mathematical Physics*, 51(10):102201, 2010. doi:10.1063/1.3483717.

[BDSW96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, Nov 1996. doi:10.1103/PhysRevA.54.3824.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964. doi:10.1103/PhysicsPhysiqueFizika.1.195.

[BFF+16] Joseph Bowles, Jérémie Francfort, Mathieu Fillettaz, Flavien Hirsch, and Nicolas Brunner. Genuinely multipartite entangled quantum states with fully local hidden variable models and hidden multipartite nonlocality. *Phys. Rev. Lett.*, 116:130401, Mar 2016. doi:10.1103/PhysRevLett.116.130401.

[BHQB16] Joseph Bowles, Flavien Hirsch, Marco Túlio Quintino, and Nicolas Brunner. Sufficient criterion for guaranteeing that a two-qubit state is unsteerable. *Phys. Rev. A*, 93:022121, Feb 2016. doi:10.1103/PhysRevA.93.022121.

[BK93] A V Belinskii and D N Klyshko. Interference of light and Bell's theorem. *Physics-Uspekhi*, 36(8):653, 1993. doi:10.1070/pu1993v036n08abeh002299.

[BKM19] Spencer Breiner, Amir Kalev, and Carl A. Miller. Parallel self-testing of the GHZ state with a proof by diagrams. In Peter Selinger and Giulio Chiribella, editors, Proceedings of the 15th International Conference on *Quantum Physics and Logic,* Halifax, Canada, 3-7th June 2018, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 43–66. Open Publishing Association, 2019. doi:10.4204/EPTCS.287.3.

[BLM+09] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani. Device-independent state estimation based on Bell's inequalities. *Phys. Rev. A*, 80:062327, Dec 2009. doi:10.1103/PhysRevA.80.062327.

[BLR93] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. *J. Comput. Syst. Sci.*, 47(3):549–595, December 1993. doi:10.1016/0022-0000(93)90044-W.

[BM05] H. Buhrman and S. Massar. Causality and Tsirelson's bounds. *Phys. Rev. A*, 72:052103, Nov 2005. doi:10.1103/PhysRevA.72.052103.

[BMP18] Cédric Bamps, Serge Massar, and Stefano Pironio. Device-independent randomness generation with sublinear shared quantum resources. *Quantum*, 2:86, August 2018. doi:10.22331/q-2018-08-22-86.

[BMR92] Samuel L. Braunstein, A. Mann, and M. Revzen. Maximal violation of Bell inequalities for mixed states. *Phys. Rev. Lett.*, 68:3259–3261, Jun 1992. doi:10.1103/PhysRevLett.68.3259.

[BNS+15] Jean-Daniel Bancal, Miguel Navascués, Valerio Scarani, Tamás Vértesi, and Tzyh Haur Yang. Physical characterization of quantum devices from nonlocal correlations. *Phys. Rev. A*, 91:022115, Feb 2015. doi:10.1103/PhysRevA.91.022115.

[BP15] Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing. *Phys. Rev. A*, 91:052111, May 2015. doi:10.1103/PhysRevA.91.052111.

[BQB14] Joseph Bowles, Marco Túlio Quintino, and Nicolas Brunner. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. *Phys. Rev. Lett.*, 112:140407, Apr 2014. doi:10.1103/PhysRevLett.112.140407.

[BRGP12] Cyril Branciard, Denis Rosset, Nicolas Gisin, and Stefano Pironio. Bilocal versus nonbilocal correlations in entanglement-swapping experiments. *Phys. Rev. A*, 85:032119, Mar 2012. doi:10.1103/PhysRevA.85.032119.

[BRLG13] Cyril Branciard, Denis Rosset, Yeong-Cherng Liang, and Nicolas Gisin. Measurement-device-independent entanglement witnesses for all entangled quantum states. *Phys. Rev. Lett.*, 110:060405, Feb 2013. doi:10.1103/PhysRevLett.110.060405.

[BRS+18] Jean-Daniel Bancal, Kai Redeker, Pavel Sekatski, Wenjamin Rosenfeld, and Nicolas Sangouard. Device-independent certification of an elementary quantum network link, 2018. arXiv:1812.09117.

[Bru98] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81:3018–3021, Oct 1998. doi:10.1103/PhysRevLett.81.3018.

[BRV+19] Kishor Bharti, Maharshi Ray, Antonios Varvitsiotis, Naqueeb Ahmad Warsi, Adán Cabello, and Leong-Chuan Kwek. Robust self-testing of quantum systems via noncontextuality inequalities. *Physical review letters*, 122(25):250403, 2019. doi:10.1103/PhysRevLett.122.250403.

[BŠCA18a] Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. Device-independent entanglement certification of all entangled states. *Phys. Rev. Lett.*, 121:180503, Oct 2018. doi:10.1103/PhysRevLett.121.180503.

[BŠCA18b] Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. Self-testing of Pauli observables for device-independent entanglement certification. *Phys. Rev. A*, 98:042336, Oct 2018. doi:10.1103/PhysRevA.98.042336.

[BSS18] Jean-Daniel Bancal, Nicolas Sangouard, and Pavel Sekatski. Noise-resistant device-independent certification of Bell state measurements. *Phys. Rev. Lett.*, 121:250506, Dec 2018. doi:10.1103/PhysRevLett.121.250506.

[Bus12] Francesco Buscemi. All entangled quantum states are nonlocal. *Phys. Rev. Lett.*, 108:200401, May 2012. doi:10.1103/PhysRevLett.108.200401.

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004. doi:10.1017/CBO9780511804441.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992. doi:10.1103/PhysRevLett.69.2881.

[CASA11] Daniel Cavalcanti, Mafalda L. Almeida, Valerio Scarani, and Antonio Acín. Quantum networks reveal quantum nonlocality. *Nature News*, Feb 2011. doi:10.1038/ncomms1193.

[CCBS17] Wan Cong, Yu Cai, Jean-Daniel Bancal, and Valerio Scarani. Witnessing irreducible dimension. *Phys. Rev. Lett.*, 119:080401, Aug 2017. doi:10.1103/PhysRevLett.119.080401.

[CGJV17] Andrea Coladangelo, Alex Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources, 2017. arXiv:1708.07359.

[CGL+02] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88:040404, Jan 2002. doi:10.1103/PhysRevLett.88.040404.

[CGS17] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8:15485, may 2017. doi:10.1038/ncomms15485.

[Cho75] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975. doi:10.1016/0024-3795(75)90075-0.

[CHRW11] E. G. Cavalcanti, Q. Y. He, M. D. Reid, and H. M. Wiseman. Unified criteria for multipartite quantum nonlocality. *Phys. Rev. A*, 84:032115, Sep 2011. doi:10.1103/PhysRevA.84.032115.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969. doi:10.1103/PhysRevLett.23.880.

[CK11a] André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 354–362. IEEE, 2011. doi:10.1109/FOCS.2011.42.

[CK11b] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011. doi:10.1088/1751-8113/44/9/095305.

[CK17] Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, 2017. doi:10.1017/9781316219317.

[CKS19] Tim Coopmans, Jędrzej Kaniewski, and Christian Schaffner. Robust self-testing of two-qubit states, 2019. arXiv:1902.00870.

[CLS17] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017. doi:10.1063/1.4973422.

[CM14] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. *Automata, Languages, and Programming Lecture Notes in Computer Science*, pages 320–331, 2014. doi:10.1007/978-3-662-43948-7_27.

[CN16] M. Coudron and A. Natarajan. The parallel-repeated magic square game is rigid, 2016. arXiv:1609.06306.

[Col06] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2006. arXiv:0911.3814.

[Col17] Andrea Coladangelo. Parallel self-testing of (tilted) epr pairs via copies of (tilted) chsh and the magic square game. *Quantum Info. Comput.*, 17(9-10):831–865, August 2017. URL: http://dl.acm.org/citation.cfm?id=3179561.3179567.

[Col18] Andrea Coladangelo. Generalization of the Clauser-Horne-Shimony-Holt inequality self-testing maximally entangled states of any local dimension. *Phys. Rev. A*, 98:052115, Nov 2018. doi:10.1103/PhysRevA.98.052115.

[Col20] Andrea Coladangelo. A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations. *Quantum*, 4:282, June 2020. URL: https://doi.org/10.22331/q-2020-06-18-282, doi:10.22331/q-2020-06-18-282.

[CRSV17] Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Overlapping Qubits. In Christos H. Papadimitriou, editor, *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, volume 67 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 48:1–48:21, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ITCS.2017.48.

[CRSV18] Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. *Quantum*, 2:92, September 2018. doi:10.22331/q-2018-09-03-92.

[CS17a] Daniel Cavalcanti and Paul Skrzypczyk. Quantum steering: a review with focus on semidefinite programming. *Reports on Progress in Physics*, 80(2):024001, 2017. doi:10.1088/1361-6633/80/2/024001.

[CS17b] Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games, 2017. arXiv:1709.09267.

[CS17c] Andrea Coladangelo and Jalex Stark. Separation of finite and infinite-dimensional quantum correlations, with infinite question or answer sets, 2017. arXiv:1708.06522.

[CS18] Andrea Coladangelo and Jalex Stark. Unconditional separation of finite and infinite-dimensional quantum correlations, 2018. arXiv:1804.05116.

[CY14] Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In *Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing*, STOC '14, pages 427–436, New York, NY, USA, 2014. ACM. doi:10.1145/2591796.2591873.

[DFR16] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation, 2016. arXiv:1607.01796.

[DPA13] Chirag Dhara, Giuseppe Prettico, and Antonio Acín. Maximal quantum randomness in Bell tests. *Phys. Rev. A*, 88:052116, Nov 2013. doi:10.1103/PhysRevA.88.052116.

[DPP19] Ken Dykema, Vern I. Paulsen, and Jitendra Prakash. Non-closure of the set of quantum correlations via graphs. *Communications in Mathematical Physics*, 365(3):1125–1142, Feb 2019. doi:10.1007/s00220-019-03301-1.

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991. doi:10.1103/PhysRevLett.67.661.

[ER14] Artur Ekert and Renato Renner. The ultimate physical limits of privacy. *Nature News*, Mar 2014. doi:10.1038/nature13132.

[Fad17] Matteo Fadel. Self-testing Dicke states, 2017. arXiv:1707.01215.

[FK19] Máté Farkas and J ędrzej Kaniewski. Self-testing mutually unbiased bases in the prepare-and-measure scenario. *Phys. Rev. A*, 99:032316, Mar 2019. doi:10.1103/PhysRevA.99.032316.

[GBD+18] Suchetana Goswami, Bihalan Bhattacharya, Debarshi Das, Souradeep Sasmal, C. Jebaratnam, and A. S. Majumdar. One-sided device-independent self-testing of any pure two-qubit entangled state. *Phys. Rev. A*, 98:022311, Aug 2018. doi:10.1103/PhysRevA.98.022311.

[GBG16] Mariami Gachechiladze, Costantino Budroni, and Otfried Gühne. Extreme violation of local realism in quantum hypergraph states. *Phys. Rev. Lett.*, 116:070401, Feb 2016. doi:10.1103/PhysRevLett.116.070401.

[GBS16] Koon Tong Goh, Jean-Daniel Bancal, and Valerio Scarani. Measurement-device-independent quantification of entanglement for given Hilbert space dimension. *New Journal of Physics*, 18(4):045022, apr 2016. doi:10.1088/1367-2630/18/4/045022.

[GC99] Daniel Gottesman and Isaac L Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390, 1999. doi:10.1038/46503.

[GH17] W T Gowers and O Hatami. Inverse and stability theorems for approximate representations of finite groups. *Sbornik: Mathematics*, 208(12):1784–1817, 2017. doi:10.1070/sm8872.

[Gis09] Nicolas Gisin. Bell inequalities: Many questions, a few answers. In Wayne C. Myrvold and Joy Christian, editors, *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle*, pages 125–138. Springer, 2009. doi:10.1007/978-1-4020-9107-0_9.

[GKK18] Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. Verification of quantum computation: An overview of existing approaches. *Theory of Computing Systems*, pages 1–94, 2018. doi:10.1007/s00224-018-9872-3.

[GKW15] Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. Robustness and device independence of verifiable blind quantum computing. *New Journal of Physics*, 17(8):083040, 2015. doi:10.1088/1367-2630/17/8/083040.

[GKW+18] Koon Tong Goh, Jędrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. Geometry of the set of quantum correlations. *Phys. Rev. A*, 97:022104, Feb 2018. doi:10.1103/PhysRevA.97.022104.

[GMM+19] S. Gómez, A. Mattar, I. Machuca, E. S. Gómez, D. Cavalcanti, O. Jiménez Farías, A. Acín, and G. Lima. Experimental investigation of partially entangled states for device-independent randomness generation and self-testing protocols. *Phys. Rev. A*, 99:032108, Mar 2019. doi:10.1103/PhysRevA.99.032108.

[GPL+19] Koon Tong Goh, Chithrabhanu Perumangatt, Zhi Xian Lee, Alexander Ling, and Valerio Scarani. Experimental comparison of tomography and self-testing in certifying entanglement. *Physical Review A*, 100(2):022305, 2019. doi:10.1103/PhysRevA.100.022305.

[GTHB05] Otfried Gühne, Géza Tóth, Philipp Hyllus, and Hans J. Briegel. Bell inequalities for graph states. *Phys. Rev. Lett.*, 95:120405, Sep 2005. doi:10.1103/PhysRevLett.95.120405.

[GVW+15] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015. doi:10.1103/PhysRevLett.115.250401.

[GWK17] Alexandru Gheorghiu, Petros Wallden, and Elham Kashefi. Rigidity of quantum steering and one-sided device-independent verifiable quantum computation. *New Journal of Physics*, 19(2):023043, 2017. doi:10.1088/1367-2630/aa5cff.

[Har92] Lucien Hardy. Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories. *Phys. Rev. Lett.*, 68:2981–2984, May 1992. doi:10.1103/PhysRevLett.68.2981.

[Har93] Lucien Hardy. Nonlocality for two particles without inequalities for almost all entangled states. *Phys. Rev. Lett.*, 71:1665–1668, Sep 1993. doi:10.1103/PhysRevLett.71.1665.

[HBD+15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, and et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015. doi:10.1038/nature15759.

[HH18] Masahito Hayashi and Michal Hajdušek. Self-guaranteed measurement-based quantum computation. *Phys. Rev. A*, 97:052308, May 2018. doi:10.1103/PhysRevA.97.052308.

[HKB+16] B. Hensen, N. Kalb, M. S. Blok, A. E. Dréau, A. Reiserer, R. F. L. Vermeulen, R. N. Schouten, M. Markham, D. J. Twitchen, K. Goodenough, and et al. Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis. *Scientific Reports*, 6(1), 2016. doi:10.1038/srep30289.

[HKR15] Teiko Heinosaari, Jukka Kiukas, and Daniel Reitzner. Noise robustness of the incompatibility of quantum measurements. *Phys. Rev. A*, 92:022115, Aug 2015. doi:10.1103/PhysRevA.92.022115.

[HQB+16] Flavien Hirsch, Marco Túlio Quintino, Joseph Bowles, Tamas Vértesi, and Nicolas Brunner. Entanglement without hidden nonlocality. *New Journal of Physics*, 18(11):113019, 2016. doi:10.1088/1367-2630/18/11/113019.

[HQBB13] Flavien Hirsch, Marco Túlio Quintino, Joseph Bowles, and Nicolas Brunner. Genuine hidden quantum nonlocality. *Phys. Rev. Lett.*, 111:160402, Oct 2013. doi:10.1103/PhysRevLett.111.160402.

[JHA+15] Sania Jevtic, Michael J. W. Hall, Malcolm R. Anderson, Marcin Zwierz, and Howard M. Wiseman. Einstein–Podolsky–Rosen steering and the steering ellipsoid. *J. Opt. Soc. Am. B*, 32(4):A40–A49, Apr 2015. doi:10.1364/JOSAB.32.000A40.

[JMS17] Rahul Jain, Carl A. Miller, and Yaoyun Shi. Parallel Device-Independent Quantum Key Distribution, 2017. arXiv:1703.05426.

[JMS20] Rahul Jain, Carl A Miller, and Yaoyun Shi. Parallel device-independent quantum key distribution. *IEEE Transactions on Information Theory*, 2020. doi:10.1109/TIT.2020.2986740.

[Kam33] Egbert R. Van Kampen. On some lemmas in the theory of groups. *American Journal of Mathematics*, 55(1):268–273, 1933. doi:10.2307/2371129.

[Kan16] Jędrzej Kaniewski. Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities. *Phys. Rev. Lett.*, 117:070402, Aug 2016. doi:10.1103/PhysRevLett.117.070402.

[Kan17] Jędrzej Kaniewski. Self-testing of binary observables based on commutation. *Phys. Rev. A*, 95:062323, Jun 2017. doi:10.1103/PhysRevA.95.062323.

[KCBS08] Alexander A. Klyachko, M. Ali Can, Sinem Binicioğlu, and Alexander S. Shumovsky.

Simple test for hidden variables in spin-1 systems. *Phys. Rev. Lett.*, 101:020403, Jul 2008. doi:10.1103/PhysRevLett.101.020403.

[KM18] Amir Kalev and Carl A Miller. Rigidity of the magic pentagram game. *Quantum Science and Technology*, 3(1):015002, 2018. doi:10.1088/2058-9565/aa931d.

[KMS11] Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84:012326, Jul 2011. doi:10.1103/PhysRevA.84.012326.

[Kra10] B. Kraus. Local unitary equivalence of multipartite pure states. *Phys. Rev. Lett.*, 104:020504, Jan 2010. doi:10.1103/PhysRevLett.104.020504.

[KS67] S. Kochen and E. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17(1):59–87, 1967. doi:10.1512/iumj.1968.17.17004.

[KŠT+19] Jędrzej Kaniewski, Ivan Šupić, Jordi Tura, Flavio Baccari, Alexia Salavrakos, and Remigiusz Augusiak. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. *Quantum*, 3:198, October 2019. URL: https://doi.org/10.22331/q-2019-10-24-198, doi:10.22331/q-2019-10-24-198.

[KW16] Jędrzej Kaniewski and Stephanie Wehner. Device-independent two-party cryptography secure against sequential attacks. *New Journal of Physics*, 18(5):055004, may 2016. doi:10.1088/1367-2630/18/5/055004.

[KWW12] R. Konig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, March 2012. doi:10.1109/TIT.2011.2177772.

[LC97] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997. doi:10.1103/physrevlett.78.3410.

[LCH+18] Xinhui Li, Yu Cai, Yunguang Han, Qiaoyan Wen, and Valerio Scarani. Self-testing using only marginal information. *Phys. Rev. A*, 98:052331, Nov 2018. doi:10.1103/PhysRevA.98.052331.

[LLP10] Thomas Lawson, Noah Linden, and Sandu Popescu. Biased nonlocal quantum games, 2010. arXiv:1011.6245v1.

[LLW+19] Jian Li, Tong-Jun Liu, Si Wang, C. Jebarathinam, and Qin Wang. Experimental violation of mermin steering inequality by three-photon entangled states with nontrivial ghz-fidelity. *Opt. Express*, 27(9):13559–13567, Apr 2019. doi:10.1364/OE.27.013559.

[Lov79] L. Lovasz. On the Shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25(1):1–7, January 1979. doi:10.1109/TIT.1979.1055985.

[LRZ+18] Pei-Sheng Lin, Denis Rosset, Yanbao Zhang, Jean-Daniel Bancal, and Yeong-Cherng Liang. Device-independent point estimation from finite data and its application to device-independent property estimation. *Physical Review A*, 97(3):032309, 2018. doi:10.1103/PhysRevA.97.032309.

[LSW11] Yeong-Cherng Liang, Robert W. Spekkens, and Howard M. Wiseman. Specker's parable of the overprotective seer: A road to contextuality, nonlocality and complementarity. *Physics Reports*, 506(1):1 – 39, 2011. doi:10.1016/j.physrep.2011.05.001.

[LWH+19] Xinhui Li, Yukun Wang, Yunguang Han, Sujuan Qin, Fei Gao, and Qiaoyan Wen. Analytic robustness bound for self-testing of the singlet with two binary measurements. *J. Opt. Soc. Am. B*, 36(2):457–463, Feb 2019. doi:10.1364/JOSAB.36.000457.

[Mah18] U. Mahadev. Classical verification of quantum computations. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 259–267, Oct 2018. doi:10.1109/FOCS.2018.00033.

[Mal10] Robert A. Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81:042319, Apr 2010. doi:10.1103/PhysRevA.81.042319.

[Man14] Laura Mančinska. *Maximally Entangled State in Pseudo-Telepathy Games*, pages 200–207. Springer International Publishing, Cham, 2014. doi:10.1007/978-3-319-13350-8_15.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414, 1997. doi:10.1103/PhysRevLett.78.3414.

[MBP19] Nikolai Miklin, Borkała Borkała, and Marcin Pawłowski. Self-testing of unsharp measurements, 2019. arXiv:1903.12533.

[McK10] Matthew McKague. *Quantum Information Processing with Adversarial Devices*. PhD thesis, University of Waterloo, 2010. URL: http://hdl.handle.net/10012/5259.

[McK14] Mathew McKague. Self-testing graph states. In D. Bacon, M. Martin-Delgado, and M. Roetteler, editors, *Theory of Quantum Computation, Communication, and Cryptography ,,* volume 6745 of *Lecture Notes in Computer Science*, pages 104–120. Springer, Berlin, Heidelberg, 2014. doi:https://doi.org/10.1007/978-3-642-54429-3_7.

[McK16a] Matthew McKague. Interactive proofs for BQP via self-tested graph states. *Theory of Computing*, 12(3):1–42, 2016. doi:10.4086/toc.2016.v012a003.

[McK16b] Matthew McKague. Self-testing in parallel. *New Journal of Physics*, 18:045013, 2016. doi:10.1088/1367-2630/18/4/045013.

[McK17] Matthew McKague. Self-testing in parallel with CHSH. *Quantum*, 1:1, April 2017. doi:10.22331/q-2017-04-25-1.

[MdW16] Ashley Montanaro and Ronald de Wolf. A survey of quantum property testing. *Theory of Computing Graduate Surveys*, 7, 2016. doi:10.4086/toc.gs.2016.007.

[Mer90a] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65:1838–1840, Oct 1990. doi:10.1103/PhysRevLett.65.1838.

[Mer90b] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, Dec 1990. doi:10.1103/PhysRevLett.65.3373.

[MM11] M. McKague and M. Mosca. Generalized self-testing and the security of the 6-state protocol. In W. van Dam, V. M. Kendon, and S. Severini, editors, *Theory of Quantum Computation, Communication, and Cryptography*, volume 6519 of *Lecture Notes in Computer Science*, pages 113–130. Springer, Berlin, Heidelberg, 2011. doi:10.1007/978-3-642-18073-6_10.

[MMMO06] Frédéric Magniez, Dominic Mayers, Michele Mosca, and Harold Ollivier. Self-testing of quantum circuits. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Automata, Languages and Programming*, pages 72–83, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. doi:10.1007/11786986_8.

[MP13] Mehdi Mhalla and Simon Perdrix. Graph States, Pivot Minor, and Universality of (X, Z)-measurements. *International Journal of Unconventional Computing*, 9(1-2):153–171, 2013. Special Issue: New Worlds of Computation. URL: https://hal.archives-ouvertes.fr/hal-00934104.

[MP19] Piotr Mironowicz and Marcin Pawłowski. Experimentally feasible semi-device-independent certification of four-outcome positive-operator-valued measurements. *Physical Review A*, 100(3):030301, 2019. doi:10.1103/PhysRevA.100.030301.

[MR19] Magdalena Musat and Mikael Rørdam. Non-closure of quantum correlation matrices and factorizable channels that require infinite dimensional ancilla (with an appendix by narutaka ozawa). *Communications in Mathematical Physics*, pages 1–16, 2019. doi:10.1007/s00220-019-03449-w.

[MS13] C. A. Miller and Y. Shi. Optimal robust self-testing by binary nonlocal XOR games. *Leibniz Int. Proc. Informat.*, 22(254), 2013. doi:10.4230/LIPIcs.TQC.2013.254.

[MS16] Carl A. Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM*, 63(4):33:1–33:63, October 2016. doi:10.1145/2885493.

[MT02] Dominic Mayers and Christian Tourenne. *Violation of Locality and Self-Checking Source: A Brief Account*, pages 269–276. Springer US, Boston, MA, 2002. doi:10.1007/0-306-47114-0_43.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, 1998. doi:10.1109/sfcs.1998.743501.

[MY04] D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4:273, 2004. arXiv:quant-ph/0307205.

[MYS12] M. McKague, T. H. Yang, and V. Scarani. Robust self-testing of the singlet. *Journal of Mathematical Physics*, 45(45):455304, 2012. doi:10.1088/1751-8113/45/45/455304.

[Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. *Proceedings of the 40th IEEE Symposium on Foundations of Computer Science (FOCS'99)*, page 369, 1999. doi:10.1109/SFFCS.1999.814608.

[NC18] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2018. doi:10.1017/CBO9780511976667.

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, Jan 2007. doi:10.1103/PhysRevLett.98.010401.

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008. doi:10.1088/1367-2630/10/7/073013.

[NV17] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 1003–1015, New York, NY, USA, 2017. ACM. doi:10.1145/3055399.3055468.

[NV18] A. Natarajan and T. Vidick. Low-degree testing for quantum states, and a quantum entangled games PCP for QMA. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 731–742, Oct 2018. doi:10.1109/FOCS.2018.00075.

[OV16] Dimiter Ostrev and Thomas Vidick. The structure of nearly-optimal quantum strategies for the CHSH (n) XOR games. *Quantum Information & Computation*, 16(13-14), pp.(13-14):1191–1211, 2016.

[OW10] Jonathan Oppenheim and Stephanie Wehner. The uncertainty principle determines the nonlocality of quantum mechanics. *Science*, 330(6007):1072–1074, 2010. doi:10.1126/science.1192065.

[PAB+09] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, apr 2009. doi:10.1088/1367-2630/11/4/045021.

[Pal12] Carlos Palazuelos. Superactivation of quantum nonlocality. *Phys. Rev. Lett.*, 109:190401, Nov 2012. doi:10.1103/PhysRevLett.109.190401.

[PAM+10] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzimitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010. doi:10.1038/nature09008.

[Pea70] Philip M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, Oct 1970. doi:10.1103/PhysRevD.2.1418.

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3-4):107–108, 1990. doi:10.1016/0375-9601(90)90172-k.

[PNA10] S. Pironio, M. Navascués, and A. Acín. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM Journal on Optimization*, 20(5):2157–2180, 2010. doi:10.1137/090760155.

[Pop95] Sandu Popescu. Bell's inequalities and density matrices: Revealing "hidden" nonlocality. *Phys. Rev. Lett.*, 74:2619–2622, Apr 1995. doi:10.1103/PhysRevLett.74.2619.

[PR92] Sandu Popescu and Daniel Rohrlich. Which states violate Bell's inequality maximally? *Physics Letters A*, 169(6):411 – 414, 1992. doi:https://doi.org/10.1016/0375-9601(92)90819-8.

[Pre98] John Preskill. *Quantum computation*. California Institute of Technology, 1998. URL: http://www.theory.caltech.edu/people/preskill/ph229.

[PT15] V. I. Paulsen and I. G. Todorov. Quantum chromatic numbers via operator systems. *The Quarterly Journal of Mathematics*, 66(2):677–692, Mar 2015. doi:10.1093/qmath/hav004.

[PVN14] Károly F. Pál, Tamás Vértesi, and Miguel Navascués. Device-independent tomography of multipartite quantum states. *Phys. Rev. A*, 90:042340, Oct 2014. doi:10.1103/PhysRevA.90.042340.

[RB01] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, May 2001. doi:10.1103/PhysRevLett.86.5188.

[RBB03] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68:022312, Aug 2003. doi:10.1103/PhysRevA.68.022312.

[RHBM13] M Rossi, M Huber, D Bruß, and C Macchiavello. Quantum hypergraph states. *New Journal of Physics*, 15(11):113022, nov 2013. doi:10.1088/1367-2630/15/11/113022.

[RHC+11] Rafael Rabelo, Melvyn Ho, Daniel Cavalcanti, Nicolas Brunner, and Valerio Scarani. Device-independent certification of entangled measurements. *Phys. Rev. Lett.*, 107:050502, Jul 2011. doi:10.1103/PhysRevLett.107.050502.

[RKB18] Marc Olivier Renou, Jędrzej Kaniewski, and Nicolas Brunner. Self-testing entangled measurements in quantum networks. *Phys. Rev. Lett.*, 121:250507, Dec 2018. doi:10.1103/PhysRevLett.121.250507.

[RM+18] Ravishankar Ramanathan, Dardo , Sadiq Muhammad, Piotr Mironowicz, Marcus Grünfeld, Mohamed Bourennane, and Paweł Horodecki. Steering is an essential feature of non-locality in quantum theory. *Nature Communications*, 9, 2018. doi:10.1038/s41467-018-06255-5.

[RS97] Ran Raz and Shmuel Safra. A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP. In *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97, pages 475–484, New York, NY, USA, 1997. ACM. doi:10.1145/258533.258641.

[RTK+18] Jérémy Ribeiro, Le Phuc Thinh, J ędrzej Kaniewski, Jonas Helsen, and Stephanie Wehner. Device independence for two-party cryptography and position verification with memoryless devices. *Phys. Rev. A*, 97:062307, Jun 2018. doi:10.1103/PhysRevA.97.062307.

[RUV13] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496:456, 2013. doi:10.1038/nature12035.

[RZS12] Rafael Rabelo, Law Yun Zhi, and Valerio Scarani. Device-independent bounds for Hardy's experiment. *Phys. Rev. Lett.*, 109:180401, Oct 2012. doi:10.1103/PhysRevLett.109.180401.

[ŠASA16] I Šupić, R Augusiak, A Salavrakos, and A Acín. Self-testing protocols based on the chained Bell inequalities. *New Journal of Physics*, 18(3):035013, apr 2016. doi:10.1088/1367-2630/18/3/035013.

[SAT+17] Alexia Salavrakos, Remigiusz Augusiak, Jordi Tura, Peter Wittek, Antonio Acín, and Stefano Pironio. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.*, 119:040402, Jul 2017. doi:10.1103/PhysRevLett.119.040402.

[SBWS18] Pavel Sekatski, Jean-Daniel Bancal, Sebastian Wagner, and Nicolas Sangouard. Certifying the building blocks of quantum computers from Bell's theorem. *Phys. Rev. Lett.*, 121:180505, Nov 2018. doi:10.1103/PhysRevLett.121.180505.

[SCA+11] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully distrustful quantum bit commitment and coin flipping. *Phys. Rev. Lett.*, 106:220501, Jun 2011. doi:10.1103/PhysRevLett.106.220501.

[Sca12] Valerio Scarani. The device-independent outlook on quantum physics (Lecture notes on the power of Bell's theorem). *Acta Physica Slovaca*, 62, 2012. URL: http://www.physics.sk/aps/pub.php?y=2012&pub=aps-12-04, doi:10.2478/v10155-012-0003-4.

[ŠCAA18] I Šupić, A Coladangelo, R Augusiak, and A Acín. Self-testing multipartite entangled states through projections onto two systems. *New Journal of Physics*, 20(8):083041, aug 2018. doi:10.1088/1367-2630/aad89b.

[SDSB+05] Aditi Sen De, Ujjwal Sen, Časlav Brukner, Vladimír Bužek, and Marek Żukowski. Entanglement swapping of noisy states: A kind of superadditivity in nonclassicality. *Phys. Rev. A*, 72:042310, Oct 2005. doi:10.1103/PhysRevA.72.042310.

[ŠH16] Ivan Šupić and Matty J Hoban. Self-testing through EPR-steering. *New Journal of Physics*, 18(7):075006, jul 2016. doi:10.1088/1367-2630/18/7/075006.

[Slo11] William Slofstra. Lower bounds on the entanglement needed to play XOR non-local games. *Journal of Mathematical Physics*, 52(10):102202, 2011. doi:10.1063/1.3652924.

[Slo19] William Slofstra. The set of quantum correlations is not closed. *Forum of Mathematics, Pi*, 7, 2019. doi:10.1017/fmp.2018.3.

[Slo20] William Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *Journal of the American Mathematical Society*, 33(1):1–56, 2020. doi:https://doi.org/10.1090/jams/929.

[SMN+20] Massimiliano Smania, Piotr Mironowicz, Mohamed Nawareg, Marcin Pawłowski, Adán Cabello, and Mohamed Bourennane. Experimental certification of an informationally complete quantum measurement in a device-independent protocol. *Optica*, 7(2):123–128, 2020. doi:10.1364/OPTICA.377959.

[SMSC+15] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, Dec 2015. doi:10.1103/PhysRevLett.115.250402.

[Sti55] W. Forrest Stinespring. Positive functions on C^*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–211, Jan 1955. doi:10.1090/s0002-9939-1955-0069403-4.

[SVW16] Jamie Sikora, Antonios Varvitsiotis, and Zhaohui Wei. Minimum dimension of a Hilbert space needed to generate a quantum correlation. *Phys. Rev. Lett.*, 117:060401, Aug 2016. doi:10.1103/PhysRevLett.117.060401.

[SW87] S. J. Summers and R. F. Werner. Maximal violation of Bell's inequalities is generic in quantum field theory. *Communications in Mathematical Physics*, 110(2):247–259, 1987. doi:10.1007/BF01207366.

[THMB15] Armin Tavakoli, Alley Hameedi, Breno Marques, and Mohamed Bourennane. Quantum random access codes using single d-level systems. *Phys. Rev. Lett.*, 114:170502, Apr 2015. doi:10.1103/PhysRevLett.114.170502.

[TKV+18] Armin Tavakoli, Jędrzej Kaniewski, Tamás Vértesi, Denis Rosset, and Nicolas Brunner. Self-testing quantum states and measurements in the prepare-and-measure scenario. *Phys. Rev. A*, 98:062307, Dec 2018. doi:10.1103/PhysRevA.98.062307.

[TRC19] Tassius Temistocles, Rafael Rabelo, and Marcelo Terra Cunha. Measurement compatibility in bell nonlocality tests. *Physical Review A*, 99(4):042120, 2019. doi:10.1103/PhysRevA.99.042120.

[TRR19] Armin Tavakoli, Denis Rosset, and Marc-Olivier Renou. Enabling computation of correlation bounds for finite-dimensional quantum systems via symmetrization. *Phys. Rev. Lett.*, 122:070501, Feb 2019. doi:10.1103/PhysRevLett.122.070501.

[Tsi87] B. S. Tsirelson. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36(4):557–570, Feb 1987. doi:10.1007/BF01663472.

[Tsi93] Boris Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronis Journal Supplement*, 8:329–45, 1993.

[TSV+14] J Tura, A B Sainz, T Vértesi, A Acín, M Lewenstein, and R Augusiak. Translationally invariant multipartite Bell inequalities involving only two-body correlators. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424024, oct 2014. doi:10.1088/1751-8113/47/42/424024.

[TSV+20] Armin Tavakoli, Massimiliano Smania, Tamás Vértesi, Nicolas Brunner, and Mohamed Bourennane. Self-testing nonprojective quantum measurements in prepare-and-measure experiments. *Science Advances*, 6(16):eaaw6664, 2020. doi:10.1126/sciadv.aaw6664.

[TWE+17] T. R. Tan, Y. Wan, S. Erickson, P. Bierhorst, D. Kienzler, S. Glancy, E. Knill, D. Leibfried, and D. J. Wineland. Chained Bell inequality experiment with high-efficiency measurements. *Phys. Rev. Lett.*, 118:130403, Mar 2017. doi:10.1103/PhysRevLett.118.130403.

[UCNG19] Roope Uola, Ana C. S. Costa, H. Chau Nguyen, and Otfried Gühne. Quantum Steering. *arXiv*, 2019. arXiv:1903.06663.

[vDH03] Wim van Dam and Patrick Hayden. Universal entanglement transformations without communication. *Phys. Rev. A*, 67:060302, Jun 2003. URL: https://link.aps.org/doi/10.1103/PhysRevA.67.060302, doi:10.1103/PhysRevA.67.060302.

[vDMMS07] Wim van Dam, Frédéric Magniez, Michele Mosca, and Miklos Santha. Self-testing of universal and fault-tolerant sets of quantum gates. *SIAM Journal on Computing*, 37(2):611–629, 2007. doi:10.1137/s0097539702404377.

[Vid17] Thomas Vidick. Parallel DIQKD from parallel repetition, 2017. arXiv:1703.08508.

[WBMS16] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Phys. Rev. A*, 93:062121, Jun 2016. doi:10.1103/PhysRevA.93.062121.

[WBSS18] Sebastian Wagner, Jean-Daniel Bancal, Nicolas Sangouard, and Pavel Sekatski. Device-independent characterization of generalized measurements, 2018. URL: https://arxiv.org/abs/1812.02628, arXiv:1812.02628.

[WCY+14] Xingyao Wu, Yu Cai, Tzyh Haur Yang, Huy Nguyen Le, Jean-Daniel Bancal, and Valerio Scarani. Robust self-testing of the three-qubit W–state. *Phys. Rev. A*, 90:042339, Oct 2014. doi:10.1103/PhysRevA.90.042339.

[Wer89] Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989. doi:10.1103/PhysRevA.40.4277.

[WJD07] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.*, 98:140402, Apr 2007. doi:10.1103/PhysRevLett.98.140402.

[WKB+19] Erik Woodhead, Jędrzej Kaniewski, Boris Bourdoncle, Alexia Salavrakos, Joseph Bowles, Remigiusz Augusiak, and Antonio Acín. Maximal randomness from partially entangled states, 2019. arXiv:1901.06912.

[WLP13] Erik Woodhead, Charles Ci Wen Lim, and Stefano Pironio. Semi-device-independent QKD based on BB84 and a CHSH-type estimation. In Kazuo Iwama, Yasuhito Kawano,

and Mio Murao, editors, *Theory of Quantum Computation, Communication, and Cryptography*, pages 107–115, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. doi:10.1007/978-3-642-35656-8_9.

[WPD+18] Jianwei Wang, Stefano Paesani, Yunhong Ding, Raffaele Santagati, Paul Skrzypczyk, Alexia Salavrakos, Jordi Tura, Remigiusz Augusiak, Laura Mančinska, Davide Bacco, Damien Bonneau, Joshua W. Silverstone, Qihuang Gong, Antonio Acín, Karsten Rottwitt, Leif K. Oxenløwe, Jeremy L. O'Brien, Anthony Laing, and Mark G. Thompson. Multidimensional quantum entanglement with large-scale integrated optics. *Science*, 2018. doi:10.1126/science.aar7053.

[Wu17] Xingyao Wu. *Self-testing: walking on the boundary of the quantum set*. PhD thesis, National University of Singapore, 2017. URL: http://scholarbank.nus.edu.sg/handle/10635/134729.

[WWS16] Yukun Wang, Xingyao Wu, and Valerio Scarani. All the self-testings of the singlet for two binary measurements. *New Journal of Physics*, 18(2):025021, feb 2016. doi:10.1088/1367-2630/18/2/025021.

[YN13] Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A*, 87:050102, May 2013. doi:10.1103/PhysRevA.87.050102.

[YVB+14] Tzyh Haur Yang, Tamás Vértesi, Jean-Daniel Bancal, Valerio Scarani, and Miguel Navascués. Robust and versatile black-box certification of quantum devices. *Phys. Rev. Lett.*, 113:040401, Jul 2014. doi:10.1103/PhysRevLett.113.040401.

[ZCP+18] Wen-Hao Zhang, Geng Chen, Xing-Xiang Peng, Xiang-Jun Ye, Peng Yin, Ya Xiao, Zhi-Bo Hou, Ze-Di Cheng, Yu-Chun Wu, Jin-Shi Xu, Chuan-Feng Li, and Guang-Can Guo. Experimentally robust self-testing for bipartite and tripartite entangled states. *Phys. Rev. Lett.*, 121:240402, Dec 2018. doi:10.1103/PhysRevLett.121.240402.

[ZCP+19] Wen-Hao Zhang, Geng Chen, Xing-Xiang Peng, Xiang-Jun Ye, Peng Yin, Xiao-Ye Xu, Jin-Shi Xu, Chuan-Feng Li, and Guang-Can Guo. Experimental realization of robust self-testing of Bell state measurements. *Phys. Rev. Lett.*, 122:090402, Mar 2019. doi:10.1103/PhysRevLett.122.090402.

[ZCY+19] Wen-Hao Zhang, Geng Chen, Peng Yin, Xing-Xiang Peng, Xiao-Min Hu, Zhi-Bo Hou, Zhi-Yuan Zhou, Shang Yu, Xiang-Jun Ye, Zong-Quan Zhou, and et al. Experimental demonstration of robust self-testing for bipartite entangled states. *npj Quantum Information*, 5(1), Nov 2019. doi:10.1038/s41534-018-0120-0.

[ZGZ+16] Yi-Zheng Zhen, Koon Tong Goh, Yu-Lin Zheng, Wen-Fei Cao, Xingyao Wu, Kai Chen, and Valerio Scarani. Nonlocal games and optimal steering at the boundary of the quantum set. *Phys. Rev. A*, 94:022116, Aug 2016. doi:10.1103/PhysRevA.94.022116.