New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft **DPG** **IOP** Institute of Physics

PAPER • OPEN ACCESS

Self-testing and certification using trusted quantum inputs

To cite this article: Ivan Šupi *et al* 2020 *New J. Phys.* **22** 073006

View the article online for updates and enhancements.

New Journal of Physics

The open access journal at the forefront of physics

PAPER

CrossMark

Self-testing and certification using trusted quantum inputs

Ivan Šupić[1] , **Matty J Hoban**[2] , **Laia Domingo Colomer**[3] **and Antonio Acín**[4,5]

1   Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland
2   Department of Computing, Goldsmiths, University of London, New Cross, London SE14 6NW, United Kingdom
3   Universitat Autónoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain
4   ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
5   ICREA—Institucio Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain

E-mail: ivan.supic@unige.ch

Abstract

Device-independent certification of quantum devices is of crucial importance for the development of secure quantum information protocols. So far, the most studied scenario corresponds to a system consisting of different non-characterized devices that observers probe with classical inputs to obtain classical outputs. The certification of relevant quantum properties follows from the observation of correlations between these events that do not have a classical counterpart. In the fully device-independent scenario no assumptions are made on the devices and therefore their non-classicality follows from Bell non-locality. There exist other scenarios, known as semi-device-independent, in which assumptions are made on the devices, such as their dimension, and non-classicality is associated to the observation of other types of correlations with no classical analogue. More recently, the use of trusted quantum inputs for certification has been introduced. The goal of this work is to study the power of this formalism and describe self-testing protocols in various settings using trusted quantum inputs. We also relate these different types of self-testing to some of the most basic quantum information protocols, such as quantum teleportation. Finally, we apply our findings to quantum networks and provide methods for estimating the quality of the whole network, as well as of parts of it.

1. Introduction

Quantum entanglement is at the heart of many quantum information protocols [1], such as quantum state teleportation [2], and utilised in quantum repeaters [3], which are fundamental for long-distance quantum communication. Entanglement can also result in Bell nonlocality through the correlations between measurements performed by distant parties, manifested as violations of Bell inequalities [4, 5]. Now this form of nonlocality can be a resource for tasks such as quantum key distribution [6–8], certifiable randomness expansion [9–11], delegated quantum computation [12], communication complexity [13] and measurement-based quantum computation [14, 15].

Besides being an information theoretic resource on their own, Bell inequality violations have the remarkable property of witnessing entanglement without the need to know the underlying physical system. In other words, Bell nonlocality witnesses entanglement in the *device-independent* paradigm in which devices are not characterized. But Bell inequality violations can certify more than the mere presence of entanglement and, in fact, they are also useful in the context of *quantum state certification*. In quantum state certification, a device claims to produce systems with particular quantum states, and the goal is to have a task that certifies this claim. The certification task for the source depends very much on the assumptions made in a scenario, such as whether measurement devices can be fully characterised and trusted (device-dependent) or not characterised nor trusted at all (device-independent). When it comes to the certification of a source of entangled particles in a completely device-independent manner, certification is based on correlations violating Bell inequalities and is described as *self-testing* [16]. This question has gained a lot of attention in recent years [17–21]. A notable trait of self-testing is the inability to recover the

exact form of the state, and measurements: the best one can hope is to certify them up to operations which leave the observed probability distributions invariant. Local isometries and complex conjugation are examples of such operations.

On the other side, in the device-dependent scenario where measurement devices are perfectly characterized, a lot is known, e.g. see [22–24] for recent progress in the efficient certification of quantum states. In between these two extreme cases one has different relaxations of the device-independent scenario, being sometimes coined as semi-device-independent. This term was originally introduced in [25] for the case in which an upper bound on the dimension of the systems is assumed, but we use it here to describe any scenario between the completely device-dependent and device-independent scenarios. For instance, if one assumes a perfect knowledge about one of the two devices, entanglement can be witnessed through correlations displaying Einstein–Podolsky–Rosen (EPR) steering [26, 27], which has led to the study of one-sided device-independent quantum information processing [28, 29] and quantum certification based on steering [30, 31]. Other works have also considered the problem of state certification by assuming a bound on the dimension of the involved quantum systems [32, 33].

While all these different scenarios differ in the assumptions invoked for the certification, they are all based on the statistics describing an input–output process consisting of classical inputs, labelling choices of measurements or states, and outputs, associated to measurement results. Our work goes beyond this framework and study certification protocols in which the inputs have a quantum nature. In this scenario, each party could individually generate other characterised quantum systems in a trusted way. These characterised quantum systems can then be used as quantum input into an uncharacterised device. This type of certification naturally appears in the context of semi-quantum nonlocal games [34] but also in quantum information protocols with no classical analogue such as teleportation [2]. It is also relevant in the context of device-independent quantum certification, as the characterised quantum systems could themselves have been certified separately in a device-independent manner, see for instance [35]. Our main results consist of different new self-testing protocols using quantum inputs.

2. Frameworks for quantum state certification

In this section we identify four basic frameworks for quantum state certification in a bipartite setting, corresponding to four forms of device-independence. Throughout this work, as a simplification, we will assume that in every instance the device produces identical and independently distributed (i.i.d.) copies of the same system. Additionally, in all bipartite scenarios the two parties will be referred to as Alice and Bob.

2.1. Device-dependent state certification

The first framework accounts for characterised and trusted measurement devices, which can be applied to systems generated by an untrusted and uncharacterised preparation device. State certification can be achieved by *quantum state tomography* [36]: informationally complete measurements [37] can be made on the i.i.d. copies of the quantum system. The probabilities of obtaining different measurement outcomes are used to determine the state. For example, if the source produces one-qubit states, an example of an informationally complete set of measurements are those projective measurements associated to the three Pauli operators $\{\sigma_x, \sigma_y, \sigma_z\}$. The probability to obtain outcome a when measuring xth measurement on the unknown state ϱ is given by

$$p(a|x) = \mathrm{Tr}\left(\mathsf{M}_{a|x}\varrho\right),$$

where $\mathsf{M}_{a|x}$ denotes the measurement element corresponding to the outcome a. The aim of quantum state tomography is to recover the state ϱ from a given set $\{p(a|x), \mathsf{M}_{a|x}\}_{a|x}$.

An analogous procedure can be described to characterise an unknown quantum measurement using a characterised set of quantum states. The set of quantum states is used as a probe and the probabilities of obtaining different measurement outcomes are used to recover the form of the measurement. The set of states sufficient for this process is called a tomographically complete set of states. For a qubit measurement, a tomographically complete set of states are, for example, the eigenstates of the three Pauli operators.

Performing tomography is however not necessary for quantum state certification in the device-dependent setting. For certification we merely wish to prove that *a particular* state is produced, and thus we only need to establish whether it is that state, or not. A solution to this, for a pure state, is to have a projective measurement with that state as one of its outcomes. For entangled states this might require entangled measurements, but there are other approaches not requiring such complicated measurements [22, 24].

2.2. Self-testing

The device-independent scenario is that which completely lacks a characterisation of the devices. In this case, Alice's and Bob's devices are treated as black boxes with classical inputs and classical outputs. The corresponding certification task is named self-testing [16]. The aim is to recover the entangled state $|\psi\rangle$ only from the probabilities of obtaining different outputs when certain inputs are chosen. Self-testing can only hope to recover a state able to produce a nonlocal probability distribution (see [38]), which mean s that it cannot be performed on single systems. The starting point in every self-testing procedure is the correctness of the Born rule, which allows to calculate the correlation probabilities when unknown measurements $\mathsf{M}_{a|x}$ and $\mathsf{M}_{b|y}$ are performed on the shared state ϱ':

$$p(a, b|x, y) = \mathrm{Tr}\left[\left(\mathsf{M}_{a|x} \otimes \mathsf{M}_{b|y}\right) \varrho'\right].$$

Since all conclusions are drawn from the probabilities, one cannot differentiate between physical set-ups (involving potentially different states and measurements) that give rise to the same probabilities. For instance, self-testing cannot prove that ϱ is exactly equal to $|\psi\rangle$ but it may allow one to prove that the two states are related by a suitable local isometry $\Phi = \Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}$:

$$\Phi(\varrho') = |\psi\rangle\langle\psi| \otimes \varrho_{\mathrm{junk}},$$

where ϱ_{junk} represents the state of the uncorrelated degrees of freedom.

2.3. One-sided device-independent certification

As mentioned, between these two cases there are methods for certification, known as semi-device-independent, based on assumptions on the devices but that do not require a full characterization. Next we illustrate this approach through two well known examples.

A quantum state can be certified in an asymmetric scenario: one party has characterised measurements while the other treats their devices as black boxes. This certification task is clearly between the device-dependent and the device-independent settings and thus it has been introduced as one-sided device-independent self-testing [30, 39]. Here it is possible to carry out tomography using trusted measurement devices, but with only classical inputs and outputs for the black-box devices. The part of the state belonging to the party with uncharacterised devices can be recovered only up to local isometries. Only states which do not admit a local hidden state model, i.e. steerable ones, can be self-tested in this way [28, 29].
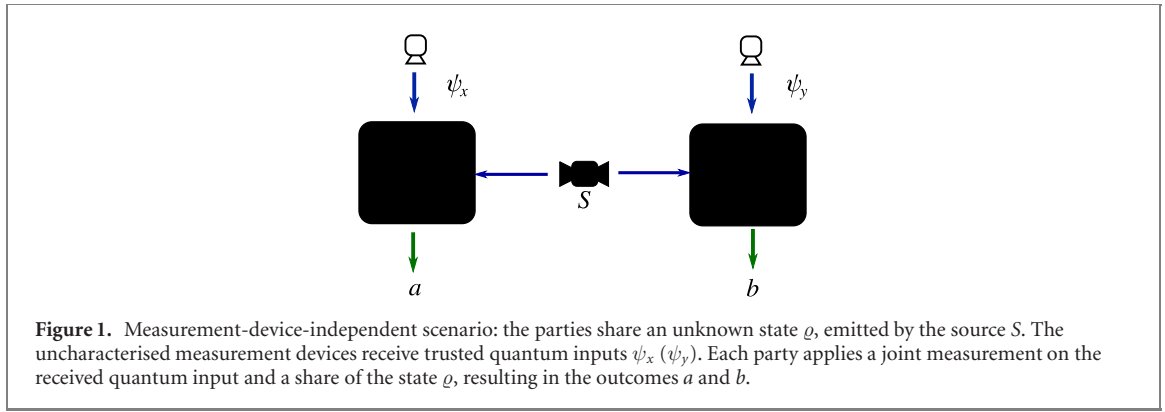
2.4. Bounded dimension self-testing

Certification protocols can be based on an assumption of the dimension of the involved systems. An advantage of this approach is that it can be applied to *prepare-and-measure* scenario [32, 33, 40]. Alice prepares systems which are subsequently measured by Bob; the task is based on communication between two parties thus making it different from the other settings certifying entangled states. The central assumption made in such settings is that the system is associated with a Hilbert space of a fixed dimension, but otherwise devices are not characterised. In [41] prepare-and-measure scenarios are used to certify properties of quantum measurements by assuming the bound on the overlap between the states Alice can prepare, instead of bounding the Hilbert state dimension.

3. Self-testing with quantum inputs

In all the previous approaches to self-testing, and independently of the assumptions on the devices, the parties feed the devices with classical information, which can label a state preparation of measurement choice, and observe an output, corresponding to a measurement result. In this work, we consider a different framework in which parties can locally prepare some characterised quantum states, which are later treated as inputs to their untrusted measurement devices. Measurement-device-independent (MDI) protocols are examples of this approach, which is becoming increasingly popular in recent years. Firstly, it has been proven that, in this scenario, all entangled states are capable of exhibiting measurement correlations which cannot be simulated with separable states [34], see also [42–44]. The same approach has been pursued in [45, 46] to clarify the role of entanglement in quantum teleportation protocols. The main goal of this work is to construct self-testing protocols in this scenario (figure 1).

Before describing self-testing with quantum inputs let us point out what kind of conclusions we can expect. Since, in this scenario, the measurement devices are not trusted along with the source of the systems, they may be associated with Hilbert spaces of arbitrary dimension. Additionally, all of the experimental observations are insensitive to a set of transformations; this is similar to the situation in

Figure 1. Measurement-device-independent scenario: the parties share an unknown state ϱ, emitted by the source *S*. The uncharacterised measurement devices receive trusted quantum inputs ψ_x (ψ_y). Each party applies a joint measurement on the received quantum input and a share of the state ϱ, resulting in the outcomes *a* and *b*.

standard self-testing protocols. So if the underlying experiment deviates from the claimed one in suitable ways as not to alter the observed statistics, these deviations cannot be determined and define an equivalence class of preparations. Any local change of basis to the states and measurements remains hidden, as well as embedding of the state in some Hilbert space of higher or lower dimension. Consequently, the best we can hope for is to find local isometries (one for Alice and one for Bob) relating the state we want to certify with the state shared by Alice and Bob. Note that one consequence of self-testing is that one can give a lower bound on the dimension of the untrusted systems. However, since arbitrary isometries leave the observed statistics invariant and isometries can increase the dimension, we cannot say what the dimension of these systems is exactly. Importantly, in this scenario, complex conjugation can be dropped from the set of undetectable state transformations. The reason for this is the full characterisation of quantum inputs, which can be chosen from a tomographically complete set of states. Thus we can distinguish the statistics produced by $|\psi\rangle$, in general, from those produced by the state $|\psi^*\rangle$. Similarly to the self-testing nomenclature we call the ideal state *reference state* and the shared state *physical state*. For the sake of simplicity, we restrict our study to protocols where in the ideal scenario parties always apply the Bell state measurement (the projector onto the Bell states of the corresponding dimension). That is, in all experiments with quantum inputs the reference measurement is the Bell state measurement, while the actual measurement the parties apply is named *physical measurement*. Of course, the formalism can in principle be generalized to other measurement settings, but we do not consider them here.

3.1. Self-testing with only quantum inputs

In this section we consider bipartite self-testing in which all parties use quantum inputs, i.e. MDI state certification. The scenario is as follows: two parties, Alice and Bob, share a quantum state ϱ'^{AB}. Each of them can perform a joint measurement on their share of the entangled state and the prepared quantum input, $\psi_x^{A'}$ for Alice and $\psi_y^{B'}$ for Bob. We are using the notation that $\psi \equiv |\psi\rangle\langle\psi|$ is the projector onto the pure state $|\psi\rangle$. Since the Hilbert spaces are unbounded in dimension, the measurements are modelled as projectors: $\{\mathsf{M}_a^{A'A}\}_a$ for Alice and $\{\mathsf{M}_b^{BB'}\}$ for Bob. Measurement outcomes are labelled with *a* for Alice and *b* for Bob (see section 1). The aim of self-testing with quantum inputs is to prove that from the observed statistics $p(a, b|\psi_x, \psi_y)$ it follows that there must exist a local isometry transforming the physical state ϱ'^{AB} into the reference one $\psi^{A''B''}$. Similarly to standard self-testing we can only hope to certify the presence of pure states. Analogously to the theorem given in [47] we can prove that the correlations of any mixed state can be achieved with a pure state of the same dimension. The proof of this theorem is presented in appendix A.
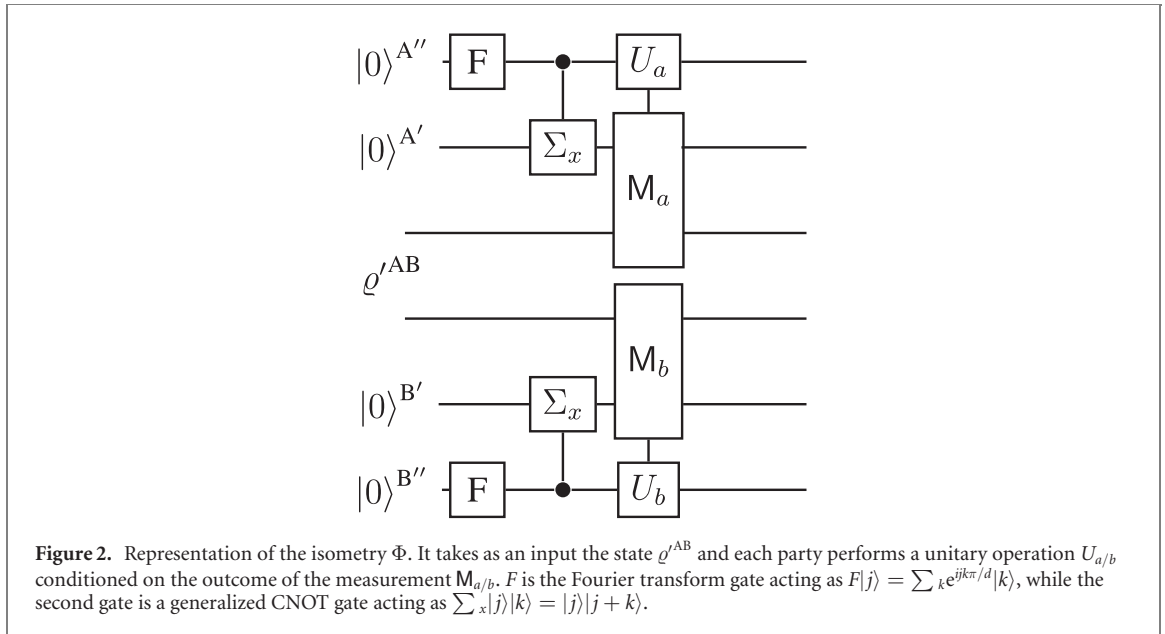
Before stating the main theorem of this section let us recall some of the specificities of the scenario when the parties can prepare tomographically complete set of inputs (for more details see [42, 43]). The observed probabilities can be written in the following way:

$$p(a, b|\psi_x, \psi_y) = \mathrm{Tr}\left[\tilde{\mathsf{M}}_{a,b}^{A'B'} \left(\psi_x^{A'} \otimes \psi_y^{B'}\right)\right],$$

where

$$\tilde{\mathsf{M}}_{a,b}^{A'B'} = \mathrm{Tr}_{AB}\left[\left(\mathsf{M}_a^{A'A} \otimes \mathsf{M}_b^{BB'}\right)\left(\mathbb{1}^{A'} \otimes \varrho'^{AB} \otimes \mathbb{1}^{B'}\right)\right] \tag{1}$$

is named the *effective measurement*. If the set of quantum input states is tomographically complete, in the sense that it is sufficient for quantum process tomography, one can recover the exact form of the effective

Figure 2. Representation of the isometry Φ. It takes as an input the state ϱ'^{AB} and each party performs a unitary operation $U_{a/b}$ conditioned on the outcome of the measurement $M_{a/b}$. F is the Fourier transform gate acting as $F|j\rangle = \sum_k e^{ijk\pi/d}|k\rangle$, while the second gate is a generalized CNOT gate acting as $\sum_x |j\rangle|k\rangle = |j\rangle|j+k\rangle$.

measurements from the observed probabilities. This insight is in the core of the proof that quantum inputs can successfully probe every entangled state [34, 42] and its analogue is the central object in the contributions to the understanding of non-classical quantum state teleportation [45, 46]. To briefly summarise, if the effective measurement is not a separable operator for every pair a, b the shared state must be entangled.

The following theorem will identify precisely how the resemblance between the effective measurement and the shared state can be used for the recovery of the state. In particular, if the effective measurements are pure and entangled the self-testing statement for the shared state can be formulated. To state the theorem, we need to introduce some notation. The d-dimensional generalized Z and X operators are defined as $Z = \sum_{j=0}^{d-1} \omega^j |j\rangle\langle j|$ and $X = \sum_{j=0}^{d-1} |j + 1 \bmod d\rangle\langle j|$, respectively, where $\omega = \exp 2\pi i/d$. These matrices can be used to define an orthonormal basis of qudit Bell states $|\phi_{kl}\rangle = X^k Z^l |\phi^+\rangle$, where $|\phi^+\rangle = \sum_{j=0}^{d-1} |jj\rangle$. As Alice's and Bob's reference measurements are $\{|\phi_{kl}\rangle\langle\phi_{kl}|\}$ their outputs a and b are comprised of two dits k and l.

Theorem 1. *Let two parties, Alice and Bob, share the state ϱ'^{AB} and have access to a tomographically complete set of inputs $\{\psi_x\}_x$ and $\{\psi_y\}_y$ respectively. Each party performs a joint measurement on their share of ϱ'^{AB} and quantum input ψ_x or ψ_y. If the correlation probabilities can be written in the form*

$$p\left(a, b|\psi_x, \psi_y\right) = \mathrm{Tr}\left[\tilde{M}_{a,b}^{A'B'}\left(\psi_x^{A'} \otimes \psi_y^{B'}\right)\right], \quad \forall a, b, x, y;$$
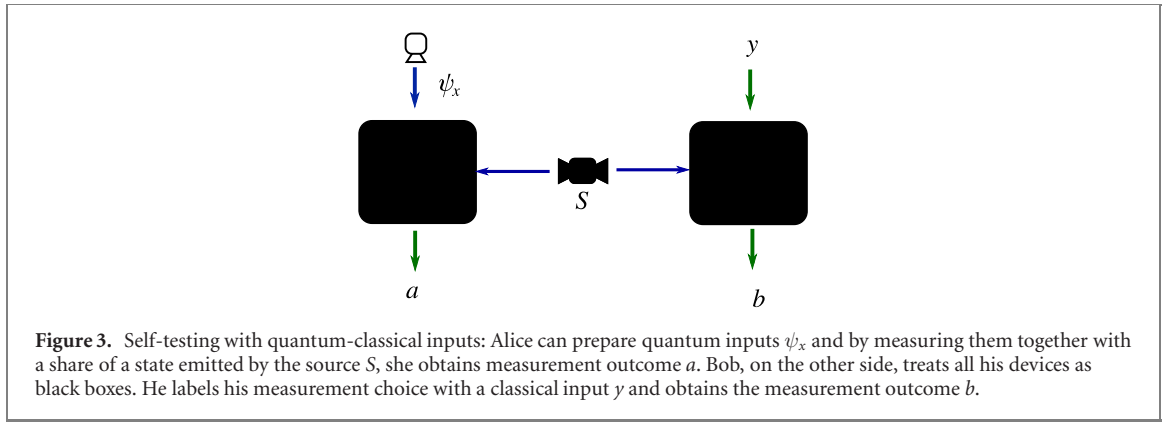
and $\tilde{M}_{a,b}^{A'B'}$ are such that

$$\frac{1}{d^2}|\psi\rangle\langle\psi| = (U_a \otimes U_b)(\tilde{M}_{a,b}^{A'B'})^{\mathrm{T}}(U_a^\dagger \otimes U_b^\dagger) \quad \forall a, b, \tag{2}$$

where U_a and U_b are the correcting unitaries defined as $U_m = \sum_{kl} X^k Z^l \delta_{m,kl}$, then there exists a local isometry Φ such that

$$\Phi(\varrho'^{AB}) = |\psi\rangle\langle\psi|^{A''B''} \otimes \varrho_{\mathrm{junk}}^{AA'BB'}. \tag{3}$$

The proof of the theorem is given in appendix B. Here we explicitly show the isometry which is used to prove the theorem. The isometry is given in figure 2. It implicitly assumes that the measurement operators are projective. Since the dimension of the shared state is not assumed, the Naimark extension can be used: if the measurements $\{M_a\}$, $\{M_b\}$ are not projective one can always increase the dimension of the registers A, B and see the measurements as projective on a higher dimensional system.

The true power of quantum inputs is exhibited when one is interested in the robustness of the self-testing procedure. The standard task of robust self-testing can be phrased as follows: if the conditions for self-testing are approximately met can we still say something about the distance between $\Phi(\varrho)$ and ψ? When the set of quantum inputs is tomographically complete the state of the registers A″ and B″ of the isometry on figure 2 can be recovered even if the conditions for the ideal self-testing (2) are not satisfied. In that case the fidelity between $\mathrm{tr}_{AA'BB'}\Phi(\varrho^{AB})$ and the reference state $|\psi\rangle$ can be directly estimated.

Figure 3. Self-testing with quantum-classical inputs: Alice can prepare quantum inputs ψ_x and by measuring them together with a share of a state emitted by the source *S*, she obtains measurement outcome *a*. Bob, on the other side, treats all his devices as black boxes. He labels his measurement choice with a classical input *y* and obtains the measurement outcome *b*.

Furthermore, if the parties used exactly the Bell state measurement the physical state will be exactly mapped to the state of registers A″ and B″, allowing to obtain the tight bound on the fidelity between $\mathrm{tr}_{\mathrm{AA'BB'}}\Phi(\varrho^{\mathrm{AB}})$ and $|\psi\rangle$. A noisy Bell state measurement will give only a lower bound on the fidelity. For example, if the noisy Bell state measurements of the form $\mathsf{M}'_i = 0.95 B_i + 0.05\mathbb{1}/4$, where $\{B_i\}_i$ is the ideal Bell state measurement, is applied on the state $\varrho = \phi^+$, the recovered fidelity between $\mathrm{tr}_{\mathrm{AA'BB'}}\Phi(\varrho^{\mathrm{AB}})$ and ϕ^+ will be 0.893.

Note that the ability to prepare quantum inputs is strictly more than what one can do in a device-independent scenario. Thus, one would expect that whenever there is a standard device-independent self-test for a state $|\psi\rangle$, it can be also performed with quantum inputs. The idea is simple: if some projectors are used to produce measurement correlations which are self-testing the state $|\psi\rangle$, they can be effectively prepared by performing a Bell state measurement and a suitable input. An example of adapting the self-test from the CHSH inequality to the scenario with quantum inputs is provided in appendix D.

The similar overall reasoning about self-testing with only quantum inputs can be applied to every multipartite entangled state. The more detailed discussion is given in appendix C. Here we just state the corollary:

Corollary 2. *Self-testing with quantum inputs can recover any pure genuinely multipartite entangled state.*

3.2. Self-testing with quantum-classical inputs
In this section we consider a hybrid scenario in which one party, say Alice, uses quantum inputs, while the other one, Bob, uses classical inputs (see figure 3). Let us consider the following scenario: Alice and Bob share a state ϱ'^{AB}. Alice can prepare quantum inputs $\{\psi_x^{\mathrm{A'}}, \bar{\psi}_x^{\mathrm{A'}}\}_x$, where $\bar{\psi}_x = \mathbb{1} - \psi_x$, and apply a joint measurement $\{\mathsf{M}_a^{\mathrm{A'A}}\}_a$, while Bob queries his device with classical input *y*, which corresponds to applying a projective measurement $\{\mathsf{M}_{b|y}\}_b$. In this scenario the probability to obtain outcomes *a* and *b*, when Alice's quantum input is ψ_x and Bob's classical input is *y* is

$$p(a,b|\psi_x, y) = \mathrm{Tr}\left[\left(\mathsf{M}_a^{\mathrm{A'A}} \otimes \mathsf{M}_{b|y}^{\mathrm{B}}\right)\left(\psi_x^{\mathrm{A'}} \otimes \varrho'^{\mathrm{AB}}\right)\right]. \tag{4}$$

For each classical input *y* we can define the effective measurements

$$\tilde{\mathsf{M}}_{a,b|y}^{\mathrm{A'}} = \mathrm{Tr}_{\mathrm{AB}}\left[\left(\mathsf{M}_a^{\mathrm{A'A}} \otimes \mathsf{M}_{b|y}^{\mathrm{B}}\right)\left(\mathbb{1}^{\mathrm{A'}} \otimes \varrho'^{\mathrm{AB}}\right)\right]. \tag{5}$$

Now we are ready to state the theorem which self-tests the state $|\phi^+\rangle$ from a Bell-like expression. Let $\mathscr{I}_{\mathrm{qc}}$ be defined in the following way:

$$\mathscr{I}_{\mathrm{qc}} = \sum_{a=0,1}(p(a,0|\psi_0, 0) + p(a,1|\bar{\psi}_0, 0)) + \sum_{a=2,3}(p(a,1|\psi_0, 0) + p(a,0|\bar{\psi}_0, 0))$$

$$+ \sum_{a=0,2}(p(a,0|\psi_1, 1) + p(a,0|\bar{\psi}_1, 1)) + \sum_{a=1,3}(p(a,1|\psi_1, 1) + p(a,0|\bar{\psi}_1, 1)). \tag{6}$$

The algebraic maximum of $\mathscr{I}_{\mathrm{qc}}$ is equal to 4. We show that there exist quantum inputs for which the only way to achieve the algebraic maximum is to share a maximally entangled pair of qubits.

Theorem 3. *Let two parties, Alice and Bob, share a state ϱ'^{AB}. Furthermore, let Alice use quantum inputs $\psi_0 = |0\rangle\langle 0|$, $\bar{\psi}_0 = |1\rangle\langle 1|$, $\psi_1 = |+\rangle\langle +|$ and $\bar{\psi}_1 = |-\rangle\langle -|$. If they observe $\mathscr{I}_{\mathrm{qc}} = 4$ where $\mathscr{I}_{\mathrm{qc}}$ is defined in (6)*

Figure 4. Representation of the local isometry Φ_{qc}. It takes as an input the state ϱ'^{AB} and resembled the standard SWAP isometry. The systems A_1' and A_2' can be discarded at the end of the process.

Figure 5. Quantum state teleportation: Alice applies a global measurement on the state ψ_x and her share of the state emitted by the source S. Bob can apply quantum state tomography and learn exactly his reduced state $\varphi_{a|x}$.

then there exists a local isometry Φ such that

$$\Phi_{qc}(\varrho'^{AB}) = |\phi^+\rangle\langle\phi^+| \otimes \varrho_{\text{junk}}. \tag{7}$$

The detailed proof is given in appendix E. Here we give the intuition for the proof. The main insight comes from the observation that the algebraic maximum of $\mathscr{I}_{qc}$ implies that the effective measurements (5) can be exactly recovered. Once they are recovered, one can use methods from standard and one-sided-device independent self-testing to prove that a convenient isometry transforms ϱ'^{AB} into ϕ^+. The isometry is explicitly given in figure 4. Operators $\mathbb{M}_{\mathbb{z}}$ and $\mathbb{M}_{\mathbb{x}}$ are given as

$$\mathbb{M}_{\mathbb{z}} = \mathsf{M}_0 + \mathsf{M}_1 - \mathsf{M}_2 - \mathsf{M}_3;$$
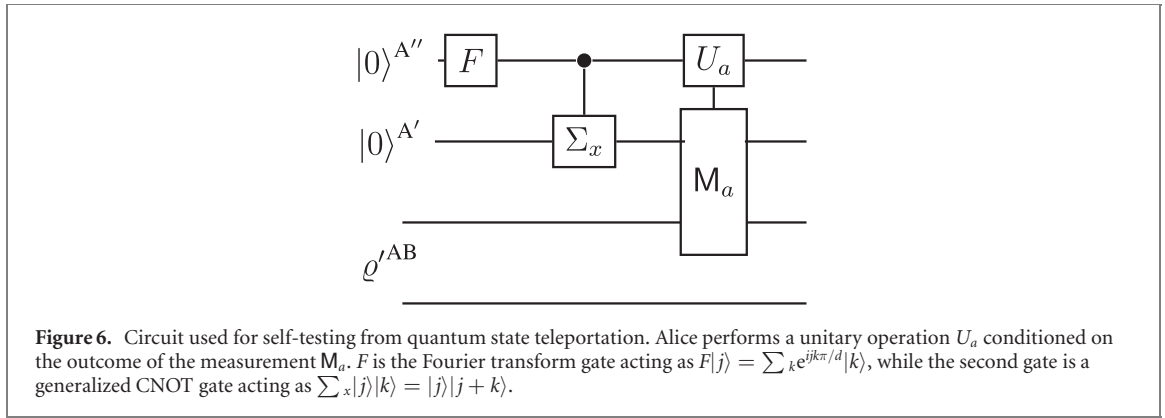$$\mathbb{M}_{\mathbb{x}} = \mathsf{M}_0 - \mathsf{M}_1 + \mathsf{M}_2 - \mathsf{M}_3.$$

4. Basic quantum information protocols as self-tests

So far we have introduced self-testing in two different semi-device-independent scenarios. In this section we show that, besides being natural extensions of standard self-testing, the introduced protocols have a practical importance in relating self-testing to some of the most widely used quantum information protocols. In section 4.1 we discuss how quantum state teleportation can be viewed as a self-test, while in section 4.2 we show how one can certify the set of states composing a quantum repeater or a quantum network (figure 5).

4.1. Quantum state teleportation as a self-test

As noted in [45], quantum state teleportation can be seen as a representative of one-sided-measurement-device-independent protocols. Indeed, Alice uses a quantum input, performs a joint measurement, while Bob performs quantum state tomography and learns his reduced state. Note that in the spirit of [45] we do not involve the part of the protocol in which Alice communicates the outcome of her measurement to Bob and he applies the correcting unitary. The correcting unitary can

Figure 6. Circuit used for self-testing from quantum state teleportation. Alice performs a unitary operation U_a conditioned on the outcome of the measurement M_a. F is the Fourier transform gate acting as $F|j\rangle = \sum_k e^{ijk\pi/d}|k\rangle$, while the second gate is a generalized CNOT gate acting as $\sum_x |j\rangle|k\rangle = |j\rangle|j+k\rangle$.

alternatively be applied by a verifier which supervises the teleportation experiment. The subnormalized reduced state of Bob $\varphi_{a|x}$ is obtained through the following expression

$$\varphi_{a|x} = \mathrm{Tr}_{A'A}\left[\left(\mathsf{M}_a^{A'A} \otimes \mathbb{1}^B\right)\left(\psi_x^{A'} \otimes \varrho'^{AB}\right)\right], \tag{8}$$

where $\psi_x^{A'}$ is a quantum input, i.e. a state to be teleported, $\mathsf{M}_a^{A'A}$ is the measurement Alice applies, while ϱ'^{AB} is the state shared between Alice and Bob (see section 5).

The success of a teleportation experiment is usually assessed from an average teleportation fidelity, defined as

$$\bar{F}_{\mathrm{tel}} = \frac{1}{|x|}\sum_{a,x}\{\langle\psi_x|U_a\varphi_{a|x}U_a^\dagger|\psi_x\rangle,$$

where $|x|$ is the total number of input. It was proven in [48] that in case the input states are tomographically complete, the state having Bell state fidelity $F_s(\varrho^{AB}) = \langle\phi^+|\varrho^{AB}|\phi^+\rangle$ leads to the average teleportation fidelity of $(F_s(\varrho^{AB})d + 1)/(d + 1)$, where d is the dimension of the states to be teleported. This can be seen also as a self-testing statement: the observed average teleportation fidelity $\bar{F}_{\mathrm{tel}}$ gives a lower bound to the Bell state fidelity F_s. However, it is obtained under assumption that the shared state is of dimension d^2. Here we show how to estimate a lower bound to the Bell state fidelity of the state shared between Alice and Bob from an arbitrary teleportation experiment, including the case when the set of input states is not tomographically complete.

As explained in [45] a teleportation experiment can be characterized by the effective teleportation measurement

$$\tilde{\mathsf{M}}_a^{A'B} = \mathrm{Tr}_A\left[\left(\mathsf{M}_a^{A'A} \otimes \mathbb{1}^B\right)\left(\mathbb{1}^{A'} \otimes \varrho'^{AB}\right)\right].$$

This is clearly tightly related to the effective measurement of equation (1), but now in this new scenario. If the set of input states is tomographically complete, $\tilde{\mathsf{M}}_a^{A'B}$ can be recovered exactly from the set of teleported states $\varphi_{a|x}$. Otherwise, a teleportation experiment is characterized by the set of effective teleportation measurements compatible with the relation

$$\varphi_{a|x}^B = \mathrm{Tr}_{A'}\left[\tilde{\mathsf{M}}_a\left(\psi_x^{A'} \otimes \mathbb{1}^B\right)\right].$$

Let us consider an arbitrary set of bipartite operators $\tilde{\mathsf{N}}_a^{A'B}$ that have a positive partial transposition and satisfy the no-signalling condition

$$\sum_a \tilde{\mathsf{N}}_a^{A'B} = \mathbb{1} \otimes \varrho_r, \quad \forall a,$$

where ρ_r is a valid quantum state. If, furthermore $\sum_a \varphi_{a|x} = \rho_r$, the $\{\tilde{N}_a^{A'B}\}$ are valid effective teleportation measurements [46, 49] for a teleportation experiment characterized by Bob's reduced states $\{\varphi_{a|x}\}$.

Observe now the quantum circuit on figure 6. Let us denote the output of the circuit as $\psi_o^{A''A'AB}$. In case ϱ'^{AB} is maximally entangled and $\{\mathsf{M}_a\}$ is the Bell state measurement, the state $\varrho_o = \mathrm{Tr}_{AA'}\psi_o$ is pure and maximally entangled. In fact, since the given quantum circuit is a valid isometry the fidelity between ϱ_o and $|\phi^+\rangle$ lower bounds the fidelity between ϱ'^{AB} and $|\phi^+\rangle$. Since there is no proof that the circuit we use is
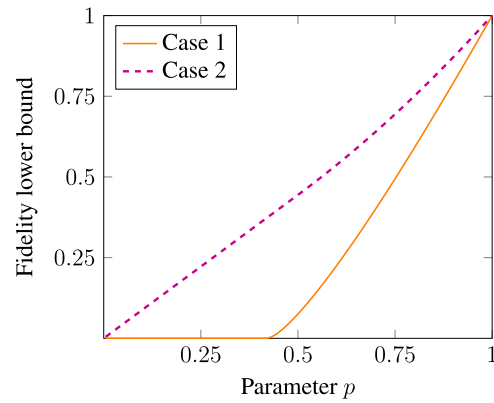
Figure 7. Alice and Bob share the qutrit–qutrit state $\rho = p|\phi^+\rangle\langle\phi^+| + (1-p)\mathbb{1}/9$. In case 1 the set of input states is $\{|0\rangle, |1\rangle, (|0\rangle + |1\rangle + |2\rangle)/\sqrt{3}, (|0\rangle + w|1\rangle + w^*|2\rangle))/\sqrt{3}\}$, while in the case 2 the set of input states is $\{|0\rangle, |1\rangle, (|0\rangle + |1\rangle + |2\rangle)/\sqrt{3}, (|0\rangle + w|1\rangle + w^*|2\rangle))/\sqrt{3}, (|0\rangle + |1\rangle + w|2\rangle)/\sqrt{3}, (w|0\rangle + |1\rangle + |2\rangle)/\sqrt{3}\}$, where $w = \exp i2\pi/3$. The graph shows the lower bounds derived from the knowledge of the whole set of teleported states on the self-tested fidelity with the maximally entangled pair of qutrits as a function of the parameter p. In none of two cases the set of input states is tomographically complete, hence no conclusion about the fidelity of the shared state with maximally entangled pair of qutrits can be drawn from the observed average teleportation fidelity.

the optimal isometry, the optimal fidelity might only be higher. In principle, when the set $\{\psi_x\}_x$ is not tomographically complete we cannot know exactly ϱ_o. However, since

$$\varrho_o = \frac{1}{d}\sum_a U_a^{A''} \tilde{\mathsf{M}}_a^{\mathrm{T}_{A''}} U_a^{\dagger A''}$$

we can optimize over all effective teleportation measurements compatible with the observed teleportation data.
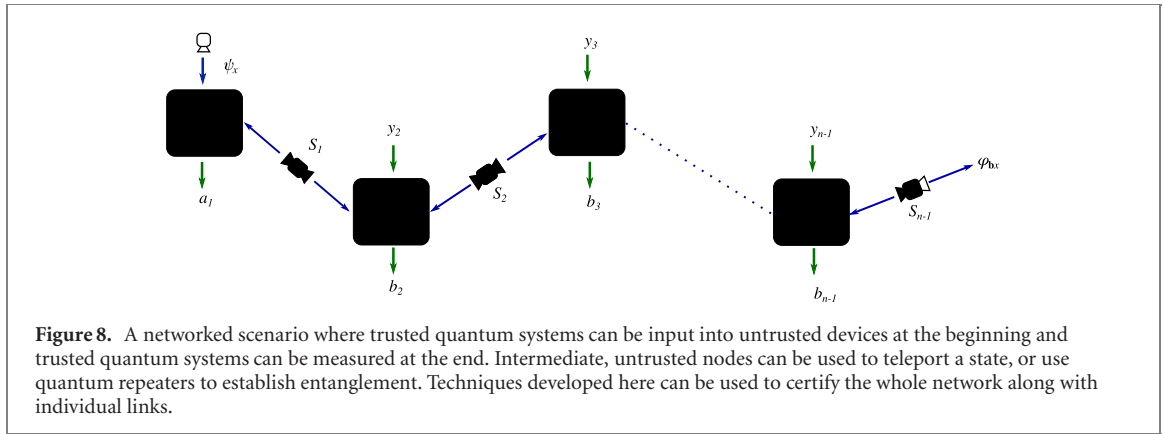
Thus, the lower bound on the fidelity between the physical state and $|\phi^+\rangle$ can be obtained as a solution to the following semi-definite programming (SDP) optimization:

$$\min \quad \frac{1}{d}\sum_a \langle\phi^+| U_a^{A'} \tilde{\mathsf{M}}_a^{\mathrm{T}_{A'}} U_a^{\dagger A'} |\phi^+\rangle$$

$$\text{s.t} \quad \varphi_{a|x} = \mathrm{Tr}_{A'}\left[\tilde{\mathsf{M}}_a^{A'B}(\psi_x^{A'} \otimes \mathbb{1}^B)\right] \quad \forall a, x, \tag{9}$$

$$\tilde{\mathsf{M}}_a^{\mathrm{T}_{A'}} \geqslant 0, \quad \forall a, \quad \sum_a \tilde{\mathsf{M}}_a = \mathbb{1} \otimes \sum_a \varphi_{a|x}, \quad \forall x.$$

The SDP (9) provides a lower bound on the fidelity between the physical state and $|\phi^+\rangle$ from the full observed data in a teleportation experiment. In principle the knowledge of the whole set of teleported states $\{\varphi_{a|x}\}_{a,x}$ is not necessary. One can fix some of the known teleportation quantifiers, such as average teleportation fidelity, teleportation weight or one of the teleportation robustness measures introduced in [46]. In figure 7 we solve the SDP in (9) for two cases without a tomographically complete set of states, two situations where the average teleportation fidelity cannot be used.

4.2. Self-testing of quantum networks

Equipped with the methods presented in the previous sections, we are in position to provide ways of self-testing elements of a quantum network. Complementary to the results about self-testing Bell state measurements [50, 51], we provide means to self-test different links of potentially hybrid quantum network. Consider a network in the form of a quantum repeater, like the one on figure 8. All measurement devices, except the first and the last, have a classical input whose choice corresponds to a Bell state measurement on the two particles or measuring one of the particles shared with one of the neighbours. One might extend our method for self-testing from teleportation and find out how well the whole quantum repeater simulates a single maximally entangled state. If the fidelity is not satisfactory, it is possible to check separate links of the network. For example, the 'quality' of the source S_1 can be estimated by using the self-testing with quantum-classical inputs (section 3.2). Self-testing through EPR steering [30] can be used to self-test source S_{n-1}. Standard self-testing protocols can be used to self-test all the remaining sources.

Figure 8. A networked scenario where trusted quantum systems can be input into untrusted devices at the beginning and trusted quantum systems can be measured at the end. Intermediate, untrusted nodes can be used to teleport a state, or use quantum repeaters to establish entanglement. Techniques developed here can be used to certify the whole network along with individual links.

5. Discussion

In this work we have expanded quantum state certification to novel scenarios using quantum inputs. Developing a hybrid approach between full device-independent and device-dependent self-testing is one of the main motivations of this work, with applications to quantum networks where some nodes in the network are trusted, and others are not. The tools developed here in the MDI setting could also find an application in a networked device-independent setting using the ideas developed in [35].

This approach also finds an application of recent work in the study of non-classical teleportation introduced by [45]. In particular, we have developed new numerical tools to relate quantum teleportation to the fidelity of the quantum states shared by the parties. Given the ubiquity of teleportation in quantum information processing, these tools could be used in the verification of teleportation-based quantum computing.

A natural question is how our scheme compares to the standard, fully device-independent, self-testing procedures. One advantage coming from our work is that we can show that all pure, multi-partite entangled states can be certified in the scenario with trusted quantum inputs. This is currently not known to be possible in the device-independent setting. Straightforwardly, our scenario requires more trusted resources, namely the preparation devices. This gave us a new set of general tools to certify quantum states without having to derive a particular Bell inequality, which is often the approach in device-independent self-testing. An important question is if we can obtain an improved robustness to noise and experimental imperfections. To answer such question one would need to develop appropriate analytical and/or numerical techniques. One direction for future research is exploring the set of quantum correlations in different scenarios with quantum inputs. This would open the doors for numerical self-testing, similar to the SWAP method from [52, 53] or the numerical self-test presented in our section 4.1. Another interesting question is to search better isometries for self-testing than those considered in this work. Finding a good isometry is crucial for obtaining better noise-resistant self-testing protocols. In turn, this could make self-testing more applicable and practical.

Note added

While finishing this manuscript we became aware of a similar work [54].

Acknowledgments

Appendix A. Remark about mixed states

Here we provide a proof that the correlations with quantum inputs obtained by measuring any mixed state can be obtained by using a pure state of the same local dimensions. It is analogous to the proof from [47].

Proof. Suppose that $\{p(a, b|\psi_x, \psi_y) = \text{Tr}((\mathsf{M}_a^{\text{A}'\text{A}} \otimes \mathsf{M}_b^{\text{BB}'}) \cdot \psi_x \otimes \varrho'^{\text{AB}} \otimes \psi_y)\}$ are generated by a mixed state ϱ'^{AB} acting on $\mathcal{H}_\text{A} \otimes \mathcal{H}_\text{B}$. Without loss of generality we consider the case $d_\text{A} \leqslant d_\text{B}$. Let $|\tilde{\phi}\rangle \in \mathcal{H}_\text{A} \otimes \mathcal{H}_\text{B} \otimes \mathcal{H}_\text{P}$ be the purification of ϱ'^{AB}, and let $|\tilde{\phi}\rangle = \sum_{i=1}^{d_A} \lambda_i |a_\text{A}^i\rangle |b_{\text{BP}}^i\rangle$ be its Schmidt decomposition, where $|a_\text{A}^i\rangle \in \mathcal{H}_\text{A}$ and $|b_{\text{BP}}^i\rangle \in \mathcal{H}_\text{B} \otimes \mathcal{H}_\text{P}$. Define the isometry $V = \sum_{i=1}^{d_A} |i_\text{B}\rangle\langle b_{\text{BP}}^i|$ from $\mathcal{H}_\text{B} \otimes \mathcal{H}_\text{P}$ to $\mathcal{H}_\text{B}$. Note that $|\phi\rangle = (\mathbb{1} \otimes V)|\tilde{\phi}\rangle = \sum_{i=1}^{d_A} \lambda_i |a_\text{A}^i\rangle |i_\text{B}\rangle \in \mathcal{H}_\text{A} \otimes \mathcal{H}_\text{B}$. One can see that the operators $\{\bar{\mathsf{M}}_b^{\text{BB}'} \otimes \mathbb{1}^\text{P} = (V \otimes \mathbb{1}^{\text{B}'})(\mathsf{M}_b^{\text{BB}'} \otimes \mathbb{1}^\text{P})(V^\dagger \otimes \mathbb{1}^{\text{B}'})\}$ define a projective measurement acting on BB'. Finally,

$$\text{Tr}((\mathsf{M}_a^{\text{A}'\text{A}} \otimes \mathsf{M}_b^{\text{BB}'})(\psi_x^{\text{A}'} \otimes \varrho'^{\text{AB}} \otimes \psi_y^{\text{B}'}) = \langle\psi_x| \otimes \langle\phi| \otimes \langle\psi_y|(\mathsf{M}_a^{\text{A}'\text{A}} \otimes \bar{\mathsf{M}}_b^{\text{BB}'})|\psi_x\rangle \otimes |\phi\rangle \otimes |\psi_y\rangle.$$

$\square$

Appendix B. Proof of theorem B1

For the sake of convenience, we repeat theorem B1 here.

Theorem B1. *Let two parties, Alice and Bob, share the state ϱ'^{AB} and have access to a tomographically complete set of inputs $\{\psi_x\}_x$ and $\{\psi_y\}_y$ respectively. Each party performs a joint measurement on their share of ϱ'^{AB} and quantum input ψ_x or ψ_y. If the correlation probabilities can be written in the form*

$$p(a, b|\psi_x, \psi_y) = \text{Tr}\left[\tilde{\mathsf{M}}_{a,b}^{\text{A}'\text{B}'}\left(\psi_x^{\text{A}'} \otimes \psi_y^{\text{B}'}\right)\right], \quad \forall a, b, x, y; \tag{B1}$$

and $\tilde{\mathsf{M}}_{a,b}^{\text{A}'\text{B}'}$ are such that

$$\frac{1}{d^2}|\psi\rangle\langle\psi| = (U_a \otimes U_b)(\tilde{\mathsf{M}}_{a,b}^{\text{A}'\text{B}'})^\text{T}(U_a^\dagger \otimes U_b^\dagger) \quad \forall a, b, \tag{B2}$$

where U_a and U_b are the correcting unitaries defined as $U_m = \sum_{kl} X^k Z^l \delta_{m,kl}$, then there exists a local isometry Φ such that

$$\Phi(\varrho'^{\text{AB}}) = |\psi\rangle\langle\psi|^{\text{A}''\text{B}''} \otimes \varrho_{\text{junk}}^{\text{AA}'\text{BB}'}. \tag{B3}$$

Since the set of quantum inputs is tomographically complete equation (B1) imply that all effective measurements defined as

$$\tilde{\mathsf{M}}_{a,b} = \text{Tr}_{\text{AB}}\left[\left(\mathsf{M}_a^{\text{A}'\text{A}} \otimes \mathsf{M}_b^{\text{BB}'}\right)\left(\mathbb{1}^{\text{A}'} \otimes \varrho^{\text{AB}} \otimes \mathbb{1}^{\text{B}'}\right)\right]$$

are proportional to rank-one projective operators satisfying constraints (B2). Consider the isometry shown in figure 2 (in the main text). Applying Φ to ϱ'^{AB} leads to

$$\Phi(\varrho'^{\text{AB}}) = \left(\sum_{a,b} U_a^{\text{A}''} \otimes \mathsf{M}_a^{\text{A}'\text{A}} \otimes \mathsf{M}_b^{\text{BB}'} \otimes U_b^{\text{B}''}\right) \cdot \left(C_{\Sigma_x}^{\text{A}''\text{A}'} \cdot \left(F^{\text{A}''} \otimes \mathbb{1}^{\text{A}'}\right) \otimes C_{\Sigma_x}^{\text{B}''\text{B}'} \cdot \left(\mathbb{1}^{\text{B}'} \otimes F^{\text{B}''}\right)\right)$$

$$\times \left(|00\rangle\langle00|^{\text{A}'\text{A}''} \otimes \varrho'^{\text{AB}} \otimes |00\rangle\langle00|^{\text{B}'\text{B}''}\right) \cdot \left(\left(F^{\dagger\text{A}''} \otimes \mathbb{1}^{\text{A}'}\right) \cdot C_{\Sigma_x}^{\dagger\ \text{A}''\text{A}'} \otimes \left(\mathbb{1}^{\text{B}'} \otimes F^{\dagger\text{B}''}\right) \cdot C_{\Sigma_x}^{\dagger\ \text{B}''\text{B}'}\right)$$

$$\times \left(\sum_{a',b'} U_{a'}^{\dagger\text{A}''} \otimes \mathsf{M}_{a'}^{\dagger\text{A}'\text{A}} \otimes \mathsf{M}_{b'}^{\dagger\text{BB}'} \otimes U_{b'}^{\dagger\text{B}''}\right)$$

$$= \sum_{a,b,a',b'} \left(U_a^{\text{A}''} \otimes \mathsf{M}_a^{\text{A}'\text{A}} \otimes \mathsf{M}_b^{\text{BB}'} \otimes U_b^{\text{B}''}\right) \cdot \left(\phi^{+\text{A}'\text{A}''} \otimes \varrho'^{\text{AB}} \otimes \phi^{+\text{B}'\text{B}''}\right)$$

$$\times \left(U_{a'}^{\dagger\text{A}''} \otimes \mathsf{M}_{a'}^{\dagger\text{A}'\text{A}} \otimes \mathsf{M}_{b'}^{\dagger\text{B}'\text{B}} \otimes U_{b'}^{\dagger\text{B}''}\right), \tag{B4}$$

where $C_{\Sigma_x} = \sum_{j,k=0}^{d-1} |j\rangle\langle j| \otimes |k + j \bmod d\rangle\langle k|$ is the generalised CNOT gate, $\phi^+ = |\phi^+\rangle\langle\phi^+|$, and $|\phi^+\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|jj\rangle$ is the maximally entangled state. Now we can trace out AA'BB' and see if the resulting state is pure.

$$\mathrm{Tr}_{\mathrm{AA'BB'}}\left[\sum_{a,b,a',b'}\left(U_a^{\mathrm{A''}}\otimes\mathsf{M}_a^{\mathrm{A'A}}\otimes\mathsf{M}_b^{\mathrm{BB'}}\otimes U_b^{\mathrm{B''}}\right)\left(\phi^{+\mathrm{A'A''}}\otimes\varrho'^{\mathrm{AB}}\otimes\phi^{+\mathrm{B'B''}}\right)\left(U_{a'}^{\dagger\mathrm{A''}}\otimes\mathsf{M}_{a'}^{\dagger\mathrm{A'A}}\otimes\mathsf{M}_{b'}^{\dagger\mathrm{BB'}}\otimes U_{b'}^{\dagger\mathrm{B''}}\right)\right]$$

$$=\sum_{a,b,a',b'}\left(U_a^{\mathrm{A''}}\otimes U_b^{\mathrm{B''}}\right)\mathrm{tr}_{\mathrm{A'ABB'}}\left[\left(\mathbb{1}^{\mathrm{A''}}\otimes\mathsf{M}_a^{\mathrm{A'A}}\otimes\mathsf{M}_b^{\mathrm{BB'}}\otimes\mathbb{1}^{\mathrm{B''}}\right)\left(\phi^{+\mathrm{A''A'}}\otimes\varrho'^{\mathrm{AB}}\otimes\phi^{+\mathrm{B'B''}}\right)\right.$$

$$\left.\times\left(\mathbb{1}^{\mathrm{A''}}\otimes\mathsf{M}_{a'}^{\dagger\mathrm{A'A}}\otimes\mathsf{M}_{b'}^{\dagger\mathrm{BB'}}\otimes\mathbb{1}^{\mathrm{B''}}\right)\right]\left(U_{a'}^{\dagger\mathrm{A''}}\otimes U_{b'}^{\dagger\mathrm{B''}}\right)$$

$$=\sum_{a,b,a',b'}(U_a^{\mathrm{A''}}\otimes U_b^{\mathrm{B''}})\mathrm{tr}_{\mathrm{A'ABB'}}\left[\left(\mathbb{1}^{\mathrm{A''}}\otimes\mathsf{M}_{a'}^{\dagger\mathrm{AA'}}\mathsf{M}_a^{\mathrm{AA'}}\otimes\mathsf{M}_{b'}^{\dagger\mathrm{BB'}}\mathsf{M}_b^{\mathrm{BB'}}\otimes\mathbb{1}^{\mathrm{B''}}\right)\right.$$

$$\left.\times\left(\phi^{+\mathrm{A''A'}}\otimes\varrho'^{\mathrm{AB}}\otimes\phi^{+\mathrm{B'B''}}\right)\right](U_{a'}^{\dagger\mathrm{A''}}\otimes U_{b'}^{\dagger\mathrm{B''}})$$

$$=\sum_{a,b,a',b'}\delta_{aa'}\delta_{bb'}(U_a^{\mathrm{A''}}\otimes U_b^{\mathrm{B''}})\mathrm{tr}_{\mathrm{A'ABB'}}\left[\left(\mathbb{1}^{\mathrm{A''}}\otimes\mathsf{M}_a^{\mathrm{A'A}}\otimes\mathsf{M}_b^{\mathrm{BB'}}\otimes\mathbb{1}^{\mathrm{B''}}\right)\right.$$

$$\left.\times\left(\phi^{+\mathrm{A''A'}}\otimes\varrho'^{\mathrm{AB}}\otimes\phi^{+\mathrm{B'B''}}\right)\right](U_{a'}^{\dagger\mathrm{A''}}\otimes U_{b'}^{\dagger\mathrm{B''}})$$

$$=\sum_{a,b,a',b'}(U_a^{\mathrm{A''}}\otimes U_b^{\mathrm{B''}})\mathrm{tr}_{\mathrm{A'ABB'}}\left[\left(\mathbb{1}^{\mathrm{A''}}\otimes\mathsf{M}_a^{\mathrm{A'A}}\otimes\mathsf{M}_b^{\mathrm{BB'}}\otimes\mathbb{1}^{\mathrm{B''}}\right)\left(\phi^{+\mathrm{A''A'}}\otimes\varrho'^{\mathrm{AB}}\otimes\phi^{+\mathrm{B'B''}}\right)\right](U_a^{\dagger\mathrm{A''}}\otimes U_b^{\dagger\mathrm{B''}})$$

$$=\frac{1}{d^2}\sum_{a,b}(U_a^{\mathrm{A''}}\otimes U_b^{\mathrm{B''}})\mathrm{tr}_{\mathrm{AB}}\left[\left(\left(\mathsf{M}_a^{\mathrm{A''A}}\right)^{T_{\mathrm{A''}}}\otimes\left(\mathsf{M}_b^{\mathrm{B''B}}\right)^{T_{\mathrm{B''}}}\right)\left(\mathbb{1}^{\mathrm{A''}}\otimes\varrho'^{\mathrm{AB}}\otimes\mathbb{1}^{\mathrm{B''}}\right)\right](U_a^{\dagger\mathrm{A''}}\otimes U_b^{\dagger\mathrm{B''}})$$

$$=\frac{1}{d^2}\sum_{a,b}(U_a^{\mathrm{A''}}\otimes U_b^{\mathrm{B''}})\tilde{\mathsf{M}}_{ab}^T(U_a^{\dagger\mathrm{A''}}\otimes U_b^{\dagger\mathrm{B''}}),\tag{B5}$$

where $\tilde{\mathsf{M}}_{ab}$ are the effective measurements. To get the second equality we used the cyclic property of the trace. The orthonormality of the projection operators is used to obtain the third equality. The fifth equality is a consequence of the identity

$$\mathrm{Tr}_{\mathrm{B}}\left[\left(\mathsf{M}^{\mathrm{AB}}\otimes\mathbb{1}^{\mathrm{C}}\right)\left(\mathbb{1}^{\mathrm{A}}\otimes\phi^{+\mathrm{BC}}\right)\right]=\frac{1}{d}\left(\mathsf{M}^{\mathrm{AC}}\right)^{T_{\mathrm{C}}}\tag{B6}$$

and equation (B5) just uses the definition of the effective measurement. Finally one can obtain

$$\mathrm{Tr}_{\mathrm{AA'BB'}}\left(\Phi(\varrho'^{\mathrm{AB}})\right)=\frac{1}{d^2}\sum_{a,b}\frac{1}{d^2}|\psi^{\mathrm{AB}}\rangle\langle\psi^{\mathrm{AB}}|\tag{B7}$$

$$=d^4\frac{1}{d^4}|\psi^{\mathrm{AB}}\rangle\langle\psi^{\mathrm{AB}}|\tag{B8}$$

where the first equality follows directly from the constraint (B2), while the second follows from (B2) and takes into account that there are d^2 different values of a and d^2 different values of b, which counts d^4 elements in the sum in (B7). Thus, $\mathrm{Tr}_{\mathrm{AA'BB'}}\left(\Phi(\varrho'^{\mathrm{AB}})\right)$ is a pure, normalised state. We conclude that there is no entanglement between AA′BB′ and A″B″. Therefore, we can write
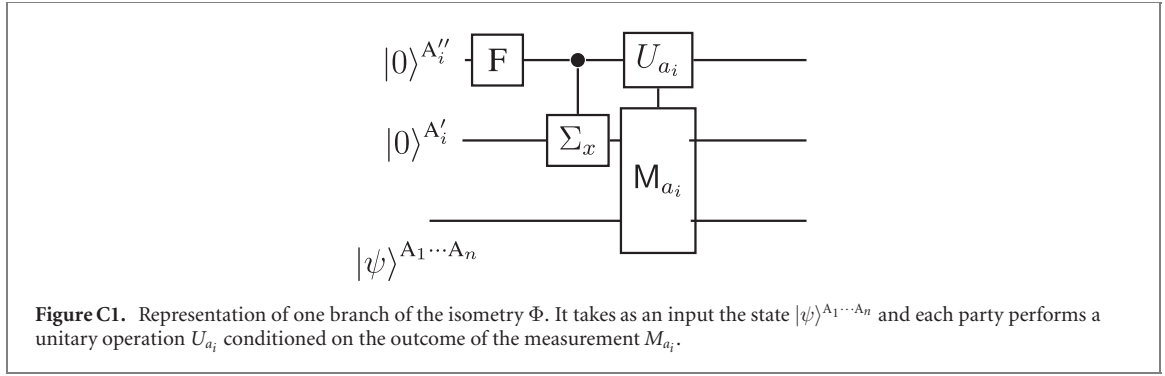
$$\Phi(\varrho'^{\mathrm{AB}})=|\psi^{\mathrm{A''B''}}\rangle\langle\psi^{\mathrm{A''B''}}|\otimes\varrho_{\mathrm{junk}}^{\mathrm{A'ABB'}}.$$

Appendix C. Self-testing of multipartite states

The bipartite result is straightforwardly generalized to the multipartite case. Before stating the theorem let us define the scenario. There are n parties (denoted by $\mathrm{A}_1,\dots,\mathrm{A}_n$) and they share the state $\varrho'^{\mathrm{A}_1\dots\mathrm{A}_n}$. Each of the parties can prepare a set of quantum inputs $\{\psi_{x_i}\}_i$, performs a joint measurement $\{\mathsf{M}_{a'_i}^{\mathrm{A}_i}\}$ on the quantum input and its share of the state $\varrho'^{\mathrm{A}_1\dots\mathrm{A}_n}$ and returns the output a_i.

Theorem C1. *Let n parties share the state $\varrho'^{\mathrm{A}_1\dots\mathrm{A}_n}$ and each of them has access to a tomographically complete set of inputs $\{\psi_{x_i}\}_{x_i}$ for $i=1,\dots,n$. Let the correlation probabilities obtained by measurements performed by each party have the form*

$$p(a_1,\dots,a_n|\psi_{x_1},\dots,\psi_{x_n})=\mathrm{Tr}\left[\tilde{\mathsf{M}}_{a_1,\dots,a_n}\left(\psi_{x_1}\otimes\cdots\otimes\psi_{x_n}\right)\right],\tag{C1}$$

Figure C1. Representation of one branch of the isometry Φ. It takes as an input the state $|\psi\rangle^{A_1\cdots A_n}$ and each party performs a unitary operation U_{a_i} conditioned on the outcome of the measurement M_{a_i}.

for every x_i. $\tilde{M}_{a_1,\ldots,a_n}$ are rank-one positive operators such that

$$\tilde{M} \equiv (U_{a_1} \otimes \cdots \otimes U_{a_n})\tilde{M}_{a_1,\ldots,a_n}{}^{\mathrm{T}}(U_{a_1}^\dagger \otimes \cdots \otimes U_{a_n}^\dagger) \tag{C2}$$

for every a_i, where U_{a_i} is the correcting unitaries generating the Bell state basis. Moreover, let

$$\tilde{M} = \frac{1}{d^n}|\psi^{A_1\ldots A_n}\rangle\langle\psi^{A_1\ldots A_n}| \tag{C3}$$

with d^n being the dimension of the whole space of the n systems. Then there exists a local isometry Φ such that

$$\Phi(\varrho'^{A_1\ldots A_n}) = |\psi^{A_1\ldots A_n}\rangle\langle\psi^{A_1\ldots A_n}| \otimes \varrho_{\mathrm{junk}}. \qquad \square$$

Proof. The isometry used in the proof is just the multipartite generalization used in the bipartite case (see figure C1)

Just as before

$$\Phi(\varrho'^{A_1\ldots A_n}) = \sum_{a_i,a_i'}(U_{a_1}^{A_1''} \otimes \cdots \otimes U_{a_n}^{A_n''} \otimes M_{a_1}^{A_1 A_1'} \otimes \cdots \otimes M_{a_n}^{A_n A_n'})$$

$$(\Phi^{+A_1'A_1''} \otimes \cdots \otimes \Phi^{+A_n'A_n''} \otimes \varrho'^{A_1\ldots A_n})(U_{a_i'}^{\dagger A_1''} \otimes \cdots \otimes U_{a_n'}^{\dagger A_n''} \otimes M_{a_1'}^{\dagger A_1 A_1'} \otimes \cdots \otimes M_{a_n'}^{\dagger A_n A_n'}).$$

Tracing over $A_1, A_1', \ldots, A_n, A_n'$ we obtain

$$\mathrm{tr}_{A_1,A_1',\ldots,A_n,A_n'}\left(\Phi\left(\varrho'^{A_1\ldots A_n}\right)\right) = \frac{1}{d^n}\sum_{a_i}(U_{a_1}^{A_1''} \otimes \cdots \otimes U_{a_n}^{A_n''})\tilde{M}_{a_1,\ldots,a_n}^T(U_{a_1}^{\dagger A_1''} \otimes \cdots \otimes U_{a_n}^{\dagger A_n''}), \tag{C4}$$

where $\tilde{M}_{a_1,\ldots,a_n}$ are the effective measurements satisfying constraints (C1)–(C3). Since every party has access to a tomographically complete set of quantum input states, (C3) is the only solution for $\tilde{M}$. Finally,

$$\mathrm{tr}_{A_1,A_1',\ldots,A_n,A_n'}\Phi(\varrho'^{A_1,\ldots,A_n}) = \sum_{a_1,\ldots,a_n}\frac{1}{d^n}\tilde{M} \tag{C5}$$

$$= d^{2n}\frac{1}{d^n}\frac{1}{d^n}|\psi^{A_1\ldots A_n}\rangle\langle\psi^{A_1\ldots A_n}|, \tag{C6}$$

where the first equality comes from (C4) and (C2), while the second is a direct consequence of (C3). Since $\mathrm{tr}_{A_1,A_1',\ldots,A_n,A_n'}\Phi(\varrho'^{A_1,\ldots,A_n})$ is a normalised pure state $\Phi(\varrho^{A_1,\ldots,A_n})$ can be written as

$$\Phi(\varrho'^{A_1,\ldots,A_n}) = |\psi^{A_1\ldots A_n}\rangle\langle\psi^{A_1\ldots A_n}| \otimes \varrho_{\mathrm{junk}}.$$

$$\square$$

Appendix D. Self-testing of maximally entangled pair of qubits through CHSH inequality

We already placed self-testing with quantum inputs in between quantum state tomography and standard self-testing. Self-testing with a tomographically complete set of quantum inputs was in spirit close to quantum state tomography (being based on the exact recovery of the effective measurement operators).

One can ask if the approach closer to standard self-testing can be used for MDI recovery of quantum states. The idea is simple: if a set of projectors is used to produce measurement correlations that self-test a given state $|\psi\rangle$, they can be obtained by performing a Bell state measurement and preparing suitable inputs. For example

$$|0\rangle\langle 0|^{\mathrm{A}} = \mathrm{tr}_{\mathrm{A}'}\left[\left(|0\rangle\langle 0|^{\mathrm{A}'}\otimes\mathbb{1}^{\mathrm{A}}\right)(\phi^{+\mathrm{A}'\mathrm{A}}+\phi^{-\mathrm{A}'\mathrm{A}})\right],$$

and

$$|1\rangle\langle 1|^{\mathrm{A}} = \mathrm{tr}_{\mathrm{A}'}\left[\left(|0\rangle\langle 0|^{\mathrm{A}'}\otimes\mathbb{1}^{\mathrm{A}}\right)(\psi^{+\mathrm{A}'\mathrm{A}}+\psi^{-\mathrm{A}'\mathrm{A}})\right].$$

Knowing this property the question is if the self-testing correlation probabilities obtained in a scenario with quantum inputs still self-test the state and moreover, if they self-test the Bell state measurement. Intuitively, the answer should be positive, since self-testing correlations can be obtained only if specific measurements are applied to a specific state. The formalization of this intuition for the case of the two-qubit maximally entangled state is given in the following theorem. For the sake of simplicity let us self-test the following form of the state

$$|\psi\rangle = \cos\left(\frac{\pi}{8}\right)|\phi^+\rangle + \sin\left(\frac{\pi}{8}\right)|\psi^+\rangle, \tag{D1}$$

since it is locally unitarilly equivalent to $|\phi^+\rangle$, but both parties apply Pauli measurements to maximally violate CHSH inequality.

Theorem D1. *Let two parties, Alice and Bob, share the state ϱ'^{AB} and let both Alice and Bob have access to the set of quantum inputs $\{\psi_0 = |0\rangle, \psi_1 = |+\rangle\}$. Alice and Bob apply a four-outcome measurement $\{M_a^{\mathrm{A}'\mathrm{A}}\}_a$ and $\{M_b^{\mathrm{B}'\mathrm{B}}\}_b$, respectively. Furthermore, let the following correlations hold*

$$\langle\psi'|A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1|\psi'\rangle = 2\sqrt{2}, \tag{D2}$$

where

$$X_0 = X_0^+ - X_0^-; \quad X_1 = X_1^+ - X_1^-;$$

$$X_0^+ = \mathrm{tr}_{X'}\left[\left(\psi_0^{X'}\otimes\mathbb{1}^X\right)\left(\mathsf{M}_0^{X'X}+\mathsf{M}_1^{X'X}\right)\right]$$

$$X_0^- = \mathrm{tr}_{X'}\left[\left(\psi_0^{X'}\otimes\mathbb{1}^X\right)\left(\mathsf{M}_2^{X'X}+\mathsf{M}_3^{X'X}\right)\right]$$

$$X_1^+ = \mathrm{tr}_{X'}\left[\left(\psi_1^{X'}\otimes\mathbb{1}^X\right)\left(\mathsf{M}_0^{X'X}+\mathsf{M}_2^{X'X}\right)\right]$$

$$X_1^- = \mathrm{tr}_{X'}\left[\left(\psi_1^{X'}\otimes\mathbb{1}^X\right)\left(\mathsf{M}_1^{X'X}+\mathsf{M}_3^{X'X}\right)\right]$$

where $X \in \{A, B\}$. Then there is a local isometry Φ such that

$$\Phi(\varrho'^{\mathrm{AB}}) = \phi^+ \otimes \varrho_{\mathrm{junk}}. \tag{D3}$$

This theorem represents the analogue of the self-testing of maximally entangled pair of qubits via the maximal violation of the CHSH (Clauser–Horn–Shimony–Holt) inequality.

Proof. Let us first verify that $\{A_j^+, A_j^-\}$ for $j = 0, 1$ represent valid measurements. Positivity is ensured by the relation

$$\langle\xi|A_0^+|\xi\rangle = \mathrm{tr}\left[\left(\psi_0^{\mathrm{A}'}\otimes\xi^{\mathrm{A}}\right)\left(\mathsf{M}_0^{\mathrm{A}'\mathrm{A}}+\mathsf{M}_1^{\mathrm{A}'\mathrm{A}}\right)\right] \geqslant 0, \quad \forall\xi \geqslant 0,$$

and similarly for the other operators $A_j^\pm$. The completeness relation is also satisfied:

$$A_j^+ + A_j^- = \mathrm{tr}_{\mathrm{A}'}\left[\left(\psi_j^{\mathrm{A}'}\otimes\mathbb{1}^{\mathrm{A}}\right)\left(\sum_k \mathsf{M}_k^{\mathrm{A}'\mathrm{A}}\right)\right]$$

$$= \mathrm{tr}_{\mathrm{A}'}\left[\left(\psi_j^{\mathrm{A}'}\otimes\mathbb{1}^{\mathrm{A}}\right)\mathbb{1}^{\mathrm{A}'\mathrm{A}}\right] = \mathbb{1}^{\mathrm{A}}.$$

In an analogue way one can prove that B_j are valid measurement observables. This is basically enough to prove the self-testing theorem, since we have that the two parties use valid quantum measurements to maximally violate the CHSH inequality. This means that there must exist a local isometry mapping the state ϱ' to the maximally entangled pair of qubits.   □

Appendix E. Proof of theorem E1

Let us, for convenience, first restate the theorem here.

Theorem E1. *Let two parties, Alice and Bob, share a state ϱ'^{AB}. Furthermore, let Alice use quantum inputs $\psi_0 = |0\rangle\langle 0|, \bar{\psi}_0 = |1\rangle\langle 1|, \psi_1 = |+\rangle\langle +| $ and $\bar{\psi}_1 = |-\rangle\langle -|$. If they observe $\mathscr{I}_{qc} = 4$ where $\mathscr{I}_{qc}$ is defined as*

$$\mathscr{I}_{qc} = \sum_{a=0,1} (p(a,0|\psi_0,0) + p(a,1|\bar{\psi}_0,0)) + \sum_{a=2,3} (p(a,1|\psi_0,0) + p(a,0|\bar{\psi}_0,0))$$

$$+ \sum_{a=0,2} (p(a,0|\psi_1,1) + p(a,0|\bar{\psi}_1,1)) + \sum_{a=1,3} (p(a,1|\psi_1,1) + p(a,0|\bar{\psi}_1,1)) \tag{E1}$$

then there exists a local isometry Φ such that

$$\Phi_{qc}(\varrho'^{AB}) = |\phi^+\rangle\langle\phi^+| \otimes \varrho_{junk}. \tag{E2}$$

Note that the expression $\mathscr{I}_{qc}$ can be seen as a sum of four terms, each of them being itself a sum to obtain few particular outcomes for certain quantum and classical inputs. The fact that everything sums up to 4 means that each term must be equal to 1, i.e.:

$$p(0,0|\psi_0,0) + p(1,0|\psi_0,0) + p(2,1|\psi_0,0) + p(3,1|\psi_0,0) = 1,$$
$$p(0,1|\bar{\psi}_0,0) + p(1,1|\bar{\psi}_0,0) + p(2,0|\bar{\psi}_0,0) + p(3,0|\bar{\psi}_0,0) = 1,$$
$$p(0,0|\psi_1,1) + p(2,0|\psi_1,1) + p(1,1|\psi_1,1) + p(3,1|\psi_1,1) = 1, \tag{E3}$$
$$p(0,1|\bar{\psi}_1,1) + p(2,1|\bar{\psi}_1,1) + p(1,0|\bar{\psi}_1,1) + p(3,0|\bar{\psi}_1,1) = 1.$$

Since we fix $|\psi_0\rangle = |0\rangle, |\bar{\psi}_0\rangle = |1\rangle, |\psi_1\rangle = |+\rangle$ and $|\bar{\psi}_1\rangle = |-\rangle$ equation (E3) imply

$$\tilde{M}_{0,0|0} + \tilde{M}_{1,0|0} + \tilde{M}_{2,1|0} + \tilde{M}_{3,1|0} = |0\rangle\langle 0|,$$
$$\tilde{M}_{2,0|0} + \tilde{M}_{3,0|0} + \tilde{M}_{0,1|0} + \tilde{M}_{1,1|0} = |1\rangle\langle 1|,$$
$$\tilde{M}_{0,0|1} + \tilde{M}_{2,0|1} + \tilde{M}_{1,1|1} + \tilde{M}_{3,1|1} = |+\rangle\langle +|, \tag{E4}$$
$$\tilde{M}_{1,0|1} + \tilde{M}_{3,0|1} + \tilde{M}_{0,1|1} + \tilde{M}_{2,1|1} = |-\rangle\langle -|,$$

where

$$\tilde{M}_{a,b|y}^{A'} = \mathrm{Tr}_{AB}\left[\left(M_a^{A'A} \otimes M_b^B\right)\left(\mathbb{1}^{A'} \otimes \varrho^{AB}\right)\right].$$

Since all the operators $\tilde{M}_{a,b|y}$ are positive, they all must be proportional to the corresponding projector ($\tilde{M}_{0,0|0}$ to $|0\rangle\langle 0|, \tilde{M}_{0,1|0}$ to $|1\rangle\langle 1|$ and so on). The no-signalling condition, expressed as

$$\sum_b \tilde{M}_{a,b|0} = \sum_b \tilde{M}_{a,b|1}, \tag{E5}$$

for all values of a imposes certain constraints on the traces of the effective measurements. Denote

$$\tilde{M}_{a,0|0} = \mu_{a,0}|0\rangle\langle 0|, \quad \text{for} \quad a = 0,1 \quad \tilde{M}_{a,0|0} = \mu_{a,0}|1\rangle\langle 1|, \quad \text{for} \quad a = 2,3$$
$$\tilde{M}_{a,1|0} = \mu_{a,1}|0\rangle\langle 0| \quad \text{for} \quad a = 2,3 \quad \tilde{M}_{a,1|0} = \mu_{a,1}|1\rangle\langle 1| \quad \text{for} \quad a = 0,1$$
$$\tilde{M}_{a,0|1} = \nu_{a,0}|+\rangle\langle +|, \quad \text{for} \quad a = 0,2 \quad \tilde{M}_{a,0|1} = \nu_{a,0}|-\rangle\langle -|, \quad \text{for} \quad a = 1,3$$
$$\tilde{M}_{a,1|1} = \nu_{a,1}|+\rangle\langle +| \quad \text{for} \quad a = 1,3 \quad \tilde{M}_{a,1|1} = \nu_{a,1}|-\rangle\langle -| \quad \text{for} \quad a = 0,2.$$

The condition (E5) imposes $\nu_{a,0} = \nu_{a,1} = \mu_{a,0} = \mu_{a,1}$ for all a. By plugging this in equation (E4) we obtain:

$$\mu_{0,0} + \mu_{1,0} + \mu_{2,0} + \mu_{3,0} = 1. \tag{E6}$$

Another no-signalling condition

$$\sum_a \tilde{M}_{a,b|0} = \sum_a \tilde{M}_{a,b|1}, \tag{E7}$$

gives

$$(\mu_{0,0} + \mu_{1,0})|0\rangle\langle 0| + (\mu_{2,0} + \mu_{3,0})|1\rangle\langle 1| = (\mu_{0,0} + \mu_{2,0})|+\rangle\langle +| + (\mu_{1,0} + \mu_{3,0})|-\rangle\langle -| \tag{E8}$$

which implies $\mu_{a,0} = 0.25$ for all a.

The above given conditions imply correctness of the following expressions

$$\text{Tr}_{AB}\left[\left((\mathsf{M}_0 + U_1\mathsf{M}_1 U_1^\dagger + U_2\mathsf{M}_2 U_2^\dagger + U_3\mathsf{M}_3 U_3^\dagger)^{A'A} \otimes \mathsf{M}_{0|0}^B\right)\left(\frac{\mathbb{1}^{A'}}{2} \otimes \varrho'^{AB}\right)\right] = \frac{1}{2}|0\rangle\langle 0|,$$

$$\text{Tr}_{AB}\left[\left((\mathsf{M}_0 + U_1\mathsf{M}_1 U_1^\dagger + U_2\mathsf{M}_2 U_2^\dagger + U_3\mathsf{M}_3 U_3^\dagger)^{A'A} \otimes \mathsf{M}_{1|0}^B\right)\left(\frac{\mathbb{1}^{A'}}{2} \otimes \varrho'^{AB}\right)\right] = \frac{1}{2}|1\rangle\langle 1|,$$

$$\text{Tr}_{AB}\left[\left((\mathsf{M}_0 + U_1\mathsf{M}_1 U_1^\dagger + U_2\mathsf{M}_2 U_2^\dagger + U_3\mathsf{M}_3 U_3^\dagger)^{A'A} \otimes \mathsf{M}_{0|1}^B\right)\left(\frac{\mathbb{1}^{A'}}{2} \otimes \varrho'^{AB}\right)\right] = \frac{1}{2}|+\rangle\langle +|,$$

$$\text{Tr}_{AB}\left[\left((\mathsf{M}_0 + U_1\mathsf{M}_1 U_1^\dagger + U_2\mathsf{M}_2 U_2^\dagger + U_3\mathsf{M}_3 U_3^\dagger)^{A'A} \otimes \mathsf{M}_{1|1}^B\right)\left(\frac{\mathbb{1}^{A'}}{2} \otimes \varrho'^{AB}\right)\right] = \frac{1}{2}|-\rangle\langle -|,$$

(E9)

where $U_1 = \sigma_z^{A'} \otimes \mathbb{1}^A$, $U_2 = \sigma_x^{A'} \otimes \mathbb{1}^A$ and $U_3 = (\sigma_z\sigma_x)^{A'} \otimes \mathbb{1}^A$. These, further, can be rewritten as

$$\text{tr}_B\left[\left(\mathbb{1}^{A'} \otimes \mathsf{M}_{0|0}^B\right)\tilde{\varrho}^{A'B}\right] = \frac{1}{2}|0\rangle\langle 0|, \qquad \text{tr}_B\left[\left(\mathbb{1}^{A'} \otimes \mathsf{M}_{1|0}^B\right)\tilde{\varrho}^{A'B}\right] = \frac{1}{2}|1\rangle\langle 1|,$$

$$\text{tr}_B\left[\left(\mathbb{1}^{A'} \otimes \mathsf{M}_{0|1}^B\right)\tilde{\varrho}^{A'B}\right] = \frac{1}{2}|+\rangle\langle +|, \qquad \text{tr}_B\left[\left(\mathbb{1}^{A'} \otimes \mathsf{M}_{1|1}^B\right)\tilde{\varrho}^{A'B}\right] = \frac{1}{2}|-\rangle\langle -|,$$

(E10)

where

$$\tilde{\varrho}^{A'B} = \text{tr}_A\left[\left((\mathsf{M}_0 + U_1\mathsf{M}_1 U_1^\dagger + U_2\mathsf{M}_2 U_2^\dagger + U_3\mathsf{M}_3 U_3^\dagger)^{A'A} \otimes \mathbb{1}^B\right)\left(\frac{\mathbb{1}^{A'}}{2} \otimes \varrho'^{AB}\right)\right].$$

Equation (E10) imply

$$\text{tr}\left[(\sigma_z^{A'} \otimes B_0)\tilde{\varrho}^{A'B}\right] = 1,$$

$$\text{tr}\left[(\sigma_x^{A'} \otimes B_1)\tilde{\varrho}^{A'B}\right] = 1,$$

(E11)

where $B_0 = \mathsf{M}_{0|0} - \mathsf{M}_{1|0}$ and $B_1 = \mathsf{M}_{0|1} - \mathsf{M}_{1|1}$. The operators of type $\text{tr}_A\left[\left(U_a^{A'}\mathsf{M}_a^{A'A}U_a^{\dagger A'} \otimes \mathbb{1}^B\right)\left(\frac{\mathbb{1}^{A'}}{2} \otimes \varrho'^{AB}\right)\right]$ are not positive in general (see [46]), but they have a positive expectation value on all separable vectors $\sum_i \pi_i^{A'} \otimes \tau_i^B$. Furthermore,

$$\text{tr}\tilde{\varrho}^{A'B} = \sum_a \mu_{a,0} = 1.$$

Thus, equation (E11) imply

$$\left(\sigma_z^{A'} \otimes \mathbb{1}^B\right)\tilde{\varrho}^{A'B} = \left(\mathbb{1}^{A'} \otimes B_0\right)\tilde{\varrho}^{A'B},$$

$$\left(\sigma_x^{A'} \otimes \mathbb{1}^B\right)\tilde{\varrho}^{A'B} = \left(\mathbb{1}^{A'} \otimes B_1\right)\tilde{\varrho}^{A'B}.$$

(E12)

These equations allow one to conclude that B_0 and B_1 anticommute

$$\{B_0, B_1\}\varrho_B = 0$$

(E13)

where ϱ_B is the reduced state of $\varrho'^{A'B}$. From equations

$$\text{tr}\left[\left(\mathbb{M}_z^{A'A} \otimes B_0\right)\left(|0\rangle\langle 0|^{A'} \otimes \varrho'^{AB}\right)\right] = 1,$$

$$\text{tr}\left[\left(\mathbb{M}_x^{A'A} \otimes B_1\right)\left(|+\rangle\langle +|^{A'} \otimes \varrho'^{AB}\right)\right] = 1,$$

(E14)

we can conclude that

$$\left(\text{tr}_{A'}\left((|0\rangle\langle 0|^{A'} \otimes \mathbb{1}^A)\mathbb{M}_z^{A'A}\right) \otimes \mathbb{1}^B\right)\varrho'^{AB} = \left(\mathbb{1}^A \otimes B_0\right)\varrho'^{AB},$$

$$\left(\text{tr}_{A'}\left((|+\rangle\langle +|^{A'} \otimes \mathbb{1}^A)\mathbb{M}_x^{A'A}\right) \otimes \mathbb{1}^B\right)\varrho'^{AB} = \left(\mathbb{1}^A \otimes B_1\right)\varrho'^{AB}.$$

(E15)

Finally, equations (E12), (E13) and (E15) allow reducing the expression $\text{tr}_{A_1',A_2'}\left[\Phi_{qc}(\varrho'^{AB})\right]$, where Φ_{qc} is the circuit given in figure E1, to the output of the standard self-testing SWAP gate, giving

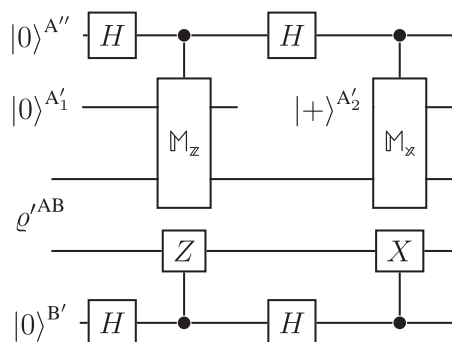$$\text{tr}_{A_1',A_2'}\left[\Phi_{qc}(\varrho'^{AB})\right] = \phi_+^{A''B'} \otimes \varrho_{\text{junk}}^{AB}.$$

(E16)

Figure E1. Isometry Φ_{qc} used in the proof of theorem E1.

ORCID iDs

Ivan Šupić ⓘ https://orcid.org/0000-0002-0361-6631
Matty J Hoban ⓘ https://orcid.org/0000-0001-9765-0373

References

[1] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 *Rev. Mod. Phys.* **81** 865–942
[2] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895–9
[3] Briegel H J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932–5
[4] Bell J S 1964 *Physics* **1** 195–200
[5] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 *Rev. Mod. Phys.* **86** 419–78
[6] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661–3
[7] Barrett J, Hardy L and Kent A 2005 *Phys. Rev. Lett.* **95** 010503
[8] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[9] Pironio S *et al* 2010 *Nature* **464** 1021–4
[10] Colbeck R 2006 Quantum and relativistic protocols for secure multi-party computation *PhD Thesis* University of Cambridge
[11] Acín A and Masanes L 2016 *Nature* **540** 213–9
[12] Reichardt B W, Unger F and Vazirani U 2013 *Nature* **496** 456
[13] Buhrman H, Cleve R, Massar S and de Wolf R 2010 *Rev. Mod. Phys.* **82** 665–98
[14] Anders J and Browne D E 2009 *Phys. Rev. Lett.* **102** 050502
[15] Hoban M J and Browne D E 2011 *Phys. Rev. Lett.* **107** 120402
[16] Mayers D and Yao A 2004 *Quant. Inf. Comput.* **4** 273
[17] McKague M 2014 *Theory of Quantum Computation, Communication, and Cryptography* (*Lecture Notes in Computer Science vol 6745*) ed D Bacon, M Martin-Delgado and M Roetteler (Berlin: Springer) pp 104–20
[18] Coladangelo A, Goh K T and Scarani V 2017 *Nat. Commun.* **8** 15485
[19] Kaniewski J 2017 *Phys. Rev. A* **95** 062323
[20] Šupić I, Coladangelo A, Augusiak R and Acín A 2018 *New J. Phys.* **20** 083041
[21] Šupić I and Bowles J 2019 Self-testing of quantum systems: a review arXiv:1904.10042
[22] Pallister S, Linden N and Montanaro A 2018 *Phys. Rev. Lett.* **120** 170502
[23] Markham D and Krause A 2018 A simple protocol for certifying graph states and applications in quantum networks arXiv:1801.05057
[24] Takeuchi Y and Morimae T 2018 *Phys. Rev. X* **8** 021060
[25] Pawłowski M and Brunner N 2011 *Phys. Rev. A* **84** 010302(R)
[26] Schrödinger E 1935 *Math. Proc. Camb. Phil. Soc.* **31** 555–63
[27] Wiseman H M, Jones S J and Doherty A C 2007 *Phys. Rev. Lett.* **98** 140402
[28] Cavalcanti D and Skrzypczyk P 2017 *Rep. Prog. Phys.* **80** 024001
[29] Uola R, Costa A C S, Nguyen H C and Gühne O 2020 *Rev. Mod. Phys.* **92** 15001
[30] Šupić I and Hoban M J 2016 *New J. Phys.* **18** 075006
[31] Gheorghiu A, Kashefi E and Wallden P 2015 *New J. Phys.* **17** 083040
[32] Tavakoli A, Kaniewski J, Vértesi T, Rosset D and Brunner N 2018 *Phys. Rev. A* **98** 062307
[33] Farkas M and Kaniewski J 2019 *Phys. Rev. A* **99** 032316
[34] Buscemi F 2012 *Phys. Rev. Lett.* **108** 200401
[35] Bowles J, Šupić I, Cavalcanti D and Acín A 2018 *Phys. Rev. Lett.* **121** 180503
[36] Paris M and Rehacek J 2004 *Quantum State Estimation* (*Lecture Notes in Physics vol 649*) (Berlin: Springer) 10.1007/b98673
[37] Prugovečki E 1977 *Int. J. Theor. Phys.* **16** 321–31
[38] Goh K T, Kaniewski J, Wolfe E, Vértesi T, Wu X, Cai Y, Liang Y C and Scarani V 2018 *Phys. Rev. A* **97** 022104
[39] Gheorghiu A, Wallden P and Kashefi E 2017 *New J. Phys.* **19** 023043
[40] Gallego R, Brunner N, Hadley C and Acín A 2010 *Phys. Rev. Lett.* **105** 230501
[41] Shi W, Cai Y, Brask J B, Zbinden H and Brunner N 2019 Semi-device-independent characterization of quantum measurements under a minimum overlap assumption *Phys. Rev. A* **100** 042108
[42] Branciard C, Rosset D, Liang Y C and Gisin N 2013 *Phys. Rev. Lett.* **110** 060405
[43] Šupić I, Skrzypczyk P and Cavalcanti D 2017 *Phys. Rev. A* **95** 042340

[44] Rosset D, Martin A, Verbanis E, Lim C C W and Thew R 2018 *Phys. Rev. A* **98** 052332
[45] Cavalcanti D, Skrzypczyk P and Šupić I 2017 *Phys. Rev. Lett.* **119** 110501
[46] Šupić I, Skrzypczyk P and Cavalcanti D 2019 *Phys. Rev. A* **99** 032334
[47] Sikora J, Varvitsiotis A and Wei Z 2016 *Phys. Rev. Lett.* **117** 060401
[48] Horodecki M, Horodecki P and Horodecki R 1999 *Phys. Rev. A* **60** 1888–98
[49] Hoban M J and Sainz A B 2018 *New J. Phys.* **20** 053048
[50] Renou M O, Kaniewski J and Brunner N 2018 *Phys. Rev. Lett.* **121** 250507
[51] Bancal J D, Sangouard N and Sekatski P 2018 *Phys. Rev. Lett.* **121** 250506
[52] Yang T H, Vértesi T, Bancal J D, Scarani V and Navascués M 2014 *Phys. Rev. Lett.* **113** 040401
[53] Bancal J D, Navascués M, Scarani V, Vértesi T and Yang T H 2015 *Phys. Rev. A* **91** 022115
[54] Zhang X and Zhao Q 2019 Simultaneous certification of entangled states and measurements in bounded dimensional semi-quantum games arXiv:1911.05981